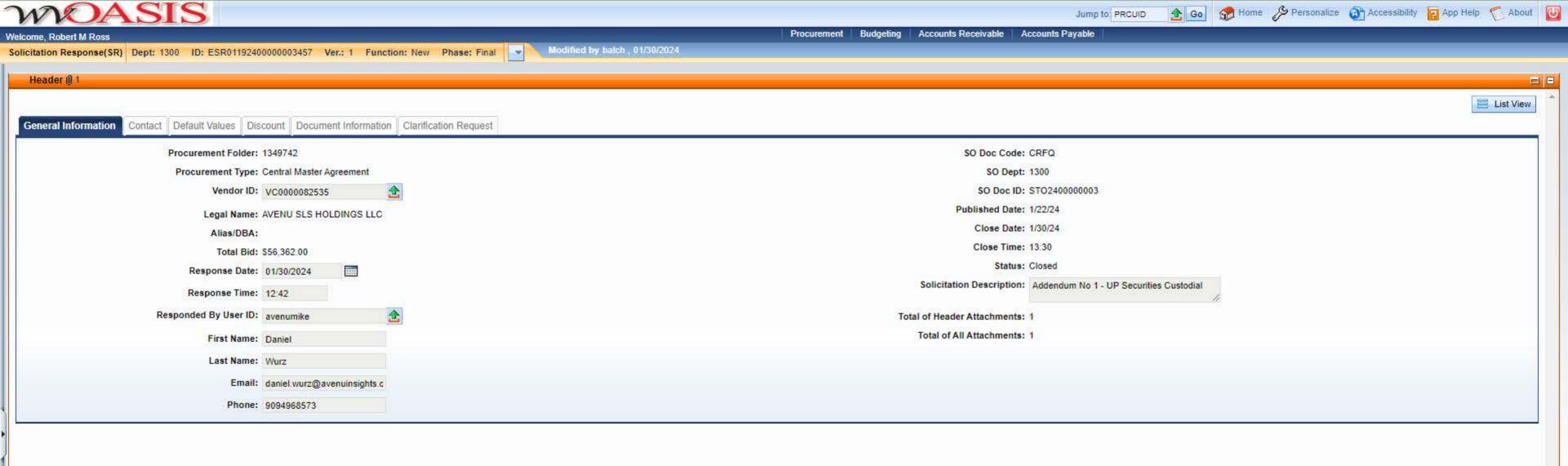


2019 Washington Street, East Charleston, WV 25305 Telephone: 304-558-2306 General Fax: 304-558-6026

Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.





Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130

## State of West Virginia Solicitation Response

Proc Folder: 1349742

Solicitation Description: Addendum No 1 - UP Securities Custodial

**Proc Type:** Central Master Agreement

 Solicitation Closes
 Solicitation Response
 Version

 2024-01-30 13:30
 SR 1300 ESR01192400000003457
 1

VENDOR

VC0000082535 AVENU SLS HOLDINGS LLC

Solicitation Number: CRFQ 1300 STO2400000003

**Total Bid:** 56362 **Response Date:** 2024-01-30 **Response Time:** 12:42:21

Comments: Although not a cost to the STO, Avenu believes that broker s fees should be disclosed in its proposal. Avenu

understands that the brokerage fees charged to rightful owners must be perceived as fair in order to protect the reputation of the STO s unclaimed property program. Accordingly, Raymond James withholds from transaction proceeds a low commission fee and charges no fees for very low value positions, with all commissions/fees deducted from gross sale proceeds prior to trade settlement as follows: \$0.05 per share commission; \$5.00 flat commission for

any position (lot) under 100 shares; SEC Section 31 Fee of \$0.0218/\$1,000.00 of principal value of trade; Commission is waived for any sale where the gross proceeds are less than or equal to the calculated commission rate; There is no commission for worthless sales. The STO will be notified in advance for decisions on Restricted Securities (\$150.00 for Legal Opinion to lift the restriction) and Foreign Securities that need to be deposited to a

foreign market prior to sale (\$250.00 per transaction).

#### FOR INFORMATION CONTACT THE BUYER

Toby L Welch (304) 558-8802 toby.l.welch@wv.gov

Vendor Signature X

FEIN#

DATE

#### All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Securities Custodial Services - Monthly Mtnce Fee	12.00000	MO	3300.000000	39600.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Monthly Maintenance Fee

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Securities Custodial Services - Physical Items	10.00000	EA	50.000000	500.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Receipt of Physical Items (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Securities Custodial Services - Receive DTC	350.0000	0 EA	20.000000	7000.00
	Item				

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Receipt of DTC Item (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Securities Custodial Services - Extensive	4.00000	EA	50.000000	200.00
	Research/Calcs				

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Extensive Research/Calculations (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	Securities Custodial Services - Receive Mutual Fund	4.00000	EA	25.000000	100.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Receipt of Mutual Fund (estimate listed)

Line Co	mm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6 Sec	curities Custodial Services - Liquidate DTC	250.00000	EA	20.000000	5000.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Liquidation of DTC Item (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	Securities Custodial Services - Liquidate Physical Item	10.00000	EA	50.000000	500.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Liquidate Physical Items (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	Securities Custodial Services - Liquidate Mutual Fund	100.000	00 EA	25.000000	2500.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Liquidate Mutual Fund (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
9	Securities Custodial Services - Return Physical Item	1.00000	EA	532.000000	532.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Return Physical Item (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
10	Securities Custodial Services - Return Mutual Fund	1.00000	EA	25.000000	25.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Return Mutual Fund (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
11	Securities Custodial Services - Return DTC	5.00000	EA	25.000000	125.00
	Item				

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Return DTC Item (estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
12	Securities Custodial Services - Mailings	5.00000	EA	20.000000	100.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Mailings

(estimate listed)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
13	Securities Custodial Services - Outgoing Wires	12.00000	EA	15.000000	180.00

Comm Code	Manufacturer	Specification	Model #	
84121806				

#### **Commodity Line Comments:**

#### **Extended Description:**

Outgoing Wires (estimate listed)

 Date Printed:
 Jan 30, 2024
 FORM ID: WV-PRC-SR-001 2020/05



## STATE OF WEST VIRGINIAPURCHASING DIVISIONSTATE TREASURER'S OFFICE UNCLAIMED PROPERTY DIVISION

REQUEST FOR QUALIFICATIONS FOR

#### SECURITIES CUSTODIAL SERVICES

CRFQ STO2400000003

JANUARY 30, 2024

#### Submitted By:

Avenu SLS Holdings, LLC 5860 Trinity Parkway, Suite 120 Centreville, VA 20120 Attn: Daniel Wurz, Director of Proposals

- (909) 496-8573
- Proposals@avenuinsights.com \_\_
  - www.avenuinsights.com (\$)



## 1 TABLE OF CONTENTS

TAB	BLE OF CONTENTS	2
COV	/ER LETTER	3
QUA	ALIFICATIONS	4
3.1 3.2 3.3 3.4	STAFF REQUIREMENTS:  WEB PORTAL REQUIREMENTS  DISASTER RECOVERY AVAILABILITY  PERSONALLY IDENTIFIABLE INFORMATION	13 17
MA	NDATORY REQUIREMENTS	23
4.1 4.2 4.3 4.4	MANDATORY CONTRACT SERVICES REQUIREMENTS AND DELIVERABLES  DELIVERABLES - ACCOUNTING AND REPORTING  DELIVERABLES - OTHER	23 39
CON	NTRACT AWARD	47
PER	FORMANCE	47
PAY	/MENT	47
TRA	VEL	48
FAC	CILITIES ACCESS	48
VEN	NDOR DEFAULT	48
MIS	SCELLANEOUS	49
WES	ST VIRGINIA MADATORY ATTACHMENTS	50
A. B. C.	PURCHASING AFFIDAVITADDENDUM ACKNOWLEDGEMENT FORMCONTACT & CERTIFICATION	50
AVE	ENU EXHIBITS	51
1. 2. 3. 4. 5. 6. 7.	CUSTODY CLIENT LIST  PERSONNEL RESUMES  NEXEN® REFERENCE GUIDE  EXTRANET REFERENCE GUIDE  AVENU REPORTS  SOC1 AND SOC2 REPORTS – CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE.  BUSINESS CONTINUITY PLAN - CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE.  DISASTER RECOVERY PLAN - CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE.	515151515151
	COV QU. 3.1 3.2 3.3 3.4 MA 4.1 4.2 4.3 4.4 COI PER PAV TRA VEN MIS WE A. B. C. AVI 1. 2. 3. 4. 5. 6. 7.	COVER LETTER  QUALIFICATIONS  3.1 STAFF REQUIREMENTS:  3.2 WEB PORTAL REQUIREMENTS  3.3 DISASTER RECOVERY AVAILABILITY  3.4 PERSONALLY IDENTIFIABLE INFORMATION  MANDATORY REQUIREMENTS  3.1 MANDATORY REQUIREMENTS  3.2 DELIVERABLES  3.3 DELIVERABLES  3.4 DELIVERABLES  3.5 DELIVERABLES  3.6 DELIVERABLES  3.7 DELIVERABLES  3.8 DELIVERABLES  3.9 DELIVERABLES  3.1 MENDATORY CONTRICT SERVICES REQUIREMENTS AND DELIVERABLES  3.1 DELIVERABLES  3.2 OF DELIVERABLES  3.3 DELIVERABLES  3.4 OF DELIVERABLES  4.5 DELIVERABLES  5. OF DELIVERABLES  5. OF DELIVERABLES  6. DELIVERABLES  7. DELIVERABLES  8. ADDENDUM ACKNOWLEDGEMENT FORM.  8. ADDENDUM ACKNOWLEDGEMENT FORM.  9. C. CONTACT & CERTIFICATION  AVENU EXHIBITS  1. CUSTODY CLIENT LIST  1. CUSTODY CLIENT LIST  2. PERSONNEL RESUMES  3. NEXEN® REFERENCE GUIDE  4. EXTRANET REFERENCE GUIDE  5. AVENU REPORTS  6. SOC1 AND SOC2 REPORTS  7. BUSINESS CONTINUITY PLAN - CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE  7. BUSINESS CONTINUITY PLAN - CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE



#### 2 COVER LETTER

January 30, 2024

Department of Administration, Purchasing Division 2019 Washington Street East Charleston WV 25305-0130 Attn: Toby L. Welch

Submitted electronically: <a href="https://www.wvoasis.gov">https://www.wvoasis.gov</a>

RE: Securities Custodial Services - Solicitation Number ARFP STO2400000003

Dear Purchasing Officer Welch:

We at Avenu SLS Holdings, LLC ("Avenu") are pleased to present our proposal for Securities Custodial Services for the above-captioned Bid Opportunity.

Avenu and its key service delivery partners (the Bank of New York Mellon and Raymond James) are not on the West Virginia State Treasurer's Restricted Financial Institution List. This differentiates us from other vendors, such as Wells Fargo, Blackrock Inc., JPMorgan Chase & Co., Goldman Sachs Group, Inc., and Morgan Stanley, We are headquartered in Centreville, Virginia, and, with the banking and brokerage expertise of our key partners, are prepared to provide best-inclass unclaimed security management services to the State of West Virginia State Treasurer's Office ("STO") for the duration of the term set out in the Solicitation.

Avenu takes immense pride in possessing the most experienced and continually innovative unclaimed securities custody team in the industry, and we are dedicated to delivering unparalleled services. The Avenu team's extensive background with STO policies and practices, along with our broad experience serving a majority of all state unclaimed security management programs, uniquely enables us to deliver results consistent with the intricacies, rules, regulations, policies, and procedures that govern the STO's unclaimed securities program. Avenu's team offers a detailed and unmatched understanding of this highly specialized administrative need, ensuring efficient oversight and outstanding management of the STO's unclaimed securities activity.

The combination of our expertise, exceptional service features, and unwavering commitment to the success of the STO's Unclaimed Property Division makes our proposal highly compelling and persuasive. For a more comprehensive overview of our key themes, please refer to the attached Proposal.

We sincerely appreciate your attention to our proposed service package and eagerly anticipate the opportunity to discuss the details further at your convenience.

Thank you.

Sincerely,

James Barkman Chief Financial Officer Avenu SLS Holdings, LLC

E-Mail: Proposals@avenuinsights.com



#### 3 QUALIFICATIONS

Avenu is pleased to respond to the STO's Qualifications requirements in this section. For ease of reference, Avenu has included the STO's requirements in bold blue text.

Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications. By signing and submitting its bid, Vendor certifies that it has the minimum qualifications. Vendor shall Provide complete responses to each requirement and provide any additional information as requested in this section. All required documents should be provided with Vendor's bid and must be provided within 24 hours of request.

Avenu certifies that it meets the requirements set out by the State Treasurer's Office (STO) and has completed responses to each requirement with additional information requested or relevant. All required documentation is included in the Avenu Proposal. Avenu is aware of, knowledgeable and compliance with the policies of the STO, including of course all rules and procedures relevant to the administration of the state's unclaimed property program, but also of the Treasurer's policy on restricting the flow of state dollars to particular financial institutions.

Avenu, using the extraordinary resources of the Bank of New York Mellon and of Raymond James, has provided Unclaimed Securities Custodial Services to state programs for over thirty-eight (38) years. Neither of these companies is on the Treasurer's Restricted Financial Institution List. We have been the proven and reliable provider of these specific services to the STO for nearly eight (8) years. Avenu has repeatedly demonstrated its commitment to provide, and to make any adjustments needed to continue to provide, these important administrative support services.

Avenu is a leading government solutions provider with a suite of offerings for unclaimed property, tax, license, records management, revenue enhancement, IT managed solutions, digital processing, and justice. Our dedication to state and local governments across the country has been recognized by Avenu being listed on the GovTech 100 list for the past six (6) consecutive years.

Our Unclaimed Property Solutions business suite includes securities custody, software and support, calls and claims management, annual reports intake management, HRS Pro annual reporting software, and rightful owner outreach. Avenu has invested over \$1.2M in its Unclaimed Property Solutions business and is constantly delivering innovative solutions to meet specific client needs. Avenu will continue to leverage its long-standing relationships with the Bank of New York Mellon ("BNY Mellon") and Raymond James ("RJ") to provide West Virginia with the most comprehensive Securities Custodial Services offering possible.

# GOVTECH GOVTECH GOVTECH 100 AWARD WINNER 6th Year In a Row

Headquartered in Centreville, Virginia, Avenu is a privately-owned Limited Liability Company (LLC) that has grown to have an expansive footprint of seven hundred (700) employees and ten (10) national offices strategically dispersed throughout the United States in Virginia, Alabama, California, Texas, Massachusetts, and New Hampshire. Avenu's solutions are used by over three thousand (3,000) clients across the country and supports clients in all 50 states. Staff in our Massachusetts office provide securities custody services for the Unclaimed Property program administrations in over half of all states and territories.

#### Avenu Qualification Highlights

- Provider of Securities Custodial
   Services for the STO since 2016
- Headquartered in Centreville, VA
- 700 employees and 10 offices
- Provider of proposed services to 29 states
- Specific experience with all 50 states in Unclaimed Property
- Dedicated Custody and Accounting Services team with 8 years of first-hand experience supporting the STO
- Strength and Stability and Extensive Corporate Resources
- Nationally recognized for service to State and Local governments





Avenu's solutions are used by over three thousand (3,000) clients across the country and supports clients in all 50 states

Avenu has all the expertise, resources, depth, and expertise needed to continue its support of the STO and its robust portfolio of \$296 million, a commitment we have upheld steadfastly for over thirty-eight (38) years. Our Unclaimed Property Services Division, honed over an expansive 40-year journey, proudly delivers an expansive suite of administrative solutions tailored to meet the needs of state unclaimed property administrators. Our specialty lies in embracing all aspects of Unclaimed Property – from security custody, innovative management solutions and efficient claims processes – seamlessly connecting property holders and rightful owners with services and software solutions unmatched nationwide.

Dating back to 2016, Avenu has been honored to serve as the unclaimed securities management provider for the STO, effectively delivering the comprehensive range of services detailed in this proposal. The effectiveness of our service and commitment to the success of the STO's unclaimed securities custody operations has been demonstrated with real life support.

With a unique blend of technical proficiency and dedicated commitment, we provide exceptional customer service to our roster of 29 state programs, more than any other provider. Our team's in-depth understanding and experience in managing West Virginia State Treasurer's Office property has proven Avenu as trustworthy and reliable partner. Avenu recognizes the utmost importance of safeguarding citizens' rights, returning property to rightful owners, delivering top-tier, responsive service to constituents, and driving efficiencies and cost reductions through technology, automation, and personal care. But above all, Avenu is committed to doing business using only the highest ethical standards, and to working with partners who share that same focus and commitment.

In addition to focusing on ethical business practices, Avenu has become the largest and most successful provider of unclaimed securities management services in large part because of its steadfast commitment to the best interests of our clients. This includes ongoing efforts to identify efficiencies and cost-saving opportunities. Our goal is to develop and maintain long-term trustworthy relationships with our clients and to provide comprehensive ever-improving services that provide unmatched benefit to their programs.

For perspective, Avenu's custody solution has been developed and enhanced over a period of almost four decades, and as a leader in the industry, we have created many ways to streamline processes and solve complex issues for state unclaimed property program administrators. Our success can be attributed to a steadfast commitment to our existing client base and our efforts to identify efficiencies and cost-saving opportunities. Our goal is to develop and maintain long-term relationships with our clients and provide comprehensive ever-improving services that provide a benefit to our clients.

Far from being a one-size-fits-all service provider, Avenu, in collaboration with our partners Raymond James and Bank of New York Mellon, delivers tailored flexibility and customization essential for STO operations. We go beyond the norm, offering unique services often overlooked by competitors, such as:



- Maintaining physical certificates on your behalf,
- · Handling of voluntary corporate actions and class actions on your behalf,
- · Providing direct liaison with holders and owners, and
- Delivering swift and agile adaptability to alter processes and reports as needed.

For nearly four decades since 1984, Avenu has been the trusted partner in safeguarding states' unclaimed securities portfolios, innovatively crafting end-to-end solutions. Our Unclaimed Property Solutions team is fully committed to addressing every facet of unclaimed property management, from seamless system and process management to secure securities custody. By reputation and by our record, the Avenu team does not just deliver solutions - it redefines them.

#### **3.1 STAFF REQUIREMENTS:**

- 3.1.1 The Vendor shall provide a quality, experienced and professional staff to perform the Services under this contract. Accordingly, staff assigned to the contract shall have least three (3) years of experience in providing unclaimed securities custodial services similar in nature to the Services required in this RFQ. Vendor shall provide the following information:
  - A. the number of staff assigned to the STO contract,
  - B. the names and contact information of the specific staff to be assigned to the STO contract, and
  - C. a resume for each staff member assigned to the **STO** contract that states their qualifications, experience, and training, including relevant continuing professional education.

Avenu's team takes pride in its customer service, which is at the core of our solution and truly sets us apart from other vendors. We act as an extension of the STO's staff and offer complete, customized support for the STO's specific unclaimed securities requirements. We perform tasks that are traditionally assigned to state staff so that those valuable employees are able to spend more time focusing on other important duties. The level of support makes a positive difference in their work environment and contributes to their ability to accomplish additional tasks and day-to-day activities. Avenu looks to enlist the talent from many different areas to ensure that we are keeping pace with the latest and greatest.

Our client service commitment to the STO is comprehensive. Avenu genuinely wants to continue to be the State of West Virginia's partner in unclaimed property. Avenu offers the STO an ethical, dedicated, and experienced account management team with a primary securities account manager to handle all aspects of the STO's needs along with knowledgeable backup support from our full operations support team of experienced personnel with the knowledge and resources to continue to meet all of the STO's requirements. Avenu will have five professionals (Mike Poth, David Lemoine, Deb Arnold, Ted Tran and Victoria Perkins) specifically assigned to the STO to respond to all inquiries regarding contract activities, questions related to ordering re-registration, liquidation, delivery, and for any other inquiry as relates to services described in this RFP, but also has access to the full breadth and scope of the entire Unclaimed Property Solutions team as well as the leadership at Avenu and our partners Raymond James and The Bank of New York Mellon.

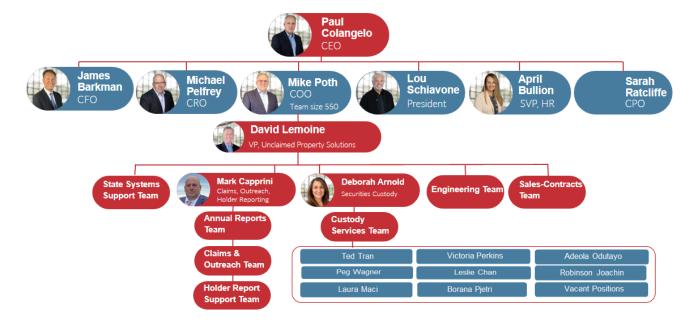
Our team experience includes a former State Treasurer, Deputy State Treasurer, State Unclaimed Property Administrator, Unclaimed Property Program Manager, and State in-house unclaimed property system administrators along with rightful owner claims management experts, and annual holder reporting specialists. All of these resources, some with as much as 30 years of experience in unclaimed property will be available to the Department, are utilized, and leveraged when the need arises. As former state employees and state officials, our team is intensely aware of the need to maintain high ethical standards for ourselves and for those vendors with whom we do business.

Victoria Perkins is the account manager for the STO and will continue to be the primary account manager if awarded the contract. This team is further supported by Deb Arnold, Director of Securities Custody, and Ted Tran who is the Deputy Director as well as the other members of the Custody service team who work closely together.

Avenu has provided an organization chart and resumes for staff assigned to the STO directly and has also included additional support team Personnel Resumes under Exhibit 1, who are also available to provide additional support as needed. Avenu also believes that our partnerships with Raymond James and The Bank of New York Mellon only strengthen our skillset and our client's, therefore we have included our top contacts below as well.



### **Avenu Leadership**



#### 3.1.1 AVENU – STO ASSIGNED STAFF RESUMES

#### MIKE POTH - Mike.poth@avenuinsights.com CHIEF OPERATING OFFICER

Mike is an award-winning leader known for his strategic and operational excellence, improving morale, streamlining operational processes, and increasing customer retention and satisfaction. He has extensive experience transforming and optimizing enterprise software, services and solutions designed for international, federal, state, and local governments. Prior to his current position Mike held Senior Executive positions for CentralSquare Technologies, Banjo LLC, and was the Chief Executive Officer of the First Responder Network Authority, an independent \$35B Authority in the federal government tasked to build, operate, and maintain the first high-speed, nationwide wireless broadband network dedicated to public safety.

As Vice President and General Manager at Hewlett Packard and Northrop Grumman he also led organizations focused on developing and delivering mission critical public safety and administrative solutions to government.

He holds a BS in Criminal Justice and a master's degree in public administration from Arizona State University. He has completed executive certifications from the University of Virginia-Darden and the University of Chicago-Booth and received numerous awards including Executive of the Year and Top Executives to watch.

#### DAVID LEMOINE - David.lemoine@avenuinsights.com VP, UNCLAIMED PROPERTY SOLUTIONS

David Lemoine is Vice President of Avenu's Unclaimed Property Solutions group. David joined Avenu in 2013 and is responsible for all aspects of Avenu's unclaimed property services, including compliance reporting, securities custody, claims management and system solutions. David is a senior level leader with a wealth of experience in law, state policy creation, public administration and most applicable here, in designing and delivering state unclaimed property administrative solutions. He was the 2016 recipient of the Lucille Maurer Award, given by the National Association of State Treasurers in recognition of outstanding service to the association by a former State Treasurer.



As a former State Treasurer, David has extensive experience in unclaimed property administration. During his time as the Maine State Treasurer (2005 to 2011), he overhauled and reorganized the office structure and implemented many new administrative processes, most of which are still in place today. His innovations included the use staggered outreach efforts that increased owner contacts, sped claimant interactions and increased reunification results. He was an early adopter of automated claims fast-tracking and engineered a coordinated effort with other branches of government to access better addresses for rightful owners. More than 60% of unclaimed property received by Maine each year was reunited with rightful owners as direct a result of these innovations.

David also was active in other areas of STO responsibilities, where he adopted new bond management tools, led cost-saving refunding, implemented the Build America Bonds program in Maine and worked with rating agencies to sustain Maine's important credit status. He also gained enormous insight into other aspects of state government through service on the boards of the State's retirement system, housing authority, 529 oversight group and Municipal Bond Bank.

Prior to being elected as State Treasurer, he was a member of the Maine House of Representatives where he chaired the powerful Taxation Committee and held a number of other leadership positions. David, a licensed attorney who began practicing law in 1989, established his own law firm in 1993 and maintained an active private law until being elected as State Treasurer. Prior to joining Avenu, David was the northern New England manager of Government Relations for TD Bank.

## DEBORAH ARNOLD - Deborah.arnold@avenuinsights.com DIRECTOR, SECURITIES CUSTODY

Deborah Arnold is the Director of Avenu's Unclaimed Securities Custody group and is responsible for overseeing the operations of the team which supports our state administrators with their Lottery and Insurance Programs and unclaimed property needs. This includes the monitoring of corporate actions, transfers receipts and liquidations, claimant, and state questions, 1099's, cash movements and cryptocurrency. She also ensures best practices, policy management and process improvements.

Deborah has over 35 years' experience in the financial services industry bringing a strong background and knowledge base of securities, custody and leadership and has held steadily progressive positions on the custodian side at both State Street Bank and Investors Bank and Trust Company from Supervisor, Assistant Vice President to Vice President and Director.

She has extensive experience leading and working in operations teams responsible for accounting, pricing, cash and custody services for Mutual Fund and Private Equity clients and funds. She has also spent over 8 years leading Investor Servicing teams focused on handling investor subscriptions/redemptions, anti-money laundering, reporting and statement generation. Deborah joined Avenu in 2021.

Deborah holds a Bachelor of Science in Finance from Pennsylvania State University with a minor in Economics.

## **TE**D TRAN - Ted.tran@avenuinsights.com DEPUTY DIRECTOR, SECURITIES CUSTODY

Ted Tran is the Deputy Director of Avenu's Unclaimed Securities Custody group and is responsible for leading a team of supervisors and specialists to support more than two dozen State unclaimed property, lottery, and insurance programs. Overseeing daily operations, client directives, P&L finances, training of clients/associates, research, and communications to/from clients, vendors, and holders. Ted joined Avenu in 2014 and has over 9 years of unclaimed securities custody experience and has had steadily progressive positions, recently being promoted to Deputy Director. Ted has a deep understanding of unclaimed property securities, workflows, and reconciliation.

Ted was actively involved in the development of Avenu's cryptocurrency custody solution and is considered a subject matter expert and covered cryptocurrency at the 2019 National Association of State Treasurers Association Symposium in Rhode Island and the 2022 Symposium in San Antonio.

Ted holds a Bachelor of Science degree in Management, with a Finance concentration, from the University of Massachusetts Boston and a Bachelor of Science degree in Information Technology from the University of Massachusetts Lowell. He understands unclaimed property along with the necessary exception processing and research that go along with



maintaining the unclaimed property portfolio. Ted has excellent customer service skills, maintaining strong professional relationships and rapport with state contacts and outside vendors.

#### VICTORIA PERKINS - Victoria.perkins@avenuinsights.com CLIENT SERVICES SUPERVISOR, SECURITIES CUSTODY

Vicki is a Client Services Manager and the current Account Manager for the STO, responsible for the daily support of state clients for the management of their portfolios for all types of transactions for both DTC and Mutual Funds. Vicki also has extensive knowledge in claims processing, dividend reinvestment plans, securities research, and unclaimed property securities. She also provides proposal support for the Avenu team due to her strong grasp of processes and procedures within unclaimed property.

Vicki first joined Avenu in 2014 in the Audit group as a Communications Administrator, but due to her ability to build client relationships and problem-solving abilities, she moved over to the Unclaimed Securities Custody team in 2017.

She strengthens Avenu's team with her experience in unclaimed property audits, clear client communications, complex report tracking for Agree to Participate (ATP), Work in Progress (WIP), ACT (Audit Communications Tool), holder research and ongoing RFP Support.

Prior to joining Avenu, Vicki held steadily progressive positions at DST Systems, PFPC (First Data Corporation) and Boston Financial Data Services (BFDS). Her background includes positions as a Senior Business Systems Analyst and a Client Services Corporate Actions Administrator. Vicki holds a bachelor's degree in business management from the University of Massachusetts at Lowell with a Certificate in Computer Proficiency.

#### 3.1.2 RAYMOND JAMES RESUMES

The principal individuals responsible for the security liquidation within RJA are Ronald L. Tillett and Pamela P. Allen. While all individuals associated with trading the unclaimed securities at Raymond James are licensed with the necessary exchanges and self-regulatory bodies, we have included the credentials of the two primary contacts with the unclaimed property liquidations with state clients.

## RONALD TILLETT CRD# 4409668 MANAGING DIRECTOR, HEAD OF MID-ATLANTIC PUBLIC FINANCE

5820 Patterson Avenue, Suite 200 Richmond, Virginia, 23226 804-225-1148 Ron.tillett@raymondjames.com

Ron Tillett joined Raymond James in April 2012 following the Firm's acquisition of Morgan Keegan and became the Head of the Mid-Atlantic Public Finance Practice in 2014. Ron, the principal assigned to lead this engagement, has extensive experience with unclaimed property programs having served as the Deputy State Treasurer and State Treasurer for the Commonwealth of Virginia. In those positions, he had direct responsibility for Virginia's unclaimed property program. As State Treasurer and a member of the National Association of State Treasurers (NAST), he has had extensive involvement at the national level for unclaimed property programs.

As Secretary of Finance for two Virginia Governors, he directed the finance agencies' activities including the State Treasury, State Budget State, State Tax State, State Comptroller, and the State Internal Auditor. He was involved in all aspects of unclaimed property for Virginia including State legislation, the Uniform Act, contracts, and the liquidation of securities.

Mr. Tillett has continued his involvement with NAST and the NAUPA organizations as a Corporate Affiliate, serving as a sponsor for events and activities. He visits States unclaimed property programs throughout the year and has worked with Avenu in submitting bids for services and in developing strategies in dealing with States and their unclaimed property programs. Ron's career highlights and credentials are listed as follows:

Head of the Raymond James Mid-Atlantic Public Finance Practice. 2001-2023



- Manage Firm's Unclaimed Property Security Liquidation Practice for 30 States, the District of Columbia, and the Commonwealth of Puerto Rico
- Manage the Mid-Atlantic Public Finance Investment Banking Practice
- Secretary of Finance, Virginia Governor's Cabinet. 1996-2001
- Treasurer of Virginia and Deputy Treasurer of Virginia. 1987-1996
- Senior Staff Advisor, Virginia General Assembly, House Appropriations Committee and the Joint Legislative Audit and Review Commission. 1978-1987
   Major Boards and Other Appointments
- Commonwealth of Virginia Debt Capacity Advisory Committee: Governor Appointment, 2010-2023
- Christopher Newport University Board of Visitors: Governor Appointment 2022-2026
  - Trustee, Wason Center for Civic Leadership, Christopher Newport University
  - Chairman, Investment Committee, CNU Education Foundation
- Board of Trustees of the National Institute for Public Finance, National Association of State Treasurers and Pepperdine University. 2015-2023
- Chairman of the Board, Atlantic Union Bankshares Corporation, 2005-2023
- Corporate Affiliate Advisory Board, National Association of State Treasurers, 2022-2025

#### **SEC** and Financial Industry Regulatory Authority Licenses (FINRA)

Series 7 - General Securities Representative

Series 50 - Municipal Advisor Representative

Series 52 - Municipal Securities Representative

Series 53 – Municipal Securities Principal

Series 54 - Municipal Advisor Principal

Series 63 - Uniform Securities Agent State Law Examination

Series 79 – Investment Banking Representative

Series 99 - Securities Operations Representative

Under a contract with the Department, Ron will oversee the brokerage services which consist of both pre- trade analysis and liquidations. In addition, he will oversee the worthless research and liquidation process if the Department chooses to sell those securities.

#### PAM ALLEN

#### FIRST VICE PRESIDENT/SALES ASSISTANT

Pam Allen joined RJA in 1981 and is a First Vice President/Sales Marketing Coordinator in the RJA Institutional Equity Trading Department. Ms. Allen began her career with Morgan Keegan as a Retail / Institutional Sales Assistant working for the firm's Vice Chairman.

Since 1991, Ms. Allen has been working in the Investment Banking Division in addition to the Institutional Equity Sales Department of Morgan Keegan coordinating the marketing efforts for Initial Public Offerings as well as secondary stock offerings and other Morgan Keegan equity events and conferences. She has extensive experience in selling and trading securities on all exchanges.

Ms. Allen holds the NASD Series 7 – General Securities Representative Professional License and has completed the NASAA Series 63 – Uniform Securities Agent State Law Examination. Ms. Allen has been involved in trading securities at RJA for 29 years. Ms. Allen has had direct responsibility for the liquidating of unclaimed securities for RJA for 11 years working with Ron Tillett and Avenu.

Under a contract with the Department, Pam will serve as the day-to-day contact with Avenu for processing liquidation of securities.

#### Pam Allen, CRD# 1039000

Vice President, Sales Assistant for Liquidating Unclaimed Securities 1380 Environ Way
Chapel Hill, NC 27517



Financial Industry Regulatory Authority Licenses (FINRA)
Series 7- General Securities Representative
Series 63 - Uniform Securities Agent Department Law Examination
Series 99 - Securities Operations Representative

#### 3.1.3 BANK OF NEW YORK MELLON RESUMES

#### J**ESS**IC**A ST**RUB <u>RELATIONSHIP MANAGER</u>

Jessica joined Asset Servicing's Investment Management segment, as a Relationship Manager, in February 2022. In this role, she leads Asset Servicing's efforts in managing key strategic relationships, in our growing Asset Manager space. She serves as the escalation contact for operational and compliance issues and has complete oversight of the relationship. Prior to this role, she served as a Senior Project Manager on the Client Onboarding team. In this capacity, she was responsible for the overall program/project management of Asset Servicing initiatives by preparing and completing action plans, resolving problems, and implementing change. Before moving to the project manager team in 2015, she served as a Middle Market Account Manager; where she acted as a liaison between the Tax-Exempt Defined Contribution and Defined Benefit clients, our servicing department, and affiliated entities.

Prior to joining BNY Mellon in 2009, Jessica was a Client Manager for Bank of America's Government Banking division. During her time, she managed over 900 municipal relationships with their operational banking needs.

In addition, she was integral in developing Cash Flow Solutions model, which assisted large government and health care institutions throughout the national Bank of America footprint to streamline treasury products, banking structure and assist in long term cash forecasting.

Jessica earned a Bachelor of Science degree in Political Science from Pennsylvania State University. Jessica and Nicole will partner with Christy to support Avenu. They will serve as a point of escalation and be responsible for the overall relationship with BNY Mellon.

#### CHRI**ST**Y W**EST**BROOK**S** CLIENT SERVICE DIRECTOR, VICE PRESIDENT

Christy Westbrooks joined BNY Mellon in 1998 and is responsible for ensuring service quality.

In this capacity the Service Director (SD) closely monitors daily operations and system workflows to ensure proper service levels are maintained or exceeded. She ensures that all service delivery commitments are met for Avenu and is in consistent communication with her assigned team at Avenu. She also ensures that BNY Mellon is in full compliance with all regulatory requirements and in turn that Avenu and our clients meet any applicable requirements. Christy also works closely with Relationship Management and the Custody team on matters that need escalation due to the nature of the issue though those are not common.

Jessica and Christy are fully engaged in all matters related to our clients, from routine service issue escalation to new product rollouts meeting twice a month with the custody team to discuss. In addition, Christy ensures deployment of new business opportunities and will look for ongoing ways to continuously improve the relationship.

Christy received a Bachelor of Arts in Mathematics – Minor in Psychology from Lake Forest College. Under a contract with the STO, Christy would support Avenu and be available for any issues that may arise and ensure that BNY Mellon processes all work as directed by Avenu both timely and accurately within agreed upon deadlines.

3.1.2. Project Implementation Team: Vendor shall provide staff with at least three (3) years' experience in providing unclaimed securities custodial services similar in nature to the Services required in this RFQ for the Project Implementation Team. Other project team members will include staff from the Unclaimed Property Division and other suggested STO staff as may be assigned by the STO and the Vendor. The Project Implementation Team will work to implement the Services to be provided by the Vendor, with the goal of a smooth transition into the contract.



Avenu is proud and honored to be the incumbent custodian with a current team in place for the West Virginia State Treasurer's Office, Division of Unclaimed Property. Because of this, a project implementation team is not required. Please refer to our Staff Resumes included above in Section 3.1 as well as additional Personnel Resumes from the Custody team are included under Avenu Exhibit 1.

3.1.3. In the response to this RFQ, Vendor shall describe the Project Implementation Team, specifying its members, their qualifications and experience, and organizational structure for this project. Specify the names of the persons on the Project Implementation Team, together with all contact information, and provide a resume that states their qualifications, experience, and training, including relevant continuing professional education. This information should be provided with the vendor's bid and shall be provided within 24 hours of request.

Avenu is proud to be the incumbent custodian with a current team in place for the West Virginia State Treasurer's Office, Division of Unclaimed Property and because of this, a project implementation team will not be required. Please refer to our Staff Resumes found in Section 3.1 above and additional Personnel Resumes from the Custody team are included under Avenu Exhibit 1.

3.1.4. The Vendor shall identify all principal supervisory and management staff, including engagement partners, managers, other supervisors, and specialists, who would be assigned to the Project Implementation Team that will serve the STO contract. This information should be provided with the vendor's bid and shall be provided within 24 hours of request.

Avenu is proud to be the incumbent custodian with a current team in place for the West Virginia State Treasurer's Office, Division of Unclaimed Property and because of this, a project implementation team will not be required. Please refer to our Staff Resumes found in Section 3.1 and additional Personnel Resumes from the Custody team are included under Avenu Exhibit 1.

3.1.5. Vendor shall provide quality of staff over the term of the contract and ensure that any new or additional staff members have the same qualifications, training and experience as the staff members Vendor provided in its bid to this RFQ. The Vendor shall inform the STO in writing of any personnel or staff changes that would affect the Services provided to the STO.

As the current provider to the STO, Avenu will continue to provide the same quality staff as is in existence currently. Victoria Perkins as the Account Manager will stay in place along with support from Ted Tran and Deb Arnold. Avenu also agrees to inform the STO in writing of any personnel or staff changes.

3.1.6. References: Vendor shall provide positive references. Provide the names of at least three (3), but no more than five (5), clients for which Vendor provides services similar to those required by the STO that may be contacted as references for purposes of this RFQ. Include the name and telephone number of the contact person for each of the clients specified. At least one (I) of these clients should have operations of at least the size, complexity, and nature of the STO as described in the Overview herein. All or none of these clients may be contacted by members of the Evaluation Committee to determine the ability of the Vendor and the level of satisfaction with the Vendor. Furthermore, the STO reserves the right to contact any person or entity it believes prudent in order to inquire about the Vendor. This information should be provided with the vendor's bid and shall be provided within 24 hours of request.

Avenu has provided three (3) references below as requested. Avenu provides all of the specific services requested in this RFQ and other related services solely to government (unclaimed property) agencies.

Based on the specific requirements of this RFQ, we have chosen the Indiana Attorney General's Office, The Tennessee State Treasury Department, and the Missouri State Treasurer's Office as our references, due to the similarities in the scope of services provided. Additionally, we have provided contact information for all our state clients can be found under Avenu Exhibit 2, Custody Client List.

The STO is encouraged to contact any or all of our clients for information on the services we provide. As the STO has been utilizing our services since 2015, it is our hope that STO staff can be one of our best references.



Unlike other custodians with limited experience and a small number of unclaimed property references, Avenu has been providing unclaimed securities custody for nearly 40 years and has remained focused on providing the best-possible customized solution to address the unique needs of unclaimed property programs.

<b>N</b> ame of Organization	Dates of <b>S</b> ervice	List of <b>S</b> ervices Performe <b>d</b>	Contact name, email a <b>ddr</b> ess, an <b>d</b> phone numbe <b>r</b>
Indiana Attorney General's Office Unclaimed Property Division	Provided Custody Services: 1990 - present	Securities Custody Services, Maintenance of Securities (Book Entry, Mutual Funds, and Others); Receipt, Liquidation and Transfer of Securities (Book Entry, Mutual Funds and Others). Perform Securities and Corporate Action research.	Amy T. Hendrix Director of Unclaimed Property Division P.O. Box 2504 Greenwood IN 46162 317.883.4521 (phone) amy.hendrix@atg.in.gov
Tennessee State Treasury Department Unclaimed Property Division	Provided Custody Services: 1990 - present	Securities Custody Services, Maintenance of Securities (Book Entry, Mutual Funds, and Others); Receipt, Liquidation and Transfer of Securities (Book Entry, Mutual Funds and Others). Perform Securities and Corporate Action research.	John Gabriel, Director Andrew Jackson Building, 10 <sup>th</sup> floor Nashville, TN 37243-0242 615.253.0242 (phone) john.gabriel@state.tn.us
Missouri State Treasurer's Office Missouri Unclaimed Property Division	Provided Custody Services: 2019 - present	Securities Custody Services, Maintenance of Securities (Book Entry, Mutual Funds, and Others); Receipt, Liquidation and Transfer of Securities (Book Entry, Mutual Funds and Others). Perform Securities and Corporate Action research.	Scott Harper Director of Unclaimed Property P.O. Box 210 Jefferson City, MO 65102  573.751.2082 (phone) scott.harper@treasurer.mo.gov

#### 3.2 WEB PORTAL REQUIREMENTS

3.2.1. Vendor remote web portal must not require Java, Silverlight, Adobe Flash, Active X Controls or any additional third-party plugins or dependencies. All web applications must be compatible with the latest version of Microsoft Edge (Chromium engine). All web communications whether remote or internal, must be secured using a minimum of TLS v 1.2. Any required cipher suites, protocols or encryption technology that has been publicly exploited (published CVE) must be immediately remediated upon discovery, including any minimum-security requirements.

Avenu acknowledges the requirements above. Avenu uses BNY Mellon's extraordinarily sophisticated and secure NEXEN® tool to deliver Web Portal services for all our Securities Custody clients. NEXEN® employs controls designed to detect and protect against unauthorized access, such as single (username/password) and two-factor user authentication for sensitive transactions, data encryption and a firewall design that ensures secure communications and is FFIEC compliant. The protocol specified for securing the communications used by NEXEN®, Transport Layer Security (TLS) 1.2, is the industry standard protocol designed to protect the privacy of information communicated over the internet between clients and the on-line portal. All data, including user passwords, is transmitted through the portal using TLS. In addition, NEXEN® will terminate or automatically log off a user from the browser session after 20 minutes of inactivity. After 15 minutes, a user is prompted with a warning message allowing them to continue if desired. Finally, the system's architecture strengths are in its private-labeled secure cloud completely enclosed in BNYM data centers which allow NEXEN® to deliver resilient, secure platform solutions that scale, cost less, and accelerate time to market. Hosting its own digital ecosystem within its secure data centers enhances the bank's agility in bringing new solutions to market and allows clients to access world class services. NEXEN® is a multifaceted, open-source, private cloud-based technology platform built on BNY Mellon's BXP Platform as a Service (PaaS). It does not require Java, Silverlight, Adobe Flash, Active X



Controls or any additional third-party plugins or dependencies, and it is compatible with the latest version of Microsoft Edge.

3.2.2. Approval of use of third-party plugins or dependencies are made at the sole discretion by the West Virginia State Treasurer's Office Information Technology Division.

Avenu agrees that approvals for the use of third-party plugins or dependencies, if ever needed, will be made at the sole discretion by the West Virginia State Treasurer's Office Information Technology Division.

3.2.3. All web portals shall be developed with a mobile-friendly HTMLS framework, allowing or access across multiple devices including, but not limited to, phones, laptops, desktops, and tablets.

Avenu agrees that all web portals shall be developed with a mobile-friendly HTMLS framework, allowing for access across multiple devices including, but not limited to, phones, laptops, desktops, and tablets.

- 3.2.4. All web portals shall be tested for fully compatibility with the following desktop browsers and their mobile equivalents:
  - Microsoft Edge (Chromium Engine)
  - Google Chrome
  - Apple Safari
  - Mozilla Firefox

Avenu agrees that all web portals should be tested for fully compatibility with the following desktop browsers and their mobile equivalents: Microsoft Edge (Chromium Engine), Google Chrome, Apple Safari, and Mozilla Firefox.

3.2.5. Upon request, the Vendor hosting any data belonging to the STO, must export and return the data in a commonly used format, at no additional cost to the STO within 30 days.

Avenu agrees that, upon written request from the STO, any data belonging to the STO will be exported and returned in a commonly used format at no additional cost to the STO within 30 days.

3.2.6. Vendor shall provide the STO their most recent SOC 2 (Type II) compliance reports, as well as any relative penetration testing reports on the minimum of an annual basis.

Avenu holds itself to the highest standards and controls to ensure best practices and adherence to all client obligations. Established control objectives are evaluated and audited as part of the annual SOC1 and SOC2 reviews. No exceptions have been identified and the most recent confidential copy of this is included under Exhibit 6 CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE. Avenu is audit compliant and our most recent SOC report covers the period of January 01, 2022, to September 30, 2022. Avenu is currently changing our audit period to include a full twelvementh period and the 2023 reports are expected to be available by the end of the third quarter for dissemination. Avenu also agrees to provide the STO with annual reports as required by the STO as needed.

In addition, Avenu holds our partners to the same high standards as ourselves and as our client's key data resides with BNY Mellon's NEXEN® system, Avenu reviews their SOC reports annually, which can be supplied upon request.

Avenu has established stringent quality controls throughout every process which includes but is not limited to the initial hiring of our employees, our code of ethics, the establishment of procedures and controls for all transactions and execution including authorized signer lists. Avenu's annual third-party compliance examinations include SOC1 and SOC2 audits and monthly meetings with sub-contractors to ensure processes, procedures and service level agreements are met. Avenu routinely evaluates all procedures and controls to ensure that we are following regulatory rules and industry best practices to provide the highest level of service to our states.

Below are just a few additional examples.

Procedural Integrity: Avenu has quality controls throughout every process to ensure that all postings are accurate and that all receipts, exchanges, transfers, cash movements, income postings and liquidations are properly executed for our



clients. This starts with our focus on ensuring proper authorization from our clients. As part of our focus on security and controls, we require every client to complete an authorized signer list including signature examples and dollar limits for any individuals authorized to initiate transactions. These lists have been incorporated into daily procedures and are reviewed and updated periodically throughout the year as needed. Documented and client specific procedures and controls have also been developed and are reviewed periodically to ensure adherence to policies and to ensure no changes or updates are required.

Employment Requirements: Prior to hiring any employee, Avenu performs a number of steps including conducting a thorough background check to ensure that only the best people are hired. Avenu enforces strict levels of security policies and consistently monitors adherence to those policies. Avenu requires all employees to complete annual security, privacy awareness and ethics training as a condition for employment, and unannounced tests are run parodically to assess compliance and remind employees of the importance of vigilance. All are also required to execute a Trade Secret and Confidentiality Agreement.

This agreement reinforces to employees the confidential nature of information encountered in the course of their work and advises them that any breach of confidentiality could subject them to civil and/or criminal prosecution. Additionally, any employee who divulges confidential information is subject to disciplinary action and termination of employment.

Segregation of Duties: Avenu segregates the duties of our staff to reduce the opportunities for any person or group to be in the position to perpetrate and conceal errors or irregularities in the normal course of an employee's duties. For each transaction type, our system has been developed to allow one person to enter the transaction and then requires a second individual to confirm the transaction. That second individual reviews the authorized instructions received from the state client to ensure that the transaction matches the original request. Liquidation requests and wire transfer requests receive an additional level of review and approval by a manager. Backup staffing is assigned for instances in which personnel are out of the office, so that at all times, transactions can be processed and verified.

All trade requests, including transfers, deliveries, and receipts, are monitored by a manager. Management additionally performs periodic audit checks on requests from states to monitor that Avenu is meeting its deadlines and accuracy requirements, as well as for regular audit purposes.

Assets and Records Access Safeguards: Only those individuals specifically authorized by the STO will have access to the systems with their own unique ID and password. Only individuals specifically authorized by Avenu and monitored by management have access to assets and records. The Authorized signers list provides proper confirmation and authorization of requested transactions and activities. The STO's personnel assign the individuals that may request each transaction type, and Avenu similarly assigns authorized individuals to execute those transaction requests. This authorization is changed when there is personnel turnover in either office and is reviewed annually or upon request as needed to ensure everything is always up to date.

Document Retention: Avenu maintains all documents and records to provide a proper audit trail. Avenu has documentation for individuals authorized by the states to request transactions on behalf of that STO as well as signature copies of all requests. Avenu can, at any time, pull a report of the individual who has requested transactions and periodically does so as part of testing our audit procedures to review the accuracy and authenticity of requests.

Avenu maintains each of our client's monthly statements onsite, which includes both a statement of transactions as well as lists of assets. Avenu will periodically compare these documents with the STO's requests that are received such as transfers, deliveries, receipts as well as research requests to properly maintain and review audit records which provides a proper audit trail to ensure that the appropriate documentation is being maintained.

3.2.7. Vendor must meet all currently applicable Payment Card Industry Data Security Standards (PCI DSS) security requirements and any updates thereto, all as reflected at poisecuritystandards.org.

Payment Card Industry Data Security currently does not apply to the requirements set forth in this RFQ. However, if needed in the future, Avenu acknowledges the requirement.

3.2.8. Vendor must meet all currently applicable National Automated Clearing House Association (NACHA) security requirements and any updates thereto, all as reflected at nacha.org.



National Automated Clearing House Association security requirements currently do not apply to the requirements set forth in this RFQ. However, if needed in the future, Avenu acknowledges the requirement.

3.2.9. Vendor must encrypt all of the STO's data at rest. This includes, but is not limited to, files exchanged via SFTP (PGP), SQL servers must support the use of TDE (transparent data encryption) and any file shares inside the vendor's network that contain the STO's data, must be encrypted at rest.

Avenu acknowledges and agrees to this requirement.

3.2.10. Vendor shall host the STO's data inside the continental United States of America only and must remain in the continental United States of America for the term of the contract. No overseas hosting is allowed for any component including, but not limited to, servers, infrastructure, or data storage repositories.

Avenu does not store data outside the Contiguous United States. Our custodial bank, the Bank of New York Mellon, operates as a global company with locations across the globe. That scope of operations is a major advantage to the STO as it provides access to many securities exchange markets around the world. BNY Mellon's data center for its business groups is located in Tennessee. However, it also has back up support for these U.S. facilities at overseas data centers. The basic structure is set out below:

Tennessee Processing Center (TPC) – located in Tennessee, U.S; this data center hosts BNY Mellon mainframe and distributed systems, voice, network, data storage, and information security services. This data center is the primary data center for BNY Mellon business groups.

**TN**2 Data Cente**r** (**TN**2) – located in Tennessee, U.S.; 26 miles from the TPC facility and enables BNY Mellon to utilize a datacenter for a synchronous replication solution for critical applications that have specific point of failure recovery requirements with very short data loss tolerance levels. This data center hosts the disaster recovery/failover services for BNY Mellon business groups.

QV**S** Data Center – located in the U.K; this data center acts as a resilient backup site for the Working Data Center – also located in the U.K. This data center hosts BNY Mellon EMEA distributed systems, voice, network, data storage, and information security services and is the primary data center for EMEA business groups.

The physical access controls to the BNY Mellon server rooms are owned and administered by BNY Mellon. Access control (such as iris scan and card access) and CCTV at the BNYM server rooms are owned and maintained by BNY Mellon. BNY Mellon maintains on-site security 24/7 that monitors the security systems at the location. Redundant monitoring of TN@ is also performed by the security officers located at the TPC data center. The Security Command Center in New York City also has monitoring capabilities as required. CCTV at the BNYM server rooms is monitored by BNY Mellon at the Security Command Center in London. Access to the data centers in the U.S. is restricted utilizing multi-factor authentication. Entrants must utilize their BNY Mellon – issued electronic access ID card as their first factor authentication with second authentication being an iris scanning reader to gain access to the facility. Access to the U.K. data centers is restricted via BNY Mellon-issued electronic access ID cards. Points of entry to the facilities are visually monitored by uniformed security personnel 24 hours a day, 7 days a week. CCTV surveillance is installed throughout the facilities and is monitored by security personnel. CCTV recordings are archived for a predefined number of days for both common and restricted areas through the data centers. Alarm systems are equipped throughout the facilities so that external data center entry points are protected from unauthorized entry.

Data centers have fire alarms and fire suppression systems. Fire alarm and suppression systems are tested annually. Raised floors are used throughout critical data center areas to help protect equipment from water damage, in addition to providing a cooling plenum and space for wiring.

Surge protectors, uninterrupted power supplies and generators are installed to protect data center equipment from power surges and power losses. Transient voltage surge suppressor (TVSS) and uninterrupted power supply (UPS) systems are installed to provide power sag/surge protection. Dual utility power services that back up each other along with backup diesel generators provide alternate power sources in the event of a utility power service loss. These systems are periodically tested, exercised, and maintained under third-party manufacturer maintenance agreements. Data centers are also equipped with Heating Ventilation and Air Conditioning (HVAC) units mechanical cooling systems to maintain a constant proper temperature and humidity levels. These systems are monitored through the Building Management System (BMS), which triggers an alarm when the temperature or humidity level goes outside the predefined limits. Regular preventative maintenance is performed in accordance with manufacturer recommendations.



As Avenu, BNY Mellon recognizes that the security, integrity, and uninterrupted delivery of data are essential and therefore, have developed a comprehensive, global, risk-based policies and standards for the control, processing, storage, transmission, and communication of its information. This policy and standards framework represents their corporate Information Protection Policies and Standards grouped by three major categories: Data Management, Third-Party Management and Technology; all which are reviewed on a periodic basis and evaluated by internal and external auditors as well as by various regulatory agencies. The below summarizes each:

#### Data Management:

- Information Protection
- Information Privacy
- Information Classification
- Electronic Communication
- Transport and Storage of Physical Media
- Classification and Handling
- · Records Management
- Information Erasure and Destruction
- Data Retention
- Clear Desk

#### Third-Party Management:

• Third-Party Management

#### Technology:

- Vulnerability Management
- Cryptography
- Configuration Management
- Technology Enterprise Change
- Privileged User Administration
- Network Security
- Information Security Incident
- Access Authorization & Certification
- Firewall
- User Developed Technology
- Anti-Malware

#### 3.3 DISASTER RECOVERY AVAILABILITY

3.3.1. The Vendor must maintain a provide a Discovery Recovery (DR) policy to the STO. A copy of the disaster recovery policy should be submitted with Vendor's bid.

Avenu has provided a copy of our DR Policy ("Disaster Recovery") for inspection by STO under Exhibit 8 CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE.

3.3.2. The Vendor must maintain a Discovery Recovery (DR) plan. Please provide a description of the Vendor's disaster recovery plan as it affects unclaimed property custodial property, including securities.

In the event of an incident that could disrupt clients, employees, or suppliers, Avenu responds with comprehensive business continuity plans. These plans are designed to minimize adverse impacts. They are well documented, communicated and tested. The plans describe procedures to be performed in the event of different disasters that could affect Avenu and our data centers. The plan provides for the identification of threats and/or disaster, notification of data center response team, damage assessment procedures, disaster response procedures recovery procedures and responsibilities as well as contingency planning and recovery. In the event of a disaster, our Incident Management Team (IMT) is responsible for managing communications, directing response and recovery activities, monitoring the recovery, and providing or reallocating resources. Avenu maintains Disaster Recovery Plans for its Data Centers in all locations. Back-ups and recovery plans are in place for the servers and all user laptops that supports Avenu's custody solution and have been tested.



Key client data is held on the BNY Mellon NEXEN® system which is subject to extensive federally regulated disaster planning and testing. They are committed to providing uninterrupted delivery of products and services to their clients. BNY Mellon conducts DR exercises annually and on a regular basis throughout the year to ensure they are prepared to maintain availability and processing. This testing includes both targeted and large-scale internal tests, as well as participation in global forums and sector exercises. Avenu regularly reviews the plan and testing to ensure compliance. An overview of BNY Mellon's disaster recovery is included under Exhibit 8 CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE.

3.3.3. The Vendor must maintain and provide a Business Continuance (BC) plan to the STO. A copy of the business continuance plan should be submitted with the Vendor's bid.

Avenu's BCP has been developed to plan for, respond to and recover from business interruptions, with a view to minimizing the impact of disruptions and facilitating service continuity within recovery time objectives and based on the prioritization of business objectives and operations. Our Business Continuity Plan includes items such as Emergency Incident Procedures, a Site Strategy Summary, Designated Incident Managers, Event Notification Procedures, Return to Site Procedures, Testing Procedures and Checklists for Disaster Assessment, Service Disruption details, and Business Resumption Safety and Procedures.

Avenu's sub-contractors are also held to high standards with regards to internal and external controls. As mentioned, our client's key data is held on the BNY Mellon NEXEN® system and therefore, it is imperative to us that their plans are considered top tier. BNY Mellon's Business Continuity Program (BCP) is based on industry-standard FFIEC guidance and follows best-practice recommendations from the Business Continuity Institute, the ISO standards and other finance and securities industry and regulatory bodies in Europe, the US and APAC. Being of the same mind set, their BCP is designed to plan for, respond to, and recover from business interruptions, with a view to minimizing the impact of disruptions and facilitating service continuity within recovery time objectives and based on prioritization of business objectives and operations. Their all-hazards approach considers diverse event scenarios, including application failures, natural disasters, civil disruptions, and severe weather as well as extreme situations, such as significant technology disruptions due to cyberattacks and staff loss due to pandemics.

- Loss or unavailability of systems: Each application has a business continuity plan.
- Wide-scale disruption / catastrophic event: Planning for events such as pandemics employs assumptions and strategies are based on the stages and trigger levels as identified by the World Health Organization Pandemic Alert system and in accordance with the US Centers for Disease Control guidelines.
- Loss or unavailability of third party: Each plan has documented recovery strategies for the loss of key third
  parties, with alternate providers identified where possible.
- Loss or unavailability of internet Disruption to infrastructure: The cybersecurity recovery plan documents the
  processes and procedures for recovering and restoring capabilities or services impaired as a result of malware,
  distributive denial of service (DDoS), or other events.

Several approaches to mitigate the disruption risk/impact of any incidents exist.

- Redundancy between their primary data centers, within their data center infrastructure (servers, networks, power), and within our applications.
- Geographic diversification of operational teams with an ability to fail over operations.
- · Alternate sites, remote work capabilities, and cross-regional recovery to transfer work among multiple locations

To support data recovery during a disaster recovery event, their primary production data center is continuously replicated to one of two backup data centers. The replicated data is validated during the quarterly exercises. BNY Mellon contingency data centers are dedicated facilities controlled and supported by BNY Mellon staff and management. These data centers are configured to operate indefinitely at 100% of the production data center's capacity and have computer operations command centers and crisis situation event rooms.

BNY Mellon leverages its diverse global footprint and operates proprietary hot sites across multiple locations around the world. U.S. data centers are configured as a combination of active-active and hot and warm stand-by, depending on the system architecture and service criticality. All servers and peripherals are available for use at the contingency data centers should a failover from the primary data center be required. BNY Mellon's Business Continuity Overview is included under Exhibit 7 CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE.



Raymond James Associates is registered as a broker-dealer with the Securities and Exchange Commission. RJA is a member of the New York Stock Exchange, FINRA, and all major exchanges. As such, RJA is required by rule to create business contingency plans in the event a disaster disrupts the firm's ability to do business.

In response to this rule made by the regulatory organizations, RJA has created contingency plans to address any such interruption of its business.

3.3.4. The Vendor shall maintain nightly backups of data, virtual machines and provide evidence of restoration testing.

Daily back-ups are made of all pertinent information, with copies stored both on and off site. Avenu maintains Disaster Recovery Plans for its Data Centers in all locations. Back-ups and recovery plans are in place for the servers and all user laptops that support Avenu's custody solution and have been tested. Key STO data is held on the BNYM NEXEN system which is subject to extensive federally regulated disaster planning and testing. BNY Mellon conducts DR exercises annually and on a regular basis throughout the year to ensure they are prepared to maintain availability and processing. This testing includes both targeted and large-scale internal tests, as well as participation in global forums and sector exercises. Certification can be provided if selected.

3.3.5. The Vendor's infrastructure and application shall maintain a 99.95% uptime, calculated monthly.

Avenu acknowledges and agrees that it meets the requirement.

#### 3.4 PERSONALLY IDENTIFIABLE INFORMATION

- 3.4.1. Personally Identifiable Information (PU) refers to any information that can be used to identify an individual, including but not limited to, name, address, telephone number, email address, social security number, financial account information, and health Information. The Vendor acknowledges while providing services under this agreement, it may have access to PII.
  - The Vendor shall use PII only for the purposes of providing services under this agreement.
  - The Vendor shall not disclose PII to any third party without the prior written consent of the State.
  - The Vendor shall implement appropriate technical organizational measures to protect PII against unauthorized or unlawful process and against accidental loss, destruction, or damage.

Avenu understands the high sensitivity of information delivered to and retained by the STO, such as social security numbers, account numbers, addresses and other personal information listed in unclaimed property reports and state records. Avenu has developed and implemented strict policies and procedures regarding the protection of client data and has dedicated staff monitoring and testing systems and operations to ensure that both client and Avenu data is always protected and secure.

Avenu follows the voluntary NIST Cybersecurity Framework (CSF), which we track in our ServiceNow Platform. Additionally, Avenu has contracted with a third-party vendor to perform ongoing NIST CSF updates on a quarterly basis to measure progress and increased maturity.

Technology and Security Deployments:

Avenu's Solution provides:

- ▶ State of the art EndPoint Security to all our servers and workstations. We use an industry leading Endpoint Detection and Response (EDR) solution that recently received the highest rated vendor in the Gartner 2020 EDR 'Voice of the customer' report.
- Industry leading Enterprise Email Security solution which consistently ranks in the top right (Leader's) Gartner Magic Quadrant.
- ▶ Industry leading Security Awareness solution, which is world's largest security training platform and consistently places in the top right (Leader's) Gartner Magic Quadrant.
- ▶ Industry leading firewalls at the perimeters, with threat prevention, URL filtering and malware detection.
- ▶ Multi-factor authentication (MFA) for applications.
- ▶ Log Management and Analytics solution with SIEM (Security Information and Event Management).



- Avenu is currently rolling out a next generation remote access solution and a secure internet access solution, which will further reduce the attack surface. The solution provides the best of breed Secure Access Service Edge (SASE) security stack in the industry.
- ▶ Avenu is contracted with GuidePoint Security, an award-winning cybersecurity solutions leader, who has helped us develop the following formal security programs:
  - Vulnerability Management Program. Scheduled vulnerability scanning will be performed utilizing an industry leading solution, and any discovered vulnerabilities will be managed in our ServiceNow platform until they have been mitigated
  - Security Risk Management Framework
  - · Security Awareness Program
  - Security Incident Response Plan
  - Data Security Assessment
  - Firewall Assessment
  - Identity and Access Management (IAM) Program
  - Third Party Risk Management Program

Avenu has also adopted many security policies which are considered proprietary and confidential information. Some examples listed below:

- Avenu Privacy Policy
- Avenu Information Security Program Policy
- Avenu Software Development Lifecycle (SDLC) and Application Development Security Policy
- Avenu Information Security Risk Management Policy
- Avenu Information Security Incident Response Policy
- Avenu Change Management Policy
- Avenu Remote Network Connection Security Policy
- Avenu Access Control Policy
- Avenu Network Security and Firewall Policy
- Avenu System Security and Build Policy
- Avenu Email and Social Media Security Policy
- Avenu Acceptable Use Policy
- Avenu Data Classification and Management Policy
- Avenu Information Security Data Retention and Destruction Policy
- Avenu Information Third-Party Risk Management Policy
- Avenu Mobile Device Security Policy
- Avenu Physical and Environmental Security Policy
- Avenu Personnel Security Policy
- Avenu Security Logging and Monitoring Policy
- Avenu Security Awareness and Training Policy.
- Avenu Vulnerability and Patch Management Policy
- Avenu Information Encryption and Key Management Policy

As the State of West Virginia's assets reside within BNY Mellon's NEXEN platform and as the leader in the custody industry, our partner also takes cybersecurity very seriously. Their approach is a multi-layered control infrastructure with built in redundancies and checks which leverage threat intelligence capabilities, monitors the enterprise for vulnerabilities and collaborates across business units, technology, risk, compliance, and internal audit.

BNYMellon maintains strong internal controls, including policies and standards which are regularly reviewed as regulatory requirements, guidelines, and technologies change. Their program is also benchmarked against ISO 27001/2 and the NIST Cybersecurity Framework and they also report on cybersecurity risk with various internal risk governance committees, including the Board of Directors. BNY Mellon's approach also focuses on:

▶ Network Protection: They separate their own computing environments from publicly accessible environments and use "defense in depth" where multiple layers of security controls are placed throughout creating deliberate redundancy.



- ▶ Information Protection: BNY Mellon has implemented a series of Data Loss Prevention (DLP) controls designed to detect and prevent the intentional or unintentional movement of data outside of BNY Mellon and all information assets are subject to the company's information protection policies and standards.
- ▶ Vulnerability Detection: Teams are constantly monitoring and scanning the environment for potential threats.
- ► Third-Party Risk Management: They operate an end-to-end third-party risk management program and escalation process to onboard, monitor and assess information risk associated with third-party providers.
- ► Cybersecurity Threat Intelligence: BNY Mellon regularly receive information on potential cybersecurity threats from diverse sources including our peers, the broader financial services industry, law enforcement, government, and a variety of other public and private sources, as well as third-party threat intelligence vendors.
- ▶ Cybersecurity Resiliency Exercises: They conduct internal cybersecurity resiliency exercises based on various hypothetical attack/outage scenarios to help raise awareness, evaluate resiliency, assess communication protocols, and test alternative procedures. In addition, we participate in industry-led exercises to help coordinate responses to significant cybersecurity incidents.
- ► Training and awareness: Like Avenu, they perform annual information refresher training and conduct awareness campaigns for staff.
  - 3.4.2. In the event of a breach or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to PII, the Vendor shall promptly notify the State and cooperate fully with the State's Privacy Office investigating of such breach and its efforts to mitigate the effects of such breach. A full incident report shall be provided to the State, fully supplying all the technical details, remediation efforts and resolution to the issue.

Avenu acknowledges and to the extent commercially possible, will notify and report to the STO any incident pertaining to a Data Security Breach.

3.4.3. Upon termination of this Agreement for any reason, the Vendor shall return all PII, certify in writing to the State that it has done so and provide evidence of its destruction.

Avenu acknowledges this requirement and will return PII as required and/or certify in writing destruction of PII.

3.5. Vendor shall be or shall contract with a financial institution insured by the Federal Deposit Insurance Corporation (FDIC).

Acknowledged. BNY Mellon, our partner, is insured by the Federal Deposit Insurance Corporation (FDIC).

3.6. Vendor shall be a member or contract with a member of the Securities Investor Protection Corporation.

Acknowledged. Through our partnership with BNY Mellon and Raymond James, we are a member of the Securities Investor Protection Corporation

3.7. Vendor shall be a member or contract with a member of the National Association of Security Dealers.

Acknowledged. Through our partnership with BNY Mellon and Raymond James, we are a member of the National Association of Security Dealers.

3.7. Vendor shall be a member or contract with a member of the NYSE, the NASDAQ and the Depository Trust Corporation.

Acknowledged. Through our partnership with Raymond James Financial Inc. and BNY Mellon, we are a member of all principal stock exchanges including New York, American, NASDAQ and OTC and trade/execute sales on all of these exchanges on behalf of our unclaimed securities custody clients – including the STO. In addition, BNY Mellon trades on over 100 global markets which are critical for the maintenance and sale of unclaimed securities. Raymond James Financial Inc. will provide services for sale of securities at the request of the STO.

3.9. Vendor shall be or shall contract with a brokerage firm that is in compliance with the **SEC**'s Customer Protection Rule and **N**et Capital Rule.

Acknowledged. Raymond James, our partner, is in compliance with the SEC's Customer Protection Rule and Net Capital Rule.



3.10. Vendor shall have at least five (5) years of continuous operation in providing unclaimed securities custodial services to at least five (5) state unclaimed property divisions. To the extent that Vendor contracts with another entity to provide specified services, that entity shall also have five (5) years of experience in providing unclaimed property securities-related services.

For perspective, Avenu's custody solution has been developed and enhanced over a period of almost four decades, and as a leader in the industry with 29 states and territories, we have developed ways to streamline processes and solve complex issues our clients face as the administrators of unclaimed securities. Far from being a one-size-fits-all service provider, Avenu, in collaboration with our partners of over eighteen years, Raymond James and Bank of New York Mellon, delivers tailored flexibility and customization essential for STO operations. We go beyond the norm, offering unique services often overlooked by competitors, such as maintaining physical certificates on your behalf, handling of voluntary corporate actions and class actions on your behalf, direct liaison with holders and owners, and agile adaptability to swiftly alter processes and reports as needed.

Since 1984, Avenu has been the trusted partner in safeguarding states' unclaimed securities portfolios, innovatively crafting end-to-end solutions. Our Unclaimed Property Solutions team is fully committed to addressing every facet of unclaimed property management, from seamless system and process management to secure securities custody. Avenu does not just deliver solutions—we redefine them.

3.11. Vendor shall be authorized to conduct business in the State of West Virginia at the time of intent to award, and during the term of the contract, including any renewals or extensions that may be granted. All assets and data relating to the STO shall be maintained in a facility located within the continental United States of America. Provide the address of the physical location of the facility from which the Services will be provided, and the nature of all business conducted from that facility.

Avenu is authorized to conduct business in the State of West Virginia. Avenu Insights & Analytics, LLC, ("Avenu") is a Delaware company with its headquarters located at 5860 Trinity Parkway, Suite 120, Centreville, VA 20120.

Avenu's website can be found at: https://www.avenuinsights.com.

The legal entity submitting this proposal and entering into any subsequent contract is Avenu SLS Holdings, LLC. The principal place of business for any work arising from the RFQ is:

Avenu SLS Holdings, LLC 100 Hancock Street, 10th Floor Quincy, MA 02171 617.371.9900 (p) 617.722.9665 (f)

All other business conducted at the Quincy office relates to Avenu's unclaimed property compliance or administrative support work and the STO's housing of data is explained more fully in 3.2.10.

3.12. If Vendor is a financial institution, it must not be included within the restricted financial institution list and disqualified from the competitive bidding process as outlined in West Virginia Code \$12-1C-1, et. seq. To learn more about this list and other information, Vendor should visit the following link: https://wvtreasury.com/Restricted-Financial-Institutions.

Avenu acknowledges meets this requirement. Avenu and its key service delivery partners, (the Bank of New York Mellon and Raymond James), unlike *Wells Fargo, Blackrock Inc., JPMorgan Chase & Co., Goldman Sachs Group, Inc., and Morgan Stanley*, are not on the West Virginia State Treasurer's Restricted Financial Institution List. We are headquartered in Centreville, Virginia, and, with the banking and brokerage expertise of our key partners, are prepared to provide best-in-class unclaimed security management services to the State of West Virginia State Treasurer's Office ("STO") for the duration of the term set out in the Solicitation.

3.13. Vendor shall agree not to engage in boycott of energy companies for the duration of the contract.

Avenu acknowledges this requirement.



#### **4 MANDATORY REQUIREMENTS**

## 4.1 MANDATORY CONTRACT SERVICES REQUIREMENTS AND DELIVERABLES

Contract Services must meet or exceed the mandatory requirements listed below. By signing and submitting its bid, Vendor certifies that it will provide the Contract Services required and Vendor meets or exceeds all mandatory requirements.

Avenu acknowledges that it meets or exceeds all the mandatory requirements required in this RFQ. We have provided a complete response to all of the mandatory requirements in the RFQ. We agree to the Contract Services Requirements and Deliverables and will provide any additional information or documents as needed or required.

#### 4.2 DELIVERABLES

Facilitate and simplify the delivery and collection of reported unclaimed securities:

4.2.1 Open, maintain and close accounts as directed by the STO. Initially, Vendor shall maintain one (1) separate custody account in the name of the West Virginia State Treasurer. If necessary, the Vendor shall also maintain separate accounts and/or sub-accounts for Unclaimed Property as may be requested by the STO if the primary custody account is unable to provide all detailed segregation, or if the STO requests such additional account.

As a current client, we have an account established in the STO's name for use solely by the STO and Avenu on its behalf. Avenu receives and accounts for cash and securities via DTC, DWAC, DRS, certificate, mutual fund, or any other form in the established account. The established segregated securities custody, brokerage, and cash account on behalf of the STO has a unique account number and account name, into which all securities received from holders, or the State are deposited and maintained in this account. All activities occurring therein and all related procedures, are referenced and detailed throughout this RFQ.

Avenu can and will open a separate or sub-account for the STO, but additional charges will apply as we are charged for each account as well. We can work with the STO to identify the reason an additional account may be required then develop and discuss alternative solutions to address the need. During the entire time we have been supporting states with securities custodial services, we have not been required to establish other accounts as the way in which we have organized the accounts and securities provides all of the requirements by all of our clients. We will be happy to discuss the requirements with the STO and establish an additional or sub-account if required.

4.2.2 Receive and safely hold assets delivered to it by the STO, by audit vendors of the STO, and by businesses reporting unclaimed property. Vendor must receive and hold securities in the name of the STO, the Vendor or others, all as directed by the STO, using the same care in the physical custody thereof as in the case of other assets held by it in a fiduciary capacity.

Avenu acquires securities on behalf of the STO whenever holders, transfer agents, private companies and other entities deliver to us based on instructions and guidelines provided by the STO's holder reporting Instructions. Securities can additionally be acquired through corporate actions and reinvested dividends. Avenu has established and will continue to maintain a segregated securities custody, brokerage, and cash account on behalf of the STO with a unique account number into which all securities received from holders or directly from the STO are deposited and then maintained.

As Avenu is presently providing all the services in this RFQ to the State, the existing securities would remain in the STO's current account and Avenu will continue to deposit all newly received negotiable shares received into the same custodial account and based upon your specifications.

Avenu continues to anticipate receiving securities via DTC, DWAC, DRS or certificate form (in the name of the STO, in the assigned nominee name, in the street name and owner's name) when certificates are delivered, however, we work to



ensure that all positions are deposited to DTC whenever possible for easy maintenance and transfer/liquidation processing.

Service details by type are set out below.

#### Depository Trust Company (DTC)

Avenu strongly advises receipt of securities through DTC with our reporting instructions. Our team will continue to assist the State to ensure that the holder reporting instructions are easy for all to follow. Using our extensive experience in unclaimed property matters and sharing language improvements we see at other clients; we can help improve the accuracy of holder reporting. This in turn reduces the amount of time required by the State's staff to have to follow up on pending receipts for outstanding reports.

Avenu staff can and will coordinate directly with many holders on behalf of the STO to resolve any reporting errors when necessary. Additionally, our experienced account manager will follow up as needed with the delivering holder to make sure that all property reported and presented for delivery into the State's account is received. Avenu credits the positions to your account immediately upon receipt of the property where you can then view the position using NEXEN®, our online reporting tool further described in this RFQ. Avenu Reports from NEXEN® are included under Exhibit 5.

#### Direct Registration Shares (DRS)

Another advantage of our customized unclaimed securities solution is the automated way in which we process Direct Registration Shares/Book Entry (DRS) positions. A key differentiator is the receipt of these positions electronically when agents refuse or do not have the capability to transfer the positions via DTC. Most other custodians process these statements manually or not at all.

With Avenu, the positions are processed by moving these positions off the books of the transfer agent and crediting the State's account. This happens within 48 hours of the transfer agent's approval.

Our unique DRS service level works because:

- ► Holders and their agents prefer delivering securities property in the form of DRS shares because it is less costly for them.
- ▶ Other custodians can require that DRS statements and mutual funds be processed by the states manually. Manual processes cause extra work for clients with the required tracking of reported, splits and spin-off shares; receiving physical checks with no knowledge of their relation to reported property; or even responding to due-diligence notifications for previously reported property that is about to be re-escheated due to inactivity.
- ▶ Avenu, upon receipt of a DRS holding statement, reviews and initiates a receipt transaction in which the DRS shares are deposited into the State's account.

This process allows the position to be settled at DTC within 48 hours of transfer agent's approval and reflected in your account. Occasionally, your dedicated account manager is able to coordinate with the transfer agent and have the position deposited into the account within 24 hours. We are able to initiate requests quickly using the DRS (Direct Registration System) which is a file transfer process developed through the Depository Trust Company to assist its participants with transferring shares from accounts held on the books of the transfer agent to the customer's account with the participant. The process has the custodian/DTC participant input a transaction into the DRS file using key fields such as cusip, number of shares, registration of account and the transfer agent account number. This information is gathered daily from all participants and collected on a file. The file is transmitted to the relevant transfer agents and barring any errors/rejections the account is debited the number of shares requested and the participant position is credited. The shares are held in custody within the participant number at DTC.

- ▶ Once DRS shares are received into the account, you are able to view on-line, monitor and track via NEXEN®, run reports and initiate transfers or liquidations unlike if the position remained directly at the transfer agent on your behalf.
- ▶ In the event that the STO receives a report for shares and is unable to find a certificate or DRS statement and the position is not reflected in the account; staff need only to contact their Avenu account manager to obtain the shares. Avenu custody consultants, account managers and other custody staff have multiple contacts with different holders and transfer agents and typically need only the CUSIP and share amount in question to identify and obtain reported shares on behalf of the STO.



- ▶ Also, any time Avenu receives a check (i.e., dividends, cash in lieu of fractions, etc.) for which no corresponding shares can be found in the account, Avenu will pro-actively follow up with the transfer agent to find out what the check is for and recover any corresponding shares, if applicable. This significantly reduces the time required for your staff to research, determine the funds that were/were not received, the reason, and then request from the agent when reconciling.
- ▶ All of the receipt and deposit activities as described in this section are comprehensively tracked, recorded, and made available to the STO in multiple reporting formats.
- ▶ Our specialized DRS services are a good example of the thought, support, and innovation that Avenu delivers as part of its unclaimed securities solution and that differentiate Avenu from other providers.

#### Deposit Withdrawal at Custodian (DWAC)

Avenu will process transactions via Deposit Withdrawal at Custodian (DWAC) as needed upon receiving authorized instructions. Avenu will coordinate with transfer agents any DWAC transactions for trades that are coming into the account and/or leaving the account for any transfer needed to owners.

#### National Securities Clearing Corporation (NSCC)

Avenu will accept, maintain, and deliver all securities eligible for the National Securities Clearing Corporation (NSCC) process. This includes equities, corporate and municipal debt, American depositary receipts, exchange-traded funds, mutual funds, and unit investment trusts.

#### Automated Customer Account Transfer Service (ACATS)

Avenu will process and coordinate transactions via Automated Customer Account Transfer Service (ACATS) for the STO as needed upon receiving authorized instructions from the STO.

#### Physical Securities

Although the number of physical securities in the market has decreased, Avenu continues to expect to receive some physical certificates on behalf of our clients just due to the nature of unclaimed property. Because of the amount of work and documentation involved with these types of securities, many shy away from providing this service.

Many certificates require legal documentation or paperwork to make them negotiable and eligible for deposit to DTC. When documentation is needed, Avenu will work with the STO to obtain the required stock powers and letters of incumbency needed for each certificate, knowing that the process can be time consuming for the STO alone to complete and obtain signatures. Avenu suggests that in the case where these documents are required, they be delivered under separate cover from the original instruments as anyone who is in receipt of both the original instrument and the supporting documentation may act with his or her own instructions as the bearer to deposit, transfer or liquidate the security. If certificates are received and Avenu is not in possession of the required paperwork to process an item for reregistration, the STO's account manager will advise the STO as to what paperwork is required. While Avenu awaits the receipt of the requested paperwork, the certificates will be deposited to the STO's account, maintained in the vault, and coded as such. For ease of use, Avenu requests that physical certificates be registered under Hare & Co, the nominee name for BNY Mellon. By using this nominee, Avenu eliminates the need for the STO to provide extra documentation, even signatures, and makes the deposit process much simpler and faster. For clarity of records, using Hare & Co as the nominee means that positions are not co-mingled or registered to a master custodian account for receipt and delivery into the STO's account.

For physicals, certificates are required to be forwarded to the BNY Mellon Vault for processing. All physical certificates are forwarded to the vault via secure/trackable mail. At the same time, the account manager sets up free receipts in the account to alert BNY of physical certificates delivery. When BNY receives physical certificates, they follow the required protocol to deposit the shares in the account or if possible, deposit the certificate to DTC. Depending on how the cert is registered, the deposit of certificates to DTC might require that the certificates be forwarded to the transfer agent for reregistration to Hare & Co (BNY's nominee name) to ensure certificate is valid. When the new certificate is received from the transfer agent – the shares are deposited to DTC. If there is a case where the transfer agent confiscates the certificate—the account manager will notify the STO with the details of the certificate and also with the confiscation notice.

#### Mutual Funds & Dividend Reinvestment Plans (DRPs)

Avenu's automated maintenance for Mutual Funds and Dividend Reinvestment Plans (DRPs) eliminates the processing of paper statements by the STO and ensures all mutual funds positions are properly maintained in the STO's account. Daily



reconciliations of accounts is done systematically by FundServe, the U.S. industry standard for processing and settling mutual fund and other pooled investment product transactions between fund companies and distributors.

Mutual Funds – Unlike other custodians, Avenu has agreements and contracts in place with many mutual fund companies. This allows us to handle these assets on behalf of our states. We establish omnibus receiving accounts to allow delivery of the securities. NEXEN® interfaces with the custody system (GSP) to acquire the balances and GSP balances are reconciled to the fund company. There is an internal system/database which stores all fund accounts established for each state which gets balanced by pulling the fund balance for the fund account number within that database and pulling the GSP balance. This would determine if there was a break between the fund account number established and GSP. The report is a file that is systematically generated and notifies operations of all NSCC transfers into our state accounts. Please also refer to Avenu Reports Exhibit 5 for an example of a Free Receive – Mutual funds report indicating this type of settlement.

**DRPs** – Reconciliations and account updates are done on a regular basis when account statements of this type are received in house by Avenu. When statements as well as checks for DRP positions are received in house, they are reviewed regularly and posted to the STO's account.

Regular reconciliations are performed throughout the year by Avenu on the mutual fund holdings in the STO's accounts. This added regime of reconciliations addresses the reality that some fund companies only forward confirmation statements semiannually while others provide only at year-end.

#### Foreign Securities

Avenu provides custody services for almost every foreign market through BNY Mellon's sub-custodian network and through the FX (Foreign Exchange) Program options.

In addition to the receipt and safekeeping of foreign securities, Avenu can automate trade processing and execution of foreign transactions. Most holders of foreign assets need only contact Avenu for appropriate foreign account details and agree on a trade date and settlement date. Once all trade decisions are exchanged and verified with the holder, Avenu will set up the trades on the Custody Platform for successful execution and settlement. If for any reason there is no account opened in a particular market, Avenu will work with BNY Mellon to open the account and process the trades for the STO. A listing of the current global markets in which we participate can be provided upon request.

As the STO's current provider, Avenu currently ensures the posting of all dividends, interest and other distributions to the account and provides the STO with full reporting and inquiry access via NEXEN®. The NEXEN® Reference Guide provided under Exhibit 3 shows additional details related to this reporting system. The principal identifier in this database is the security's CUSIP number.

After initial receipt of all security types, including certificates, Avenu tracks associated mergers, stock splits, spin offs, dividends, interest payments, etc., until the security is sold or claimed and transferred to an owner. Avenu systematically processes accrued income and corporate actions and ensures they are posted and settled. Receipts are reconciled at the end of each day to ensure the STO's account has been properly credited. All information related to all security types is available on NEXEN® as well as in the reports delivered in the required format. All records and reports are maintained online using NEXEN® and can be accessed immediately by the Administrator and all data is available for 24 months. For transactions older than 24 months, Avenu maintains copies that can be delivered upon request.

Avenu offers many types of reports that display the information requested by the STO. Examples are provided in Avenu Reports, Exhibit 5.

Avenu will also continue to monitor, process, and redeem all activity surrounding bond activity including collecting income payments for the STO as part of our daily account maintenance. Avenu redeems bonds at maturity, including coupons, and collects the proceeds as part of our normal procedures. These securities are constantly monitored to ensure that they are presented at the time of maturity so that the STO will be provided with the appropriate funds. All funds are posted to your account on the payable date and all income and principal balances are reconciled to ensure that your account has been properly credited.

4.2.3 Allow physical deposit of stock and commodity certificates.



Unlike many, Avenu understands that certificates still exist in the industry and Avenu will deposit all negotiable shares into the custodial account for the benefit of the STO, including those received in the form of a physical stock and commodity certificates. Please see 4.2.2 (Physical Securities) for additional information.

4.2.4 Accept Depository Trust & Clearing Corporation (DTCC) eligible securities and commodities, such as precious metals.

Avenu will accept all eligible securities to be deposited in the account through DTC as described in further details in section 4.2.2 and 4.2.3, preceding this section. Holding a Precious Metal Certificate would be treated like any other physical certificate and held in our DTC vault and Avenu confirms these types of certificates can be held. These certificates are a reflection/statement of something held in the vault of the precious metal dealer which is like holding a stock certificate reflecting a position at the transfer agent. Currently we do not offer an Unallocated Precious Metals service to hold the actual physical precious metals (i.e., gold bar). If physical items need to be held, a broker service could be used to maintain an account directly with a service provider. Precious Metal Services may be subject to specific fees.

4.2.5 Maintain the proper and current amount of shares of securities in the State's account, including but not limited to updating the accounts when actions, such as stock splits, reverse splits, mergers, consolidations, dividends paid and dividends reinvested, and other events, could affect the volume or value of the shares.

Avenu believes a true partner should focus on looking for ways to make our clients' lives easier and more efficient. We believe our handling of corporate actions does just that. Avenu currently provides all data concerning corporate actions, mergers, spin-offs, tenders, etc. and systematically monitors, collects, and reconciles dividend payments, interest payments, stock splits, tenders or other activities associated with reorganizations, voluntary or mandatory corporate actions on your behalf.

Avenu offers a unique process concerning all voluntary corporate actions. Avenu will notify the STO of voluntary corporate actions and place the information on our Extranet site to ensure that the STO can make an informed decision if standing instructions are not utilized. If standing instructions are not utilized, Avenu will act upon the STO's desire and process all paperwork needed to complete the action.

As part of our standard service, Avenu also monitors all class actions on behalf of the STO and automatically will ensure participation if eligible. Avenu believes that processing voluntary and class actions on our clients behalf is a standard service that should be provided to the STO. Please refer to Avenu Exhibit 5, Avenu Reports for an example of a Class Action Report that can be scheduled or sent to the STO on a regular basis. Please see below for a more in-depth process on both voluntary and non-voluntary actions.

#### Voluntary Corporate Actions Process and Controls

Voluntary corporate actions are any actions on which the STO (or owner) has a right to choose which option they would like to exercise. Unlike some custodians, Avenu will process these types of corporate actions on behalf of the STO. Avenu promptly notifies the STO of all voluntary corporate actions made by issuers of securities, including but not limited to offerings, exchanges, tenders, and consolidations, which are held in each account. The notification is posted to the Avenu Extranet site for an authorized STO representative to view and act upon. Further details related to the Extranet are provided under Avenu Exhibit 4, Extranet Reference Guide. Avenu provides all the necessary information for you to make an informed decision. Additionally, all voluntary (and mandatory) corporate action information is available to view on NEXEN®.

The Extranet provides a cutoff-date as to when an option needs to be chosen and communicated back to Avenu. Avenu will follow up to ensure that the options are understood, and an educated choice can be made. After choosing to take action on a given voluntary corporate action, you will receive confirmation of the response via email, and we will then enter the instructions as received and complete any necessary paperwork on your behalf to fulfill the action. Extranet and NEXEN® can both be used to view which voluntary corporate actions are pending, those which have expired, and the options previously chosen, as these files are maintained on the website for as long as you would like to see them. Avenu may operate on a standing instruction to take the 'default' option on all voluntary corporate actions if you so choose.

All postings can be viewed daily using NEXEN®. The complete description of all corporate action postings is part of the monthly reporting package, specifically the Custody Transaction History, to assist with any reconciliation. This report is available at the end of each month both online through NEXEN® and via monthly statements which are delivered to you



at the beginning of each month. Please refer to Avenu Reports Exhibit 5 for the report entitled Transaction Report PDF Format—Corporate Action Activity transactions for more information.

#### Mandatory Corporate Actions

Avenu tracks and processes all mandatory corporate actions made by issuers of securities which are held in Avenu's custody for the STO. Mandatory or involuntary Corporate Actions automatically post and settle to the STO's account. As with any settlements, all receipts are reconciled at the end of the day.

Avenu systematically processes and accounts for all corporate actions for items being held in the account regardless of the type of security (DTC, mutual fund, physical, etc.) for the STO. Actions on physicals may take slightly longer to process, as they must be mailed to the agents for any exchanges, etc. Any physical certificates received as the result of a stock split, distribution, etc., will automatically be deposited in the STO's account and held in our vault.

Avenu collects and records all dividends, interest, and cash from corporate actions such as exchanges and all other cash receipts and allocates the funds to the appropriate CUSIP numbers within the STO's account

Avenu also redeems bonds at maturity, including coupons, and collects the proceeds as part of our normal procedures. These securities are constantly monitored to ensure that they are presented at the time of maturity so that states will be provided with the appropriate funds. All funds are posted to your account on the payable date. All income and principal balances are reconciled daily to ensure that the account has been properly credited with the appropriate income. Avenu also collects and allocates all corporate restructuring activity for the STO such as stock splits, stock dividends, mergers, etc. Avenu processes and posts all corporate actions made by issuers of securities which are held under Avenu's custody on your behalf.

Avenu provides detailed information of all corporate actions that have transacted in the account. This information is available on NEXEN® as well as in the monthly reports delivered to you currently. Information such as the number of shares or units on which income is being paid, the record and payable date, income amount and market value of an asset may be viewed to assist with any reconcilements. The description of the corporate action is part of the transaction information to assist states with any reconciliation. These transactions are also included as part of the electronic submission and the standard monthly reporting package delivered to our clients.

Avenu collects all dividends and interest income and allocates all income to the appropriate CUSIP numbers within the STO's account. All income balances are reconciled daily to ensure that the STO's account has been properly credited with the appropriate income. All income will be posted to the account on the payable date. Cash transactions occurring within the account can be viewed at any time on NEXEN® and all relevant details are provided under Exhibit 5, Avenu Reports. Avenu will post physical income received for certificates that are being held in the vault. Depending upon the registration of these certificates, the physical checks would come directly to Avenu, and income would be posted, or the checks may be delivered to you if the registration address is that of the STO.

4.2.6 Maintain dedicated accounts for all mutual funds and securities in the name of the STO. STO assets shall not be held in an omnibus account or comingled with positions held by anyone other than the STO.

As mentioned, to account for all security and other positions including cash, Avenu has established segregated securities custody, brokerage, and cash accounts on behalf of the STO's Office with a unique account number and account name, into which all securities received from holders are deposited and maintained. "Segregated" in this context means that STO's assets are kept in a separate and unique account. Each state account has its own unique six-digit account number qualifier. All activities occurring therein, and all related procedures are referenced and detailed throughout this proposal. Mutual fund accounts also have unique fund account numbers specific to the STO by security/cusip. Avenu deposits all negotiable shares and cash received in the account into the custodial account for the benefit of the STO. The STO's accounts are reconciled on a daily basis to ensure that all income and principal is properly allocated and credited, and all securities transactions are settled properly, and wires are submitted as required upon request to the STO.

Avenu offers the ability for all sales proceeds, cash related to corporate activity, dividends, and interest to be swept daily into an interest-bearing account chosen by the STO. The money market fund, which is managed by Dreyfus Investors, only invests in securities which are Triple-A rated. The Dreyfus Corporation, established in 1951 and headquartered in New York City, is one of the nation's leading mutual fund companies. A copy of the Dreyfus Prospectus and fund



information is available upon request. The STO has access to this account at any time using our custody recordkeeping platform NEXEN®. NEXEN® is described throughout this proposal and additional detail is included as Exhibit 3, NEXEN® Reference Guide.

Avenu will ensure that all asset types are properly held in safekeeping, and that they are accurately settled and maintained on our system. The portfolio is available for on-line viewing or reporting at any time. We record each security received by CUSIP number, name of issue or security, number of shares, type of security, date received and the method of receipt. Recording and maintaining this information for each unique position ensures proper accounting and reconciliation.

4.2.7 Provide ongoing consulting, custodial and research services. At the request of the STO, Vendor shall conduct research on corporate actions such as mergers, name changes, discontinued corporations, etc. Such research is to be completed within 30 days of request, unless the STO approves the Vendor additional time in conducting extensive research, and/or entitlement calculations, beyond 30 days.

Avenu will provide ongoing consulting, custodial and research services. Avenu understands that many calculations on securities will be straightforward, accurately calculating the value or entitlement of shares received many years ago that have been liquidated and then claimed in the future could be difficult and time-consuming. Avenu provides research or calculations on securities to numerous clients and does have the experience and capabilities to provide these services to STO. Avenu has invested in and utilizes several databases and services which provide historical securities information as relying upon one database or resource can provide inaccurate results. Additionally, Avenu retains transaction history statements for all of its unclaimed securities custody clients that can be utilized to pull historical corporate action information. It is a combination of these resources that allows Avenu to have the most accurate historical information as depending upon one source does not typically provide accurate results.

Avenu currently provides investigative services for the purpose of researching unpublished and unknown items received by our unclaimed securities clients. We understand the unique nature of the types of securities that are reported to state unclaimed property programs and have developed procedures to research all securities that are submitted for deposit.

In addition to the functions of depositing the certificates reported to states, sometimes on a daily basis, Avenu has the ability to research older certificates that may be reported as safe deposit box contents or from a batch of older certificates that had not previously been researched.

All research is conducted within 30 days of request unless the request requires extensive research. If any request takes a longer period than typically required, we will inform the STO. Please refer to Avenu Reports Exhibit 5 for as example of an Entitlement Calculation.

4.2.8 Acquire securities, mutual funds, or other investment properties that are held by other investment brokers, transfer agents, or other accounts that should be in the **S**tate's account.

Avenu will acquire securities, mutual funds, and other investments that are held by other entities and should be held in the STO's account. Avenu conducts periodic reconciliations to determine if there are additional assets that should be in our client's accounts. We additionally will contact entities, at the request of the STO, or if we identify that they are holding securities that should be in the STO's account.

#### 4.2.9 Determine the valuation of securities it holds.

Avenu currently generates a monthly List of Assets Report of all securities held in the STO's account which includes the overall market value, the CUSIP, security name, number of units held, price per share and market value of all positions as of the close of business on the last day of the month. This report is delivered at the beginning of each month and may be generated at any time by the STO or Avenu on NEXEN® and in multiple formats.

Through our partner, BNY Mellon, we receive automated pricing feeds from numerous vendors daily and provide monthly accounting valuation statements. The month end prices are audited based on the standard pricing vendor.



After the elimination of extreme values, the remaining validated prices are used in the order of established vendor order for each security class. When a pricing vendor does not send a price for a particular asset, it may indicate an inactive, delisted, bankrupt and or suspended asset for which our pricing vendors no longer have enough data to provide a price. In such cases, BNY Mellon's Global Pricing team would use a secondary vendor, if available. If one is not available, they will reflect the last available price. If a security has never been priced by a vendor and a price is not found (i) fixed income instruments will be priced at 100 percent of face amount, and (ii) equities will be priced at one unit of issue currency. See below for our Global Pricing Unit Vendor Chart.

The price per share and market value are reconciled after the closing price is assigned on the last day of the month once again to ensure that the price is accurate and that all positions are valued at the last closing price. The STO can, at any time, create a similar list of assets held using NEXEN® and can print or save the report as a file locally. Avenu can provide a monthly valuation statement of the entire portfolio by issue segregated by stock, dividend reinvestment plans, book-entry, and mutual funds at the end of each month in electronic format to the STO. This statement is delivered in EXCEL and PDF format via secure, encrypted email along with the monthly account transaction and cash reports. We can additionally provide the report in any other format as required by the STO or to an SFTP site for ingestion into your unclaimed property system.

#### Global Pricing Unit Vendor Chart

Asset Classification	Frequency	Primary	Secondary
Equities (U.S./Canada)	Daily	Six Financial	ICE, Bloomberg, Extel, Euroclear
Bonds (U.S./Canada)	Daily	ICE	Bloomberg, Six Financial Euroclear, Extel
Rights Offering (U.S.)	Daily	Six Financial	ICE, Bloomberg
Rights Offerings (non-U.S.)	Daily	Six Financial	ICE, Bloomberg, Extel
Non-US Securities	Daily	ICE	Six Financial, Bloomberg Euroclear / EUCLID
U.S. Treasury Bills, Notes, Bonds	Daily	ICE	Bloomberg, Six Financial
Spot and Forward Currency Rates*	Daily	WM Reuters - via FT ICE	Bloomberg
U.S. Government and Agency Securities	Daily	ICE	Bloomberg, Six Financial
Exchange Traded Futures and Futures Options	Daily	Bloomberg	
Exchange Traded Equity and Index Options	Daily	Bloomberg	
Mortgage-Backed Securities	Daily	ICE	Bloomberg, Six Financial
Agency Mortgages	Daily	ICE	Bloomberg, Six Financial
Asset-backed Securities	Daily	ICE	Bloomberg, Six Financial
Medium-Term Notes	Daily	ICE	Bloomberg, Six Financial
Municipal Bonds	Daily	ICE	Bloomberg, Six Financial
Collateralized Mortgage Obligations	Daily	ICE	Bloomberg, Six Financial
Variable-Rate Notes	Daily	ICE	Bloomberg, Six Financial
Private Placements	Daily	ICE	Bloomberg, Six Financial
Warrants	Daily	Six Financial	ICE, Bloomberg
Convertible Bonds	Daily	ICE	Bloomberg, Six Financial
Mutual Funds	Daily	ICE	Bloomberg, Six Financial
Discounted Commercial Paper and Banker's Acceptance	Daily	ICE	Bloomberg, Euroclear / EUCLID,

<sup>\*</sup> The WM FX Rates are closing rates as of 4pm London/11am EST.

4.2.10 Maintain records relating to services provided herein, for the life of the contract. Vendor shall maintain the security and confidentiality of those records, as required by the Act.



Avenu will maintain records relating to all services provided for the life of the contract or a minimum of 10 years. All records are maintained according to Avenu standard security and confidentially procedures. We currently have our clients' records dating back to 1992 which assist with reconciliation and other efforts. Immediate access to all historical data is available to the STO for 24 months following any transaction via NEXEN®. Records older than 24 months are also maintained securely and can be provided to the STO upon request. In addition, we provide standard monthly reporting packages which include a List of Assets and Transaction Statement in .pdf as well as Excel for the STO's records.

4.2.11 Obtain prior written approval from the STO and shall execute the specific written instructions of the appropriate STO unit with respect to the release, submission, withdrawal, sale, substitution, investment or other disposition of the securities.

Avenu will release securities upon receipt of written authorized direction from an approved and authorized State representative. Avenu can receive these instructions via secure FTP site/electronic transmission, over the Extranet, via fax/hard-copy mail, or e-mail based upon the preference of the STO. An authorized signature is required on all instructions that are sent via fax/hard-copy or mail, as the Avenu account manager will compare this to the list of the STO's authorized signers for verification.

Avenu recommends transmitting these instructions by using our Extranet Method as all instructions are sent and received securely though our Extranet and are submitted by an authorized user from the STO. Additional information on Avenu's Extranet is provided under Avenu Exhibit 4.

After the verification process is complete, transactions are processed and immediately will show in the STO's custodial account as transaction pending for settlement. The information may be viewed at any time during the process using online access via NEXEN®. Additional information on NEXEN® is provided under Avenu Exhibit 3.

4.2.12 Provide CUSIP numbers on securities as requested, preferably electronically by e-mail.

Avenu currently provides CUSIP numbers on securities as requested by the STO. In addition, the STO has the ability to perform a "quick" lookup by security name on the NEXEN® home page to obtain any CUSIP numbers. Avenu is happy to provide training in how to use these tools at any time. Additionally, STO can locate this information and instructions as how to use some of these tools in NEXEN® User Guide included with Avenu Exhibit 3.

4.2.13 Provide a web-based interface for use by the STO and other authorized entities.

Our solution provides our clients with secure access to our web-based products NEXEN® which provides access to intellectual properties, reports, and transactions. This on-line inquiry system allows you to track all transactions, inventory, portfolio value, transaction history and value for a particular security using a date range as well as liquidations or sales. The STO can also utilize this system to research the discrepancies between its portfolio and what is on the STO's unclaimed property management system.

NEXEN® is BNY Mellon's Internet-based product for institutional clients and their investment managers. NEXEN® is an integrated website which is available 24 hours a day, 7 days a week. NEXEN® runs via the internet using all major browsers and requires no extra software to be installed by the STO.

NEXEN® is secured by a unique user ID and password for each user. Each user is set up with access to the STO's account by an authorized individual. This allows the STO to have inquiry-only access to a variety of intellectual properties, reports, and transactions. NEXEN® provides a single gateway and employs controls designed to detect and protect against unauthorized access, such as single (username/password) and two-factor user authentication, data encryption, and a firewall design that ensures secure communications. It is FFIEC compliant. Using this site requires no additional software installation and Avenu will provide training sessions as needed to ensure that the STO's staff is fully knowledgeable and familiar with all the resources available. A NEXEN® Reference Guide is available under Avenu Exhibit 3.

Authorized individuals on NEXEN® have access to view information contained in the STO's accounts and can select from a library of available reports to query, sort and download into multiple formats account data. Additional information related to NEXEN can be found in section 4.3.5.



#### 4.2.14 Provide a Medallion Guarantee of signatures as requested by the STO.

Avenu provides medallion signature guarantees for all of its clients as part of our standard solution and will also continue to provide them to the STO at no charge if awarded this contract. The STO completes the stock power or other documents for medallion signature and forwards them to Avenu. We then obtain a medallion signature guarantee and forward the completed documentation back to STO or designated parties as authorized/directed by STO.

As stated previously in our quotation, by utilizing some of our automated solutions such as mutual funds, we have eliminated the need for STO to obtain stock powers, which is a significant benefit to many of our state clients.

4.2.15 Maintain the mutual fund shares in the same account as the stock shares and include their market value on all reports.

Avenu currently receives and deposits into the STO's unique account all securities, including Mutual Funds delivered by either holder, brokers, fund companies, or other entities for the benefit of the STO.

All of our accounts, including that of the STO, are reconciled on a daily basis to ensure that all income is properly allocated and credited, and all securities transactions are settled properly. The market value is included on the reports in the same manner as all other securities received and held for the STO.

The STO will have access to view this account at any time using our NEXEN® product described throughout this proposal and with more detail under Avenu Exhibit 3.

4.2.16 Send communication regarding any security having no substantial commercial value to the STO stating the security has been researched and has no market value. Upon request from the Unclaimed Property Division, the Vendor shall remove all securities deemed worthless from the STO Custody Account using a Positional Removal (PREM) function or other similar method deemed acceptable by the STO.

As we do now for the STO, Avenu currently researches on a monthly basis, all unpublished and unknown items, or any security received using multiple resources and will provide all details pertaining to the security to the STO and will maintain all unlisted, non-transferable, and worthless securities until receiving instructions from you to do otherwise.

Avenu also offers a unique, one-of-a-kind, and extensive securities research and liquidation process as part of our comprehensive unclaimed securities solution which includes worthless, unpublished, and unknown items.

This service is not found with other custodians and is used by our clients to remove positions from their portfolios. Our worthless security verification process is as follows:

- ▶ Securities identified with "No Value" in the research liquidation process are reviewed to determine if they are "worthless." Worthless securities are defined as securities for which an attempt is made to liquidate and for which no market exists. No market will exist for several reasons, including if the company is bankrupt, trading has been suspended by the exchange, there is no interest in the security by the investor community because of the company size, the financial condition of the company, or some other problem with its trading history.
- ▶ A physical copy of the liquidation form is given to the Raymond James (RJA) OTC Traders. The traders will check the symbol versus the NASDAQ Workstation to see if the symbol registers. If the symbol now has a market, the trade will be executed at the market price and will follow the liquidation procedures described above.
- ▶ When no market appears on NASDAQ, electronic pink sheets are checked to see if there is a market for that symbol. If there are markets, the trade is executed at the market price. The CUSIP number is then checked using RJA's inhouse security management system to determine if the CUSIP number is registered within the system. (Generally, this system will identify if the CUSIP or security is worthless.)
- ► Securities identified through these processes that have potential value will be resubmitted to complete a trade. If a trade is not executed following a request from the STO, then several factors exist within the transaction:
  - 1. The security may be worthless or thinly traded.



- 2. There may be a large block of thinly traded securities that might disrupt the trading price of a security requiring multiple sales.
- 3. The security may be a municipal bond or treasury security that requires additional research and documentation to liquidate. (Before these types of securities are sold, all bonds are researched to determine the fair market value. A number of US Government securities are pooled asset-backed securities and mortgage-backed securities that require substantial research prior to offering to the market. In addition, we liquidate treasury bills, treasury notes, and treasury bonds. Federal Agency securities or Government Sponsored Enterprises (GSE) are often sold as well. The research is generally making a determination of the current value based upon redemptions and prior interest payments. Certain blocks of bonds cannot be sold in odd lots in the open markets and require additional work by the bond trading staff. The first pass to sell one of these type bonds does not always result in a sale and this may require additional research by staff.)
- 4. There may be an error in the documentation requesting the sale such as CUSIP, account number, or number of shares. When one of the events described above occurs, the account manager will notify the STO immediately with a recommended solution to the issue. Once the issue is resolved, the security will, to the extent necessary, be resubmitted through the security liquidation process.
- A security is deemed worthless when it has a reportable cusip according to the regulatory agencies but no public market available to liquidate the shares. These shares can be purchased by RJA for \$0.01 per block upon the STO's approval to liquidate as such.
- ▶ Always looking for new and innovative ways to service our states, Avenu also now offers a process where through RJA we can "write off" non-active securities including DTC and certificates that are unable to be sold and whose cusips are DELISTED or INVALID through the indeterminate Value Removal form supplied by RJA which requires consent from authorized parties within the STO.

Avenu also provides a monthly review of account holdings to remove worthless securities subject to the STO's approval. As the custodian for many of the state unclaimed securities portfolios, we are a large holder of worthless securities and have been a large holder throughout our history due to the nature of abandoned securities, particularly those that are identified through the PREM process.

As part of our standard process, any securities that have been deposited to DTC and are determined to be worthless by DTC will be delivered off the STO's portfolio with explanations. DTC refers to this process as PREM or Position REMoval. The review is done monthly, and a list of PREM eligible securities is forwarded to the STO for review and approval. Once approval is received, the securities are removed from the account, and they are deposited into an omnibus worthless account that DTC maintains and monitors. The STO will receive the shares or value as determined by DTC if the security ever regains value. PREM securities are detailed as part of the transaction history that would be included as part of the STO's regular reports.

These transactions will appear in the statement and on NEXEN® online reporting. The STO also receives email notifications from the Avenu administrator monthly should the STO have any securities that fall into this category.

Avenu communicates and makes recommendations regarding the disposition of any worthless or problem securities that cannot be traded in the open market. Additionally, Avenu will hold worthless positions in the STO's account until specific directions are received from the STO.

4.2.17 Upon request from the STO, take any action necessary to liquidate all securities held by the STO.

As we do now, Avenu, and only with the written approval from the STO's administrator, will execute the sale of any listed securities and deposit proceeds based on the STO's instructions and report each liquidation with a detailed transaction breakdown of sale proceeds upon a set schedule. Avenu provides and maintains a secure, on-line environment for receiving and executing sale requests and Avenu liquidates securities only upon authorization and/or either special or standing instructions from the STO. Collaborating with our partners at Raymond James, Avenu executes sales of securities within three business days including liquidating mutual fund accounts upon instruction from the STO. Funds for these sales are deposited into the STO's investment Account immediately upon settlement of the sale.

Avenu Key Solutions for Securities Liquidation



The next four sections provide information related to the following processes:

- 1. Liquidation process for Stocks, Bonds, Privately Held Securities
- 2. Liquidation of Mutual Funds
- 3. Automated Liquidation Process
- 4. Identifying and Processing Liquidation of Worthless Securities

#### Liquidation Process for Stocks, Bonds, Privately Held Securities

Working with Raymond James, Avenu executes sales of securities within 24 business hours of receiving authorized instruction from the STO. Funds for any sales are deposited into the STO's account upon settlement and wired upon request or agreed upon schedule.

Our experience with Raymond James has provided unparalleled results in executing unclaimed securities sales, worthless research, and liquidations. Avenu receives no compensation from Raymond James, nor do we mark up the associated fees, ensuring the best commission costs for the STO and rightful owners. In addition, working with Raymond James, Avenu has been able to automate the trade process and build in features that protect the STO against possible situations such as oversells.

Upon receipt of instructions, Avenu confirms that the STO is currently holding the requested position and that there are no holds on the item such as a chill, pending transaction, etc. If Avenu finds a discrepancy in the number of shares requested for liquidation (for example: holding less than the amount currently being requested for liquidation, or if a disbursement is pending), Avenu will coordinate with the STO for follow up and resolution. If no discrepancies are identified, Avenu executes the trade same day (or within 24 hours of receipt for requests received late in the day or after trading has closed). The settlement time will depend on the type of security. More time will be required to settle liquidation transactions that relate to Foreign, Physical, Worthless, Restricted and some mutual fund securities. These types of securities require special handling where manual paperwork is required to communicate with transfer agents, privately held and some mutual funds companies. For most of the transactions resulting from trading these types of securities, proceeds might be presented via physical checks.

Avenu systematically forwards the trade instructions received from the State to Raymond James, which are then sent to the depository to await verification and settlement. Any unverified trades are reviewed, and the status updated to enable the trade to automatically settle with the depository. When trades settle, shares are removed from the STO's account.

Simultaneously, sale proceeds will be deposited to the account then swept to the STO's Investment Account. All settlement occurs using the industry standard of T+2. For mutual fund companies that participate in FundWeb, settlement typically occurs as T+1 or T+2. All sale transactions are recorded on the system with the issue name, security type, CUSIP number, number of shares/units sold, trade and settlement date, price per share/unit, gross sale amount, net sale amount and broker commission.

Avenu can accept sale orders from the STO generated out of KAPs and sent electronically to us or via SFTP/electronic transmission, through Extranet, fax/hard-copy or email based on preference. These orders are electronically sent to our broker, Raymond James, and then to the depository to await verification and settlement. Any unverified trades are reviewed daily, and the status updated to enable the trade to automatically settle with the depository. When trades settle, shares are removed from the STO's account and simultaneously, sale proceeds deposited to the account then automatically swept to the State's chosen investment account. All settlement occurs using the industry standard of T+2. For mutual fund companies that participate in FundWeb, settlement typically occurs as T+1 or T+2. The Extranet Reference Guide is included as Exhibit 4.

The Avenu account manager reviews all instructions that are sent and will compare this to the list of the STO's authorized signers for full verification and then uploads the cells to our Avenu Liquidation Console. This in-house developed system verifies that the STO is holding an adequate number of shares to cover the sale to avoid a possible oversell situation. Any rejections are forwarded to the account manager for review, who in turn works with the STO as needed to resolve any discrepancies.

Marketable and valid securities are systematically sent to Raymond James via a secure FTP for the sale execution. The requests are forwarded to Raymond James each day at 10:00 AM and 2:00 PM EST. Raymond James initiates the sale of all marketable securities, which creates a transaction on BNY Mellon's Global Securities Processing System and in turn alerts the STO's account manager that a sale is pending. The securities that are identified with "No Value" are reviewed to determine if they are "worthless" and the STO will be notified.



For the sale transaction to settle, the STO's account manager with Avenu must actively verify each sale transaction, ensuring for a third and final time that all positions are being sold precisely as requested by the STO, and that commission charges are calculated and applied correctly. Once verified, the transaction settles within two business days. The applicable shares are delivered out of the STO's account and sale proceeds are received at that time. These shares are simultaneously marked as sold/settled and viewed on NEXEN®.

Avenu's account administrator will provide the STO with a list of securities that cannot be sold along with the reason for the non-sale status. Please refer to Avenu Reports under Exhibit 5, Position – Unable to Trade Report, for illustration and more information. Avenu can sell securities on listed exchanges as well as execute private sales.

Avenu and Raymond James will assist in determining whether a private sale is the only market for such securities and follow all authorized instructions of the STO. Below is an overview of our trade process flow:

- ► The STO's authorized individual inputs a trade request through our web-based trade entry system (or other agreed upon method) and Avenu is alerted to the transaction request
- ▶ Avenu verifies position; informs the STO of any discrepancies/problems identified
- Trade is executed
- ▶ Executed trades are sent to the depository to await settlement
- ► Avenu receives trade details via NEXEN®
- ▶ Trade details are entered into the DTC ID system in unverified status
- ▶ Unverified trades are viewed through our web based NEXEN® real-time custody product
- ▶ Avenu affirms trades online in NEXEN® for all DTC-eligible securities
- ► Trades settle T+2 (trade date plus two days)

Avenu provides superior record keeping of all sales including sales proceeds, gross and net of commissions through NEXEN® online reports, monthly reports and custom data files which can be created upon request. Avenu will additionally provide a breakdown on the commission charge for each sale if requested by the STO. Please refer to Avenu Reports Exhibit 5 - Securities Liquidation Report for an example of this report.

With the information available in the NEXEN® reports, the STO or Avenu can schedule a report to run and be available each morning which will identify all securities sold and settled in the STOs account. Due to the extremely flexible nature of our system, this reporting can be run in many different formats such as CSV, TXT, Excel, PDF etc. This information can then be uploaded to the STO's Unclaimed Property System.

#### Liquidation of Mutual Funds

As mentioned earlier, Avenu has created an automated way of processing and maintaining mutual funds which is like that of DTC. The STO's account manager at Avenu receives the STO's instructions to liquidate, and instead of forwarding the request to Raymond James as with securities, the sale request is forwarded to the individual fund companies via BNY Mellon. These requests are processed directly at the fund companies, shares are debited from the account and proceeds received. The turnaround time for mutual fund liquidation is typically between 24-72 hours. However, some fund companies do not participate in FundServe or otherwise require written instruction, which can result in a longer timeframe for the transaction to be completed. Please refer to Avenu Reports under Exhibit 5, Mutual Fund Sales Report for more information.

#### Liquidation of Foreign Securities

Raymond James is a registered broker dealer with vast experience in both domestic and international brokerage dealer services and will work with the Avenu account manager to execute and assist on liquidating foreign securities for the STO.

#### Automated Liquidation Option

Avenu offers an automated process for liquidations. With this feature, once a sale transaction has settled, a file can be generated and sent to the STO's Unclaimed Property Management System to update those records systematically. Avenu's internal liquidation system was developed as part of our solution for states to automate the process of liquidating securities. Every morning, on business days, the account holding position file is downloaded from NEXEN® and uploaded to our liquidation system to where liquidation requests are checked for adequate number of shares to cover the sale of securities. The system is reconciled against NEXEN® account holding positions.



The STO will then receive an automated report and/or data file detailing the particulars of the sale for each sale date including all information recorded with the transaction such as: issue name including security type, CUSIP number, number of shares/units sold, trade and settlement date, price per share/unit, gross sale amount, net sale amount, broker commission rate per transaction, and any other fees. The STO's unclaimed property database is updated accordingly.

All sale transactions are recorded on the system with all the needed information like issue name, security type, CUSIP number, number of shares/units sold, trade and settlement date, price per share/unit, gross sale amount, net sale amount and broker commission. All settlement details can be seen on-line or electronically transmitted within 5 days of settlement or at any frequency or method as required (daily, weekly, monthly etc.) in a multitude of formats for upload or ingestion into the STO's Unclaimed Property system. Avenu can set up a daily transmission of the transaction file data to the STO.

Avenu will process liquidations within 24 hours of receiving authorized instructions from the STO below indicates a timetable for each type of security and its settlement for reference:

Security Type	Liquidation Duration
DTC	T + 2
Federal Reserve	T + 1
Physical	5-15 Business Days – Depending on
	Company
Statement	5-20 Depending on Transfer Agent
Mutual Fund	1-5 Business Days
Foreign Securities	Depends on Foreign Market

4.2.18 Upon request from the STO, electronically re-register securities directly to claimants or register via physical certificate, insured against loss, and return receipt requested. Vendor shall prepare paperwork, send for Medallion Signature guarantee, send paperwork to transfer agent, and receive confirmation from transfer agent. Additionally, Vendor shall provide confirmation letters and copies of the returned certificates to the STO.

Avenu understands and deeply appreciates the central purpose of holding property in custody is for rightful owners and has developed procedures to best perform this function for our state clients. Upon receipt of proper instructions either electronically or in an agreed upon format, Avenu will continue to initiate the reissuance of a security to an owner within 24 hours of receiving the request.

As part of our commitment, Avenu checks the portfolio to ensure that the STO is currently maintaining the position in its account prior to finalizing any transactions. If there are discrepancies with the number of shares/units requested to transfer and the number of shares/units currently being held, or if there are questions on the registration instructions, the STO's dedicated account manager, Vicki Perkins, will coordinate for problem resolution. Once the discrepancy is resolved, Avenu will update the request and confirm with STO authorized personnel for final authorization, if needed.

The STO will be able to verify that the submission is processed within 24 hours of receipt by running a report of pending trades on NEXEN®. The STO will be able to see the trade date, which is the date the trade was entered, and verify that the trade was entered according to our procedures and timeline. A sample of this report is provided under Avenu Reports Exhibit 5- Unsettled Trade Report.

Avenu settles the transaction to the STO's account with a complete description of the transaction including information such as registration name or owner name, date of transaction, security, number of shares/units and claim number if provided. This owner information along with the claim number is also included in the standard monthly/daily reports and available online, ensuring easy tracking of the claim transfers for reconciliation and follow up. We have customized and increased the length of the fields in our system to accommodate additional information concerning the owner as it is extremely useful to an unclaimed property program. Other custodians may have a limited number of characters and not be able to accommodate this additional detail.

#### Methods of Transaction Requests

Avenu has the ability to receive proper instructions/requests in a variety of ways depending upon the preference of the STO.

**File Transfer Protocol** – The STO can generate a file from its unclaimed property management system, which can be delivered to Avenu's secure FTP site to initiate transfer requests.



This method eliminates all paper letters or reports to then either fax or mail to Avenu for our clients and reduces the amount of manual effort required for both the STO and Avenu to deliver a transfer request which additionally reduces the amount of time a transfer will take to be completed. In addition, this method allows the STO's staff to spend the time currently dedicated to preparing transfer requests on other unclaimed property related tasks.

The file will include: the claimant's name, social security number, current mailing address and/or DTC number, receiving agent's name and customer account number (if applicable), issue name, CUSIP number and quantity of shares/units to be transferred.

All the information provided in this request is required, as it will be used to transfer shares to the owner and will appear in the settled transaction report which the STO can view at any time using NEXEN®. The request will be forwarded to Avenu via secure FTP site and systematically processed through DTC. Avenu will continue to review and monitor the file for any exceptions and work with the STO and the transfer agent to promptly resolve and process these transfers. Upon settlement, a return file will be forwarded to the STO to mark open transfers as completed. A high-level overview of this automated process is provided below:

- ► Acknowledge receipt of the file.
- ▶ Confirm that the STO is holding the position.
- ► Forward to the transfer agent with minimal amount of re-keying
- ▶ Provide to the STO an electronic report showing transfer request has been sent to transfer agent by date.
- ▶ Provide electronic notification of issuance of certificates to owners, as well as an image if certificates are issued when necessary.

**Written Request** -The request includes but is not limited to the claimant's name, social security number, current mailing address and/or DTC number, receiving agent's name and customer account number (if applicable), issue name, CUSIP number and quantity of shares/units to be transferred.

All the information provided in this request is required, as it will be used to transfer shares to the owner and will appear in the settled transaction report which the STO can view at any time using NEXEN®.

**Avenu Extranet** – The STO can initiate transfer requests using Avenu's online Extranet system. Please refer to Avenu Exhibit 4 for a copy of our Extranet Reference Guide. An authorized individual at the STO can upload transfer information on this website and the user receives confirmation that the transaction has been received along with a tracking number. The information that has been requested is displayed with the username, time, and date of request.

For the purposes of dual authorization, we offer a second confirmation of receipt to be delivered to a separate authorized user via email. This ensures that more than one individual is involved with all transaction requests and that all information being requested is tracked. By initiating a transfer request online using our website, the STO can track the number of requests being generated by any user, verify at any time how the information was requested, track the turnaround time for completion and ensure that proper audit procedures for dual authorization are being followed. As with any transaction that Avenu would initiate on behalf of the STO, there are strict guidelines and procedures that are followed. These procedures were put into place to protect both Avenu and its clients.

As part of our commitment to ensure we prevent any potential problems for our state clients, Avenu checks the portfolio to ensure that the STO is currently maintaining the position in its account and confirms that there are no outstanding actions that impact the position prior to finalizing any transactions. All requests are processed within 24 hours of receipt and verification. If there are any discrepancies with the number of shares/units being requested for transfer and the number of shares/units currently being held, or if there are questions on the registration instructions, the STO's dedicated account manager will coordinate with the STO for problem resolution. Once the discrepancy is resolved, Avenu will update the request and confirm with the STO for final authorization, if needed.

Upon successful transfer of securities, Avenu settles the transaction to the STO's account with a complete description of the transaction including information such as registration name or owner name, date of transaction, security, number of shares/units and claim number if provided. This owner information is also included in the standard monthly reports, ensuring easy tracking of the claim transfers for reconciliation and follow-up.

Direct Registration Shares (DRS)



Direct registration shares ("DRS") is a practice that is being increasingly promoted by transfer agents and holding companies which presents another challenge to state programs due to the increase in paper as well as having assets held outside of the STO's DTC account.

With DRS, the ownership of shares is recorded in the books of the transfer agents or the holding companies and holding statements are issued rather than certificates. Transferring shares via DRS is far more cost-effective than processing and issuing certificates. While this cost-effective method works well for the agents and their customers, the use of DRS presents a large problem to state unclaimed property programs because of the volume of transactions and the way in which unclaimed securities transactions are held and need to be processed. For the STO, we can also develop our automated solution to manage these DRS positions, eliminate the paper and manual processing which simplifies the process for our state clients.

Upon receipt of a transfer request from the STO, Avenu instructs DTC to issue the requested position into the name of the owner(s). DTC then forwards the instructions to the transfer agents or holding companies, which (in the case of DRS) open an account on behalf of the owner(s). The DRS statements are mailed directly by the transfer agents or holding companies via first class mail to the owners.

The statement includes share amount, security name, type of stock, CUSIP, owner name, owner address, account number, transaction date and type of transaction. A duplicate statement is not mailed to either Avenu or the STO but instead, the STO accesses NEXEN® for the date the transfer was completed, and the statement mailed to the owner.

This reduces paper coming into both offices and provides an automated means of obtaining this information to then record the completed transaction in the STO's unclaimed property management system. The STO can additionally schedule a report to be delivered each day which provides the information on these completed transactions. Finally, the STO can utilize NEXEN® to check the status of the transfer throughout the process.

### Depository Trust Company (DTC) Transfer

If the position is being transferred to an owner's account via DTC, the securities will be deposited to the owner's brokerage account within 24 hours of receipt as there is no need to issue a DRS statement or stock certificate and mail it to the individual. Transferring via DTC is the most efficient, cost effective, and the quickest way to return shares to rightful owners. Avenu encourages the STO to include a place for owners' brokerage account information on the claim form when shares are involved.

#### Physical Certificate

In the case where a physical certificate is required and issued, the transfer agent will mail the certificate, registered in the name of the owner according to the STO's instructions, either directly to the STO or directly to the claimant depending upon the preference of the STO.

Avenu has a standing procedure in place for all transfers to owners where DRS is the default. This is far less costly than issuing physical certificates. Some companies still offer a choice between DRS and physical, though most companies offer exclusively one or the other and only a small number of companies issue physical certificates only. Avenu will work closely with the STO to find alternative ways to complete the transfer when the possibility of certificate issuance is identified.

Approximate timeline of processing these types of transfers is included at the below indicated table:

Format	Re-registration Duration
Depository to Depository (DTC)	24 hours
Direct Registration Shares	3 – 5 business days
Physical Certificate	10 – 15 business days
Open-end Mutual Funds	5 – 10 business days
Close-end Mutual Funds	10 – 15 business days
Dividend Reinvestment Plans	10 – 20 business days

If there are any discrepancies with the number of shares/units requested to be transferred and the number of shares/units currently being held, or if there are questions on the registration instructions, the STO's dedicated account manager will



coordinate with the STO s staff for problem resolution within 24 hours of identifying the issue. Once the discrepancy is resolved, Avenu will update the request and confirm with STO's staff for final authorization. Please refer to Avenu Reports Exhibit 5, Transaction Report PDF Format specifically to Transfer to Claimant Transaction for more information.

#### Mutual Fund

Avenu will reissue a mutual fund into an owner's name upon receipt of authorized instruction from the STO. In instances where the owner already has an active account at the respective fund company, Avenu will work directly with the claimant, fund company or broker to have the shares transferred to the owner's account whenever possible. In some cases, an account application is needed if an owner does not already have an active account. In these instances, Avenu will work with the STO or directly with the owner to get these required documents for the transfer to complete. For many of our state clients, we deal directly with the owners to assist in the completion of the documentation, explaining why Avenu encourages the STO to include a place for an owner's brokerage account information on the claim form for a quick turnaround.

Avenu has the ability to coordinate multiple transfer requests simultaneously and we regularly send emails and place phone calls in an effort to work directly with claimants and their brokers to explain the process to ensure they have a clear understanding in regard to their options for receiving back their rightfully owned shares. Avenu provides individualized case by case service and answers claimant questions throughout to ensure a smooth process for all parties involved. This unique service proves to be what sets Avenu apart from other providers. We understand that many situations are sensitive and can at times be emotional for some claimants and we work hard to accommodate their needs to ensure that the shares are returned to the rightful owners as quickly as possible. In all instances, tracking of claims can be viewed online via NEXEN® but the Avenu account manager also provides a more detailed monthly report to the STO detailing the status of all pending claims.

4.2.19 Within three (3) days of completing a transaction, report all interest, dividends, corporation actions, proceeds of sale and any other earnings related to the securities held in safekeeping as unclaimed property, and follow all instructions from the STO as to the sale of securities related to unclaimed property.

Avenu collects all dividends, interest income, sale proceeds and allocates all income to the appropriate CUSIP numbers within the STO's account. All cash balances are reconciled on a daily basis to ensure that the STO's account has been properly credited with the appropriate income. All principal and income are posted to the STO's account on the payable date.

Avenu also collects and allocates all corporate restructuring activity such as stock splits, stock dividends, mergers, etc. Avenu processes and posts all corporate actions made by issuers of securities which are held in Avenu's custody for the STO. As with any settlements, all receipts are reconciled at the end of each day to ensure that the STO's account has received what was due.

All transactions are accurately reported in the transactions reports that can be retrieved by the STO anytime though our online portal – NEXEN, and also reported to the STO on the first business day of the month.

4.2.20 Complete all wire transfers within one (1) business day requested by the STO.

Avenu currently processes wire transfers to the STO on a monthly basis. Avenu has standing procedures whereby cash account balances are remitted to the STO on the first business day of the month. As with any part of our flexible solution, procedures can always be modified upon agreement by the STO and Avenu. Wires can also be initiated as needed upon request upon receipt of the STO authorized instructions.

### 4.3 DELIVERABLE - ACCOUNTING AND REPORTING

4.3.1. Vendor shall provide custodial and securities accounting services for unclaimed securities including mutual funds.

Acknowledged. Avenu currently provides custodial and securities accounting services to the STO and upon request can incorporate additional mutual fund services to include transfer to claimants should the STO require.



4.3.2. The Vendor shall deliver all reports and documents to the STO in an electronic format and, if requested, in a printed version. The Vendor shall provide electronic versions of the documents as follows: Spreadsheets shall be compatible with Microsoft Excel files; expository reports shall be compatible with Microsoft Word and/or Adobe PDF-format files; and database files shall be compatible with Microsoft Access software. Vendor should provide samples of each report with Vendor's bid.

Acknowledged. Avenu currently provides scheduled reports to the STO and currently delivers reports on a daily/monthly basis as needed and can provide these reports in the format that best accommodates the needs of the STO. Due to the extreme flexibility of our reporting system, NEXEN®, the generation of reports can be done in a multitude of formats such as PDF, CSV, XLS, and TXT and can be immediately changed as the STO's needs change. The STO also has the ability to schedule reports through NEXEN® at any point in time. Examples of reports provide are available for reference in Avenu Reports Exhibit 5.

4.3.3. The Vendor shall provide the STO the ability to schedule reports as needed.

Acknowledged. Avenu currently provides scheduled reports to the STO and currently delivers reports on a daily/monthly basis. The delivery of reports can be changed at any point in time due to the need of the STO. The STO can also schedule reports through NEXEN® as desired and as needed.

4.3.4. The Vendor shall format reports to be compatible with the STO Unclaimed Property System, KAPS.

Avenu, using a Secure File Transfer Protocol (SFTP) site, can provide automated updates of all key Bank of New York Mellon NEXEN® information for the STO's unclaimed property management system at a frequency determined by yourselves, eliminating the need for manual attention while keeping the STO's records up to date for accurate administration of all transactions, liquidations and other activities that may affect properties held in custody.

Currently, Avenu provides a monthly valuation statement of the entire portfolio by issue segregated by stock, dividend reinvestment plans, book-entry, and mutual funds at the end of each month in electronic format to the STO. This statement is delivered in EXCEL and PDF format via secure, encrypted email along with the monthly account transaction and cash reports.

Due to the flexibility of our system, we can additionally provide the report in any other format as required by the STO (PDF, XLS, CSV, TXT) or deliver it to an SFTP site for ingestion into your KAPs system.

The monthly statement contains the issue name, CUSIP number, location that the assets are held, i.e., dividend reinvestment plan held at agent, book-entry, mutual fund at fund, physical etc., price per share/unit and market value for all positions held by the STO. With NEXEN®, the STO has additional capabilities to add or to delete fields from these reports.

4.3.5. The Vendor shall provide online reporting capabilities that can be utilized by the STO staff.

As mentioned earlier, Avenu currently provides 24/7 access to NEXEN®, our online access inquiry and reporting product. NEXEN® is BNY Mellon's Internet-based product that meets this requirement. NEXEN® is an integrated website which allows the STO to have inquiry-only access to a variety of intellectual properties, reports, and transactions. NEXEN® provides a single gateway and employs controls designed to detect and protect against unauthorized access, such as single (username/password) and two-factor user authentication, data encryption, and a firewall design that ensures secure communications. It is FFIEC compliant. Using this site requires no additional software installation and Avenu will provide training sessions as needed to ensure that your staff is fully knowledgeable and familiar with all the resources available. The NEXEN® Reference Guide can be found in Exhibit 3.

The STO provides Avenu with a list of authorized individuals that should have access to view information contained in the accounts and this listing is reviewed on an annual basis. Users can select from a library of available reports to query, sort and download account data. Reports can be run on demand or scheduled to run at the time of your choosing such as daily, weekly, monthly and at a particular time of day. Reports can also be set up for delivery to FTP locations or directly to emails and in a multitude of formats such as PDF, CSV, XLS providing instant flexibility. NEXEN® Reporting offers the



enhanced reporting capabilities of quickly changing the logical sort order within a report and drilling down as many as two levels to see selected data in greater detail. Avenu will work with the STO to accommodate reporting needs as they change.

NEXEN® provides the ability to track all transactions on your portfolio including but not limited to, inventory, account value, value for a particular security, transaction history for a particular security or date range as well as liquidations or sales, corporate actions, market values, reports, class actions and cash. All reports can be run at a specific point in time or for any particular date range. And as mentioned, run in a multitude of formats. Also helpful to you is the tracking of transfers to owners in which Avenu includes the claim number, owner name and registration of the security.

This proves helpful when performing research on an old claim or if an owner claims that property was never received. Avenu can also provide this service for liquidations executed for the benefit of an individual claimant. The same information can be included for tracking purposes. Each NEXEN® user has authorized access to a menu of reporting options, resources, and tools. Details and options include, but are not limited to:

#### Reporting

- ▶ Timely access to real-time cash, custody, accounting, performance and more
- ► Analytics, securities lending, and benefit disbursement reports
- ► Fully customizable reports via the use of user defined parameters
- ► Comprehensive scheduling facility
- ► Sophisticated report writer
- ▶ Drill-down capabilities
- Supports a series of industry standard file formats such as HTML, PDF, XLS, XML, CSV, TXT, RTF, and PRN file formats.

#### Real-Time Custody

- ▶ Direct access to the real-time core processing engine
- ► Status of transactions
- ► Details of asset positions
- Corporate action announcements which include voluntary, mandatory and class action

#### Intellectual Properties

- ► Global news updates
- Market conditions and trends
- ► Operational policies & global custody standards
- Securities lending market updates
- ▶ Depositary risk analysis

#### Russell/Mellon Analytical Services

- ► Performance web generator
- ► Universe information
- ► Index product information
- ► News and upcoming events
- ► Market outlook
- Analytical insights

All authorized users can run management reports to assist with research and updating of activity on the STO's unclaimed property management system or for annual reporting. This ensures that the portfolio is available at the touch of a button at any time to all authorized users.

4.3.6. The Vendor shall provide the STO with all reports by the first business day after the end of the applicable reporting period.

Acknowledged. Avenu currently provides scheduled reports to the STO and currently delivers the below reports on a daily/monthly basis as needed. The STO also has the ability to schedule reports through NEXEN®.

Cash and Security Transactions



- Custody Valuation
- Settled Cash Balances
- 4.3.7. Monthly Reports: Vendor shall provide the following reports or information in a format agreed upon by the Vendor and the STO:
  - A detailed report identifying number of transactions, unit cost, and total cost;
  - · An inventory of the securities held;
  - A summary of cash receipts and disbursements, which includes, but is not limited to:
    - Date of Transaction
    - Number of Units
    - Market Value
  - Any change to the account due to dividends, redemption, stock splits or other action affecting the
    account: and
  - A summary of earnings for the month, which includes, but is not limited to:
    - Income Earned
    - Dividends
    - Interest
    - Corporation Action
    - Other Receipts
    - Fees & Other Expenses
    - Transfers

All reports can be automatically generated out of NEXEN®, which can provide the STO with all required details needed. Files typically run in an excel format, however, based on our systems' flexibility, they can be generated in multiple formats such as XLS, XLMS, CSV, PDF, TXT. Files can also be sent securely and electronically to the STO as needed. Avenu can also quickly change the method of delivery should the needs of the STO change. Systematic delivery (daily, weekly, monthly) can be accomplished to an SFTP site for automatic submission into your unclaimed property management system. Avenu also can automatically schedule reports to run at required frequencies and times and auto deliver them to an SFTP site whereby your data can be automatically incorporated into KAPS or any unclaimed property management system. Avenu can additionally schedule reports that will be automatically delivered to the STO each day.

Avenu also provides the STO with access to NEXEN®, our online reporting system which tracks all deposit dates, trade dates and settlement dates for not just securities but cash-related transactions, dividends, monthly valuations, corporate actions, etc. NEXEN® provides clients with immediate access to current account information as well as for the previous 24 months. Our system has a multitude of other reports in addition to transaction files but not limited to:

- ► Monthly reporting showing all transactions per security, ending balance for all security, cash positions, and value of all incoming securities:
  - ✓ Cash and Security Transaction Report
  - ✓ Custody Security Transaction Report
  - ✓ Settled Cash Balance
- ► Listing of all securities eligible for sale:
  - ✓ Custody Valuation Report
  - ✓ Lot Level Valuation
- ► Listing of securities with a total market value:
  - ✓ Custody Valuation Report
  - ✓ Custody Holding Report
- ► Custom/Ad-hoc reports that offer the flexibility to present account activity, status, market value and other information in a format as desired by the STO. Custom/Ad-hoc that offers the flexibility to present account activity, status, market value and other information in a format as desired by the STO.



- 4.3.8. Holdings Reports: The Vendor shall furnish a **S**tatement of Holdings Report **d**etailing the following information:
  - Number of Units
  - Issue Name
  - Market Value
  - Dividends Earned in detail
  - Corporate Actions (CUSIP number changes, mergers, splits, etc.)

Avenu currently provides and will continue to provide holdings reports. Information related to these reports is included in 4.3.7 above. Please refer to Avenu Reports Exhibit 5, Lot Level Valuation Report PDF Format, which illustrates account holdings by the date of receiving the security in the account.

4.3.9. Conversion: Vendor shall provide a conversion process that will enable the STO to convert to the new system with a minimum interruption of its business that will allow for the establishment of new accounts and will provide for the smooth transfer of all securities from the current vendor. At the conclusion of the contract, the Vendor agrees to allow the STO access to all account history and reports for six months.

Avenu is proud and honored to be the incumbent for the STO and as such if awarded this contract, the headache of a conversion will not be necessary.

In the event that a conversion to a new custodian is required, Avenu will commit to the necessary resources and will work closely with the STO to ensure a smooth and easy conversion process. We will ensure that there is clear communication between all parties throughout the conversion process as well as beyond as additional income and positions may be delivered to Avenu as the STO's current custodian/broker. Avenu will ensure an easy and thorough transition process by being very transparent and working closely with the STO and/or their custodian. Avenu will perform the following:

- ► Transfer all securities designated by the STO to the successor contractor. Avenu will deliver all DTC and physical certificates to the successor. Should the successor be unable to hold certificates, Avenu will forward them directly to the STO for safe keeping. As is the case with unclaimed property programs, Avenu anticipates the continual receipt of certificates in current nominee name and/or positions via DTC. Avenu would, for a period of one year, provide legal documentation required for the successor to deposit the certificates. All Avenu positions will be sent back with a message indicating the new instructions and delivery address.
- ▶ Provide the successor contractor with all information related to the services. All information would be communicated concerning the management of the account prior to conversion.
- ▶ Respond to any questions from the STO or successor contractor related to Avenu's prior administration of the program. Avenu would provide a conversion contact familiar with the administration of the program. This person would be able to answer all questions and follow up on any outstanding issues until completion.
- ▶ Retain all books, records, and other documents relative to this contract for five (5) years after final payment or until audited by the STO, whichever is sooner.
- 4.3.10. Implementation Date: Vendor shall have all Services established and operating within sixty (60) business days of the effective contract date. If the Vendor fails to meet this time frame requirement, the STO may, in its discretion, deem the Vendor in breach of contract and take such action that is in the best interest of the STO. Any such delay will result in the Vendor being liable to the STO for the cost of maintaining its current safekeeping provider plus a twenty-five percent (25%) administrative fee. In no event shall the administrative fee exceed the cost of a one-year term as provided by the contract.

Avenu is proud to be the incumbent custodian with a current team in place for the West Virginia, State Treasurer's Office, Division of Unclaimed Property, and no delays will result should a contract be awarded.



### **4.4 DELIVERABLES - OTHER**

4.4.1 Problem Resolution: Vendor shall provide timely problem resolution solutions regarding the Services provided to the STO.

Acknowledged. Avenu will provide timely problem resolution to the STO as set forth throughout this proposal.

4.4.2 Disclosure of **S**ubcontractors: If the Contractor intends to utilize subcontractors to perform any of the services in this contract, the Contractor must **d**isclose the following:

In order to provide best-in-class service to our clients, Avenu has partnered with industry leaders, Raymond James, and The Bank of New York Mellon. Avenu believes that segregating the duties of custody, processing and liquidation provides an added benefit to our clients such as providing more flexibility to cope with capacity, enhanced innovation, and flexibility, increases checks and balances and reduces dependency and risk without the hassle or challenges of our clients having to manage.

For the last 20 years, Avenu has partnered with the Bank of New York Mellon (BNY Mellon) and Raymond James & Associates (Raymond James).

#### Neither of these institutions appears on the West Virginia Restricted Financial Institution List.

With these world-class partners, Avenu offers features and functionality such as worthless securities research and liquidation, physical certificate vaulting, automated mutual funds processing, direct registration shares statement processing and systems integration not available with other vendors. We have been able to create these features due to our leadership and experience in the industry, creative approaches, and true partnerships with our subcontractors. Through our partnerships with Raymond James Financial Inc. and BNY Mellon, we are a member of all principal stock exchanges including New York, American and OTC and trade/execute sales on all these exchanges on behalf of our unclaimed securities custody clients. In addition, BNY Mellon trades on over 100 global markets which are critical for the maintenance and sale of unclaimed securities. Raymond James Financial Inc. provides services for the sale of securities at the request of the State. Always looking forward for our clients, Avenu has also recently partnered with Gemini to provide Cryptocustody services for our states. Avenu meets at least monthly with all of our partners.

Required Information	Bi <b>dd</b> er Response
Legal business name and full address	Raymond James & Associates, Inc.
State business was incorporated in	Florida
Phone Number	804.225.1148
Description of subcontractor's organization and the services it will provide	American multinational independent investment bank and financial services company providing financial services to individuals, corporations, and municipalities through its subsidiary companies that engage primarily in investment and financial planning, in addition to investment banking and asset management.
Description of the Contract Activities that will be performed or provided by the subcontractor.	Raymond James will perform security liquidations for the STO.
Information demonstrating the subcontractor meets the requirements for providing those services.	As the current subcontractor for Avenu Raymond James is currently processing these trades for the STO.
Website address	https://www.raymondjames.com/
The relationship of the subcontractor to the Contractor	Current subcontractor for 29 State contracts.
If the Contractor has a previous working experience with the subcontractor, provide the details of that previous relationship	As the current subcontractor for Avenu Raymond James are regularly in contact to provide the needs for all of our state clients.



Raymond James & Associates, Inc. ("RJA" or "Raymond James") has been in the business of processing and liquidating unclaimed securities for more than 20 years, beginning in 2003. Raymond James will serve as a subcontractor to Avenu Insights & Analytics and will perform security liquidations for the STO.

**Economics** 



Raymond James Financial, Inc. is a Florida-based diversified holding company providing financial services to individuals, corporations, and municipalities through its subsidiary companies. Raymond James was founded in 1962 with the objective of providing a comprehensive range of investment opportunities to investors, while maintaining a policy of professional integrity. Since its modest beginnings, the Firm has grown into one of the largest financial services firms in the United States. A public company since 1983, Raymond James is listed on the New York Stock Exchange under the symbol "RJF", and its shares are currently owned by more than 18,000 individual and institutional investors. In the Commonwealth of Virginia, Raymond James maintains 107 local offices, employs 382 associates, and manages more than 96,400 retail accounts totaling \$23.1 billion.

Raymond James and its subsidiaries have more than 21,000 employees with nearly 8,700 financial advisors serving more than 3.5 million accounts with offices in all 50 states, Canada and overseas. Raymond James is now the largest independent securities firm in the United States by market capitalization and has nearly \$1.17 trillion in client assets under management.

As of January 1, 2023, the Firm's total equity capital was \$9.7 billion, including \$1.1 billion in excess net capital. Their capital position provides flexibility to service their clients' accounts and trade and support the pricing of transactions.

Deep Understanding of the Business. We know they have a deep understanding of the business of liquidating unclaimed securities as it has been a primary focus of their Unclaimed Security Liquidation practice for more than 20 years. They have agreements in place with 30 states to handle this service. RJA typically handles more than 31,000 individual transactions each year for our clients involving more than 320 million shares of tradeable and worthless securities. No other firm in the country handles this volume of transactions and shares for unclaimed security liquidations. RJA understands the nuances associated with complicated and thinly traded securities. Their Operations and Reorganization Departments have extensive databases with expansive histories of companies and securities. Their procedures, systems, and internal control structures provide a platform from which their clients can be assured securities will be liquidated in a manner that is consistent with state and federal regulatory requirements, as well as agreements with clients.

Raymond James has processed the below highlighted volumes of transactions for the states through 2022 as detailed in the table below.

Number of Shares

### Raymond James Processing of Unclaimed Securities

Number of Transactions				
Calendar				
Year	Tradeable	Non-Tradeable	Total	
2013	22,344	4,063	26,407	
2014	23,641	3,637	27,278	
2015	27,267	5,222	32,489	
2016	28,606	4,401	33,007	
2017	34,751	5,526	40,277	
2018	31,984	4,403	36,387	
2019	25,057	2,342	27,399	
2020	26,340	763	27,100	
2021	31,286	487	31,773	
2022	32,646	283	32,929	
Total	283,922	31,127	315,046	
A ****	20 202	2 112	21 246	
Average	28,392	3,113	31,346	
Median	27,267	4,063	31,773	

	11111	liber of Shares			Economics
Calendar					Transaction
Year	Tradeable	Non-Tradeable	Total		Dollar Value
2013	47,711,425	8,491,422	56,202,847	\$	569,941,457
2014	142,261,735	47,924,528	190,186,263	\$	570,746,807
2015	109,949,954	234,158,300	344,108,254	\$	787,986,439
2016	47,689,049	92,093,628	139,782,677	\$	542,299,547
2017	45,014,745	317,104,684	362,119,429	\$	746,346,496
2018	76,140,167	279,328,635	355,468,802	\$	763,708,396
2019	79,635,902	99,420,309	179,056,211	\$	524,813,659
2020	294,621,706	63,135,445	414,601,999	\$	617,384,900
2021	752,108,172	84,472,069	836,580,241	\$	923,909,114
2022	737,845,055	20,265,659	758,110,714	\$	678,034,557
	2,332,977,910	1,246,394,679	3,636,217,437	\$ 6	5,725,171,372.21
Average	233,297,791	124,639,468	319,789,636	\$	672,517,137.22
Median	79,635,902	92,093,628	344,108,254	\$	617,384,900.29

RJA is one of the largest Broker/Dealers in the United States and has extensive resources from which to draw.

It is the non-tradeable or worthless securities that creates the greatest workload for any firm and presents the greatest risk for the firm or broker, Avenu, and the State.

Proper control systems, extensive databases, and the need to manually intervene in these processes are critical to ensuring the transactions are handled appropriately. While automated systems are extremely important in this process to expedite the transactions, a strong and well-versed staff is equally important to research and resolve issues as they arise.



Much of RJA's success can be attributed to the firm's commitment to its existing client base and the firm's efforts to identify efficiencies and cost-saving opportunities for its clients. RJA's philosophy is to develop long-term relationships with all its clients and provide comprehensive financial services on all transactions that provide benefit regardless of size or profitability. The State will have access to all of RJA's resources and can call upon their firm to fulfill any of its financial needs.

Required Information	Bi <b>dder</b> Response
Legal business name and full address	Bank of New York Mellon
State business was incorporated in	Delaware
Phone Number	508-871-8662
Description of subcontractor's organization and the services it will provide	BNY Mellon is a global investments company dedicated to helping its clients manage and service their financial assets throughout the investment lifecycle.
Description of the Contract Activities that will be performed or provided by the subcontractor.	The Bank of New York Mellon ("BNYMellon") receives, maintains, and delivers securities and cash upon our instruction on behalf of our state clients. Avenu provides all instructions for transacting securities and cash and BNY Mellon executes those transactions via NEXEN® which is BNY's platform.
Information demonstrating the subcontractor meets the requirements for providing those services.	As the current subcontractor for Avenu, BNY currently supports NEXEN® so Avenu can support clients daily processing needs including reporting, liquidations, transfers, wire processing, corporate action, vault storage, reconciliation, receipts, and all other account maintenance.
Website address	https://www.bnymellon.com/
The relationship of the subcontractor to the Contractor	Current subcontractor for 29 State contracts.
If the Contractor has a previous working experience with the subcontractor, provide the details of that previous relationship	As the current subcontractor for Avenu BNY are regularly in contact to provide the needs for all of our state clients.



The Bank of New York Mellon ("BNY Mellon") receives, maintains, and delivers securities and cash upon our instruction on behalf of our state clients. Avenu provides all instructions for transacting securities and cash and BNY Mellon executes those transactions.

BNY Mellon is a global investments company dedicated to helping its clients manage and service their financial assets throughout the investment lifecycle. Whether providing financial services for institutions, corporations, or individual investors, BNY Mellon delivers informed

investment management and investment services in 35 countries and more than 100 markets.

BNY Mellon Asset Servicing offers clients world-class products, technology, and service to help enhance the management, administration, and oversight of their investment process. As one of the world's leading securities providers, we combine unrivalled client service with innovative technology that delivers rich client data in user-friendly systems.

BNY is dedicated to supporting the entire investment process that is reflected in the breadth and depth of product offerings and our commitment to client satisfaction every day. Their core services include trust and safekeeping, portfolio and fund accounting, global custody, middle office outsourcing, transfer agency, sub-accounting, cash management and security movement, participant services, securities lending, foreign exchange, hedge fund administration, performance measurement and analytics, clearing services, online information delivery, and support services for internal investment management.

4.4.3 If the Vendor subcontracts or delegates any of its obligations under a contract awarded pursuant to this RFQ, all of the mandatory requirements shall be met by the Vendor or its subcontractor, as appropriate. The Vendor shall remain fully responsible for complete performance of all of the Vendor's obligations set forth in this RFQ, and for any such third party's compliance with the provisions set forth herein. A proposal that includes Services provided by a Subcontractor is not considered a joint bid. See Section 3.12 and 3.13 to ensure subcontracts meet requirements.



#### Avenu acknowledges this requirement.

4.4.4 Insurance: Vendor shall maintain in full force and effect, with insurance companies of recognized responsibility, at its sole expense, insurance covering its work of the type and in amounts reasonably required by the STO or any resulting Contract, per the categories and amounts listed in the General Terms and Conditions document. Vendor's insurance shall, among other things, insure against loss or damage resulting from Vendor's performance of this Contract. All such insurance policies shall remain in full force in effect for the entire term of the Contract and shall not be canceled or changed except after 30 days written notice to the STO. The certificates of insurance are subject to approval by the STO and/or the WV Board of Risk and Insurance Management.

Avenu understands and accepts that we are to maintain in full force and effect, with insurance companies of recognized responsibility, at our sole expense, insurance covering our work and amounts as reasonably required by the STO.

4.4.4.1 Warranty: The Vendor shall warrant that it has examined its insurance coverage and has determined that the STO can be named as additional insured on Vendor's commercial general liability insurance without creating an adverse effect on the Vendor's coverage. Such additional insured requirement may be met through a blanket additional insured basis.

Avenu warrants that we have examined our insurance coverage and we have determined that the STO can be named as an additional insured on our commercial general liability insurance without creating an adverse effect on our coverage.

## **5 CONTRACT AWARD**

5.1 Contract Award: The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the Vendor that provides the Contract Services meeting the required specifications for the lowest overall total annual cost as shown on the Pricing Pages.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.

5.2 Pricing Page: Vendor should complete the Pricing Page by in accordance with the instructions on the pricing page. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.

## **6 PERFORMANCE**

Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.

## **7 PAYMENT**

Agency shall pay invoices monthly, in arrears, per the categories reflected on the Pricing Page for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.



7.1 Vendor must submit invoices either in hard copy or via email. The preferred payment methods by the State are either by EFT/ACH or state credit card. Invoices must match the name of the Vendor listed on the contract. Any variance of name or address information listed within the State's financial system or other business registrations will require supporting documentation to verify and/or may require the issuance of an administrative change order to the contract, or other updates to business registrations.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.

### 8 TRAVEL

Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.

## 9 FACILITIES ACCESS

Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:

- 9.1. Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
- 9.2. Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
- 9.3. Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
- 9.4. Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
- 9.5. Vendor shall inform all staff of Agency's security protocol and procedures.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.

## 10 VENDOR DEFAULT

- 10.1. The following shall be considered a vendor default under this Contract.
  - 10.1.1 Failure to perform Contract Services in accordance with the requirements contained herein.
  - 10.1.2 Failure to comply with other specifications and requirements contained herein.
  - 10.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.
  - 10.1.4 Failure to remedy deficient performance upon request.
- 10.2 The following remedies shall be available to Agency upon default.
  - 10.2.1 Immediate cancellation of the Contract.
  - 10.2.2 Immediate cancellation of one or more release orders issued under this Contract.
  - 10.2.3 Any other remedies available in law or equity.

Acknowledged. Avenu will adhere to STO's instructions as set forth above.



## 11 MISCELLANEOUS

11.1. Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Deborah Arnold Telephone Number: 617-722-9657

Fax Number: 617-722-9660

Email Address: Deborah.arnold@avenuinsights.com



## 12 WEST VIRGINIA MADATORY ATTACHMENTS

- A. PURCHASING AFFIDAVIT
- B. ADDENDUM ACKNOWLEDGEMENT FORM
- C. CONTACT & CERTIFICATION

## STATE OF WEST VIRGINIA Purchasing Division

## **PURCHASING AFFIDAVIT**

**CONSTRUCTION CONTRACTS:** Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

**ALL CONTRACTS:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

#### **DEFINITIONS:**

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

#### WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Avenu St S Holdings, LLC	
Authorized Signature:	Date: 01/24/24
State of VRGINIA	
County of FARFAX, to-wit:	
Taken, subscribed, and sworn to before me this 4 day of	, 2024.
My Commission expires  NOTARY PUBLIC REG # 8085084 MY COMMISSION EXPIRES 10/31/2027  NOTARY PUBLIC NOTARY PUBLIC	Purchasing Affidavit (Revised 01/19/2018)

# ADDENDUM ACKNOWLEDGEMENT FORM SOLICITATION NO.: CRFQ STO240000003

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

	-,	iain roccivo	ox next to each adder	(Check the b
Addendum No. 6	]	[	Addendum No. 1	[x]
Addendum No. 7	]	[	Addendum No. 2	[ ]
Addendum No. 8	]	[	Addendum No. 3	[ ]
Addendum No. 9	1	ſ	Addendum No. 4	[ ]

Addendum Numbers Received:

(Check the box next to each addendum received)

Addendum No. 5

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

[ ] Addendum No. 10

Avenu SLS Holdings, LLC

Company

Authorized Signature

01/24/24

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Deborah Arnold	
(Printed Name) Director, Unclaimed Property	
(Printed Title) 100 Hancock Street, 10th Floor, Quincy MA 02171	
(Address) 617-722-9657	
(Phone Number) / (Fax Number) Deborah.Arnold@avenuinsights.com	
(email address)	

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Avenu SLS Holdings, LLC	
(Company)	
(Authorized Signature) (Representative Name, Title)	
James Barkman, Chief Financial Officer	
(Printed Name and Title of Authorized Representative)	
January 29, 2024	
(Date)	
617-722-9660	
(Phone Number) (Fax Number)	



## 13 AVENU EXHIBITS

- 1. CUSTODY CLIENT LIST
- 2. ADDITIONAL PERSONNEL RESUMES
- 3. NEXEN® REFERENCE GUIDE
- 4. EXTRANET REFERENCE GUIDE
- 5. AVENU REPORTS
- 6. SOC1 AND SOC2 REPORTS CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE
- 7. BUSINESS CONTINUITY PLAN CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE
- 8. DISASTER RECOVERY PLAN CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE

**Custody Client List** 

## Avenu Custody Client List

Provided Custody Services: 1990 - present



Alabama Office of the State Treasurer Arizona Department of Revenue Unclaimed Property Unit Unclaimed Property Division Chad Wright, CPM Will Nagel Administrator Director, Unclaimed Property Division PO Box 302520 1600 W. Monroe Phoenix, AZ 85007 Montgomery, AL 36130 334.353-3627(phone) 602.716.6033 (phone) Chad.Wright@treasury.alabama.gov wnagel@azdor.gov Provided Custody Services: 1990 - present Provided Custody Services: 2016 - present Connecticut Office of the State Treasurer Delaware Department of Finance Unclaimed Property Division Division of Revenue, Unclaimed Property - Escheat Michelle Seagull, Assistant Treasurer Office of the State Treasurer Brenda R. Mayrack Second Injury Fund & Unclaimed Property Director, Office of Unclaimed Property 165 Capitol Avenue Carvel Street Office Building, 8th Floor Hartford, CT 06106 820 N. French Street Wilmington, DE 19801 860.702.3125 (phone) michelle.seagull@ct.gov 302.577.8691 (phone) Brenda.Mayrack@delaware.gov Provided Custody Services: 1994 - present Provided Custody Services: 1995 - present District of Columbia Office of Finance and Florida Department of Financial Services Treasury, Unclaimed Property Unit Bureau of Unclaimed Property Liz Tatum, Financial Administrator Lynn Hall, Manager 1101 4th Street, SW, Suite 800B Washington, DC 20024 Division of Unclaimed Property Office of Chief Financial Officer Jimmy Patronis Florida Department of Financial Services 202.442.8193 (phone 850-413-5623 (phone) Jynn.hall@dc.gov Elizabeth.Tatum@MyFloridaCFO.com Provided Custody Services: 1990 - present Provided Custody Services: 2009 - present lowa Treasurer of State Office of the Kansas State Treasuer Unclaimed Property Division Karen Austin Jessica Schleif Chief of Staff Holder Reporting 321 E 12<sup>th</sup> Street 1<sup>st</sup> Floor 900 SW Jackson, Suite 201 Topeka, KS 66612 Des Moines, Iowa 50319 515.281.7677 (phone karen.austin@tos.iowa.gov 785.291.3174 (phone) Jessica@treasurer.ks.gov Provided Custody Services: 2019-present Provided Custody Services: 2009- Present Indiana Attorney General's Office Unclaimed Property Division Amy T. Hendrix Director of Unclaimed Property Division P.O. Box 2504 Greenwood, IN 46142 317.883.4521 (phone) Amy.hendrix@atg.in.gov

## Avenu Custody Client List



Office of Kentucky State Treasurer Unclaimed Property Division

Katrina Stoner Branch Manager Unclaimed Property Division 1050 US Hwy 127 South, Suite 100 Frankfort, KY 40601

800.465.4722 (phone) Katrina.stoner@ky.gov

Provided Custody Services: 2019- present

Michigan Department of Treasury Unclaimed Property Division

Terry A. Stanton State Administrative Manager for Unclaimed Property PO BOX 30756 Lansing, MI 48909

517.636.5307 (phone) stantont@michigan.gov

Provided Custody Services: 1990 - present

Massachusetts Lottery Commission

Kevin M. Player Comptroller 60 Columbian Street Braintree, MA 02184

781-849-5651 (phone) kplayer@masslottery.com

Provided Services: 2012 - present

Missouri State Treasurer's Office Missouri Unclaimed Property Division

Scott Harper Director of Unclaimed Property P.O. Box 210 Jefferson City, MO 65102

573.751.2082 (phone)
Scott.harper@treasurer.mo.gov
Provided Custody Services: 2019 - present

New York Office of the State Comptroller Office of Unclaimed Funds

Kelly Kuracina Assistant Bureau Director Office of the State Comptroller 110 State Street, 8th Floor Albany, NY 12236

518.474.6049 (phone) kkuracina@osc.state.ny.us

Provided Custody Services 2016- present

Montana Department of Revenue Miscellaneous Tax Unit

Tracy Morano Bureau Chief, Unclaimed Property Sam W. Mitchell Building 125 N. Roberts Street, 3rd Floor Helena, MT 59620

406.444.4008 (phone) TMorano@mt.gov

Provided Custody Services: 1990 - present

Maine State Treasurer's Office Unclaimed Property

Jeff Chetkauskas Ass. Director of Internal Operations 39 State House Station 111 Sewall Street, 3rd FL Augusta, ME 04333-0039

207.624.7476 (phone)
Jeff.Chetkauskas@maine.gov

Provided Custody Services: 1990 – present

Massachusetts Treasury Cash Management
Insurance Account

Nina Hollien Asst. Director of Cash Management Operations Office of the State Treasurer One Ashburton Place Boston, MA 02108

617-367-9333 x419 (phone) scott.a.blois@tre.state.ma.us

Provided Services: 2012 - present

Nevada Office of the State Treasurer Unclaimed property Division

Danielle Anthony Deputy Treasurer 555 East Washington Ave, Suite 5200 Las Vegas, NV 89101

702.486.4354 (phone)

Itobin@nevadatreasurer.gov

Provided Custody Services: 2006 - present

New Mexico Taxation and Revenue Department Unclaimed Property Unit

Stephanie Dennis, Supervisor 1200 South St. Francis Drive P.O. Box 25123 Santa Fe, NM 87504-5123

505.827.0762 (phone)

stephanie .dennis@state.nm.us

Provided Custody Services: 1990 - present

## Avenu Custody Client List



State of New Hampshire Treasury Abandoned Property Division

James R. Karas Abandoned Property Director 25 Capitol Street, Room 205 Concord, NH 03301

603.271.1499 (phone) james.karas@treasury.nh.gov

Provided Custody Services: 1998 - present

Oregon State Treasury

Unclaimed Property Program

Claudia Ciobanu Trust Property Director 775 Summer Street NE, Suite 100 Salem, OR 97301

503.986.5248 (phone) Claudia.Ciobanu@ost.state.or. us

Provided Custody Services: 2015 - present

Puerto Rico Office of the Commissioner of Financial Institutions, Unclaimed Property Division

Salva D. Valentin Maldonado Edif. Centro Europa, Suite 600 Ponce de Leon #1492 San Juan, PR 00907-4127

787.723.3131 (phone) salvad@ocif.pr.gov

Provided Custody Services: 2005 - present

South Carolina's Treasurer's Office

Dayle DeLong, Senior Assistant State Treasurer 1200 Senate Street – Suite 214 Wade Hampton Building Columbia, SC 29201

803-734-2683 (phone)
Dayle.DeLong@sto.sc.gov

Provided Custody Services: 2022 - present

Tennessee State Treasury Department Unclaimed Property Division

John Gabriel, Director Andrew Jackson Building 10th Floor Nashville, TN 37243-0242

615.253.5354 (phone) john.gabriel@tn.gov

Provided Custody Services: 1990- present

Office of the Vermont State Treasurer Unclaimed Property Division

Al LaPerle, Coordinator Pavilion Building 109 State Street, 4th Floor Montpelier, VT 05609-6200

802.828.2318 (phone) al.laperle@vermont.gov

Provided Custody Services: 2005 - present

Virginia Department of the **Tr**easurer Unclaimed Property Division

Bradley Earl, Director 101 North 14th Street James Monroe Building 3rd Fbor Richmond, VA 23219

804.225.2515 (phone) melinda.barbish@trs.virginia.gov

Provided Custody Services: 1998 - present

Government of the Virgin Islands
Department of Property and Procurement
Office of the Lieutenant Governor

Tregenza A. Roach, Esq. Lieutenant Governor 8201 Sub Base, 3rd Floor St. Thomas, U.S. Virgin Islands 00802

Custody Services: Starting in 2023

Wisconsin Department of Revenue Unclaimed Property Unit

Erin Egan Director, Bureau of Tax Operations 2135 Rimrock Road 6-40 Madison, WI 53713

608.261.5235 (phone) erinb.egan@revenue.wi.gov

Provided Custody Services: 1990 - present

West Virginia **S**tate **Tr**easurer's Office Unclaimed Property Division

Abigail Campbell Receipts Manager Unclaimed Property 322 70th Street SE Charleston WV, 25305

304.340.2711 (phone) abigal.campbell@wvsto.com

Provided Custody Services: 2016 - present

## Additional Personnel Resumes



## Additional Personnel Resumes for Avenu's Client Custody Team

Additional members of Avenu's team available to the STO are listed below. Avenu's team is always available to assist the STO with any and all services.

Margaret A. Wagner, Client Services Professional I With Avenu since 2010

Margaret "Peg" Wagner is a Senior Account Manager responsible for the daily customer support of state clients as well as the overall management of their portfolios.

Peg also administers mutual fund and DRP processing transactions for several custody clients. These transactions include but are not limited to account transfers, account consolidations securities liquidations, re- registration requests, reconciliations.

Prior to joining Avenu, Peg held positions within the transfer agent industry for more than 20 years. She held steadily progressive positions at Computershare as a Business Unit Team Leader, a Technology Services Team Leader, a Systems Conversion Analyst and a Business and Product Support Analyst.

Peg brings a wealth of transfer agency experience, expertise, and leadership to her role at Avenu, strengthening the Unclaimed Securities Custody team and benefiting Avenu's custody clients with her contacts and knowledge base.

Laura Maci, Client Services Professional I With Avenu since 2001 – Quincy MA

Laura is an Account Manager within the Unclaimed Securities Custody team responsible for the management of several state client relationships. She provides daily support coordinating the sale, receipt, transfer and reconciliation of securities, claims processing, research, problem resolution and other tasks related to all daily/monthly processes within unclaimed property.

Laura joined Avenu in 2001 starting her career as a manager in the Delivery Department where she compiled documentation needed for the initial delivery and future delivery of securities to states. Her expertise lies in DTC, physical certificates and DRP/MF statements.

Laura progressed to the Unclaimed Securities Custody team based on her strong knowledge and background. Laura has been with Avenu since September of 2001 and provides daily assistance for clients to support their unclaimed property program and reconciliation of securities and Mutual Funds from holder. She coordinates the sale of securities, claim processing, research and problem resolution.

Laura earned a bachelor's degree in Finance & Accounting in 1984 from Tirana University, Albania.

Les Chan, Customer Care Associate IV With Avenu since 2019 – Quincy, MA

Les Chan is a Customer Care Associate responsible for the daily support of state clients, handling mutual fund transactions as well as serving as the backup resource for several operational functions. Additional services handled by Les include corporate actions, receipt and reconciliation of securities from holders, sale of securities and claim processing money movement and problem resolution.



Les has excellent customer service skills and maintains collaborative professional relationships and rapport with team members, state contacts, outside vendors, brokerage contacts and transfer agents. Les has a securities industry background and shares that knowledge and experience to strengthen the Custody Team.

Les worked in financial services for 30 years with a national firm, holding roles in customer service, brokerage trading, legal support, problem resolution and legal operations. Before joining the Avenu team, Les spent the preceding 9 years as a Senior Legal Operations Analyst.

Les holds a BS degree in Marketing/Economics from Boston College.

Robinson Joachin, Client **Ser**vices **A**ssociate With Avenu since 2022- Quincy, MA

Robinson Joachin is an Account Manager within the Unclaimed Securities Custody team responsible for the management of several state client relationships. He provides daily support coordinating the sale, receipt, transfer and reconciliation of securities, claims processing and research. He is currently the account administrator for three states.

Robinson's background includes trading financial markets. He facilitated the opening of self-directed trading accounts through rollovers, transfers or withdrawals from several types of retirement accounts including 401k, 403B and 457B. Robinson is a customer-centered, professional with demonstrated analytical abilities.

Robinson uses his problem-solving skills to ensure satisfaction, exceptional written and verbal communication skills with strong telephone etiquette. He has proven organizational skills with the ability to multitask and adapt in a rapidly changing and fast-paced environment.

Borana Pjetri, Client **S**ervices **A**ssociate III With Avenu since May 2023

Borana Pjetri is a Client Service Associate III of Avenu's Unclaimed Securities Custody group and is responsible for the management of several state client relationships. She provides daily support coordinating the sale, transfer and reconciliation of securities, and other tasks related to all daily/monthly processes within unclaimed property.

Borana has excellent customer service skills and maintains collaborative professional relationships from previous experiences in the banking and financial industry. She has strong interpersonal, organizational and communication skills.

Prior to joining Avenu, Borana's background consists of over 10 years of customer service experience in banking sector, Human Resources and Financial Services.

Borana holds a Bachelor of Science degree in Finance & Accounting and a Bachelor of Science degree in Mathematics from the University of Tirana, Albania.



## **M**elissa Cea**r**lock, **S**olutions Consultant With Avenu since 2004

With Avenu since 2004, Melissa now serves as Avenu's Systems Project Manager and Training Coordinator. Her duties include training, documentation, updates, and customized solutions to all workplace needs surrounding unclaimed property processing.

Melissa serves as the Product Owner for Avenu | Connect and was instrumental in bringing the product to market. Melissa provides technical expertise in identifying, evaluating, and developing systems and procedures that are cost effective and meet a wide variety of end-user requirements.

Prior to coming to Avenu, Melissa worked for the Illinois State Treasure's Unclaimed Property office. Over the years holding the title of Holder Reporting Manager, Claims Manager and Securities Manager. This gave her the ability to join Avenu with a strong understanding of the intricacies of Unclaimed Property

Melissa is a veteran of the United States Navy, holds a B.S. in Informational Technology Management and Management from Kaplan University, Florida.

## NEXEN® Reference Guide



# NEXEN® Reference Guide

Request Trades and Monitor Transactions of Your Unclaimed Securities Portfolio Online

### September 2021







## **Preface**

NEXEN® is The Bank of New York Mellon's ("BNY Mellon") internet-based product, which is available 24 hours a day, 7 days a week. The NEXEN® portal is a digital platform that requires no extra software to be installed. Each user is set up with access only to their particular state and is assigned their own unique ID and password.

Avenu Insights & Analytics uses NEXEN® to input transfer requests, security deposits, liquidations, check deposits, and cash withdrawals on your behalf. As a result, the state can use NEXEN® to review all activity and monitor the status of all the transactions in real time. States have view only access and can review transactions, balances, positions and have access to robust reporting capabilities.

©2021 Avenu Insights & Analytics, LLC. All rights reserved. Avenu® and Avenu and Design® are trademarks of Avenu Insights & Analytics, LLC. in the United States and/or other countries.

The contents of this manual are considered to be Avenu private data and are provided for the exclusive use of the state. The contents herein may not be reproduced without the specific written permission of Avenu Insights & Analytics, LLC. This document is for informational purposes only and does not constitute a contract or an offer to contract.

NEXEN® is a product of The Bank of New York Mellon.

Document Version: 5.1 (Sept 2021, Avenu Insights & Analytics, LLC.)





## **Table of Contents**

## Contents

NEXEN® Homepage	3
NEXEN® Reporting	
Custody Positions	
1. Custody Holdings	
Custody Valuation	
Custody Variation     Custody Security Transactions	
Cash Reporting	
Settled Cash Statements	
Settled Cash Balances	
Cash & Security Transactions	
Cash Inquiry	

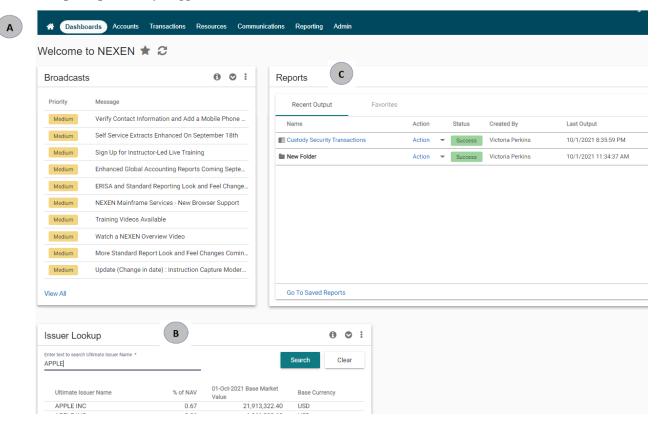




# NEXEN® Homepage

State clients will have authorized access to NEXEN<sup>®</sup>. This is the same reporting system that Avenu uses. When a user logs in they are directed to the NEXEN home page and dashboard (shown below). This dashboard can be customized by adding different components (widgets) based on client preferences. The homepage can also show recent output which reflects reports generated by the user in the last 10 days.

Users can run a report from the Homepage by clicking on the report name or they can open and edit parameters and run and view output. Users can also display a list of favorite reports by selecting the additional tab. This quick view also allows the user access to run reports previously flagged.

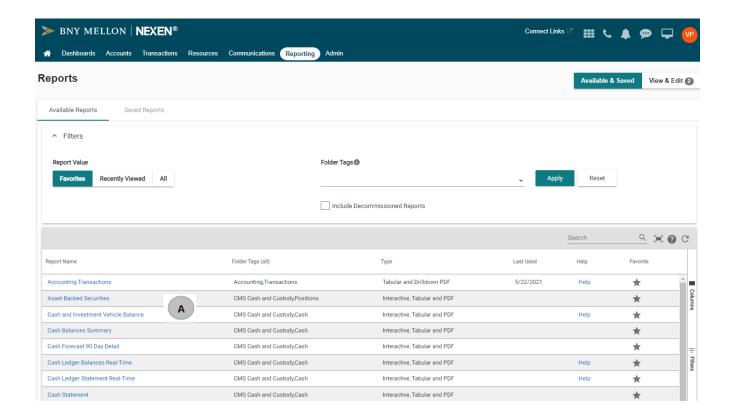


- A Reporting Options Tool Bar
- B Market Reference Lookup Prior Day Market Value
- c Reporting Quick View and Process Recent Output or Favorites



# **NEXEN®** Reporting

Clients will have full access to eReporting on NEXEN $^{\circledR}$ . As an additional tool for performing inquiries, eReporting will enhance the state's ability to obtain information about their account . You will be able to view, run, schedule and save as well as view and save in multiple formats, automatically distribute or share with other members of your team. Shown below is a small sample of some of the reports available.



A Commonly Used Reports - Favorites



## **Custody Positions**

NEXEN<sup>®</sup> provides many reports to assist the states to track the positions that they are holding. Some examples of reporting capabilities below:

### 1. Custody Holdings

This report provides the status of any shares that the state is holding. Either the entire portfolio at once or individual share positions by security. It shows both pending shares and settled shares and can provides the location of each position. These features allow the state to have a clear idea as to the availability of the shares.

	E N U			В		y - Details B	gs y Status			
99999 - AUZF S	TATE OF XXXXXXXX					10/4/2021				
ISIN	Description	Ccy	Ctry Inc	Status	Loc	Reg	Traded Shares/Par Amortized Face	Settled Shares/Par	Pending Receive Shares / Par	Pending Delive Shares/Pa
US20461S1087	COMPOSITE TECHNOLOGY CORP USD 0.001	USD	US	AVAILABLE	NIE A	NIB8	16,250.0000	16,250.0000		
US2057503003	COMSTOCK MNG INC USD 0.000866	USD	US	AVAILABLE	DTC	DTC	c 2.0000	2.0000		D
US2057634022	COMSTOCK P COMSTOCK CAPITAL VALUE F	USD	US	AVAILABLE	MUT	MAC		100.3370		100.337
US2058182062	COMTEC INT COM USD0.001	USD	US	AVAILABLE	DTC	DTC	157,344.0000	157,344.0000		
US2058262096	COMTECH TELECOMMUNICATIONS USD 0.1	USD	US	AVAILABLE	DTC	DTC	67.0000	67.0000		
US2058871029	CONAGRA BRANDS INC	USD	US	TOTAL			531.6630	531.6630		
				AVAILABLE AVAILABLE	DTC NIB	DTC NIB8	430.0000 101.6630	430.0000 101.6630		
US20602D1019	CONCENTRIX CORP USD 0.0001	USD	US	AVAILABLE	DTC	DTC	132.0000	132.0000	В	
US2065141010	CONCORDE G COM USD.01	USD	US	AVAILABLE	DTC	DTC	8,800.0000	4,400.0000	4,400.0000	
US2067871036	CONDUENT INC USD 0.01	USD	US	AVAILABLE	DTC	DTC	102.0000	102.0000		
US2068274040	CONECTISYS CORP USD 0.001	USD	US	TOTAL			2.0000	2.0000		
				AVAILABLE	DTC	DTC	1.0000	1.0000		
				AVAILABLE	NYV	HARE	1.0000	1.0000		
US2071461014	CONNEXUS CORP USD 0.001	USD	US	AVAILABLE	DTC	DTC	1.0000	1.0000		
US20752L1017	CONNECTAJET COM INC USD 0.5	USD	US	AVAILABLE	DTC	DTC	8,500.0000	8,500.0000		
US20786W1071	CONNECTONE BANCORP INC NEW NPV	USD	US	AVAILABLE	DTC	DTC	110.0000	110.0000		
US2082548627	CONOLOG CORP USD 0.01	USD	US	AVAILABLE	DTC	DTC	5.0000	5.0000		
US20825C1045	CONOCOPHIL COM USD0.01	USD	US	AVAILABLE	DTC	DTC	1,732.0000	1,732.0000		
US2088922081	CONSOLIDATED CAP NO USD 0.0001 144A	USD	US	AVAILABLE	DTC	DTC	180,000.0000	180,000.0000		

- A Sorted by Location Where Securities are Held and Shows Total Shares for Each
- B Shows Pending Trades (Delivery and Receipt)
- c Total Share Amount for Traded and Settled Positions
- Shows Pending Shares

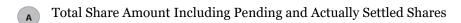


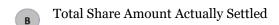


### **Custody Holdings Continued**

The last page of the report will show the total units held as well as the total pending shares.

A V E	N U				Cu	stody Hold	ings		Re	port ID: ICUS0016
INSIGNTS & AN				В	y Securi	ity - Details	By Status			
99999 - AUZF ST	ATE OF XXXXXXXXXX					10/4/2021				
ISIN	Description	Ссу	Ctry Inc	Status	Loc	Reg	Traded Shares/Par Amortized Face	Settled Shares/Par	Pending Receive Shares / Par	Pending Deliver Shares/Par
US98986T1088	ZYNGA INC USD 0.000006	USD	US	AVAILABLE	DTC	DTC	115.0000	115.0000		
US99VVA4JB76	XO HOLDINGS CVR	USD	US	AVAILABLE	NIB	NIB8	1,084.0000	1,084.0000		
US99VVA9UU16	GOLDEN PACIFIC BANCORP INC	USD	US	AVAILABLE	NYV	NAME	130.0000	130.0000		
USDEE4374016	FONAR CORP NEW 100,000TH FRA	CUSD	US	AVAILABLE	DTC	DTC	25,107.0000	25,107.0000		
USJBH84E1067	FRAC SEVEN HILLS RLT	USD	US	AVAILABLE	DTC	DTC	37,081.0000	37,081.0000		
USMM001UBSC8	INDONESIAN DIAMOND COR	USD	US	AVAILABLE	NIB	NIB8	360.0000	360.0000		
USMM001V1KV9	TMC PROPERTIES P+I UNSECURED NOTE	OUSD	US	AVAILABLE	NIB	NIB8	180,000.0000	180,000.0000		
USMM001VNDE9	AEI NET LEASE INCOME + GROWTI FD XX	HUSD	US	AVAILABLE	NIB	NIB8	5.0000	5.0000		
USN070592100	ASML HOLDING NV EUR 0.09	USD	NL	AVAILABLE	DTC	DTC	255.0000	255.0000		
VGG041JN1065	ANTELOPE ENTERPRISE HLDGS LTD	USD	VG	AVAILABLE	DTC	DTC	4.0000	4.0000		
VGG1890L1076	CAPRI HOLDINGS LTD	USD	VG	AVAILABLE	DTC	DTC	6.0000	6.0000		
VGG639071023	NAM TAI PROPERTY INC USD 0.01	USD	VG	AVAILABLE	DTC	DTC	488.0000	488.0000		
VGG7996N1298	SEFTON RES NPV	GBP	VG	AVAILABLE	DTC	DTC	50,000.0000		50,000.0000	
VGG843851061	CHINA TECHNOLOGY GLOBAL CORP NPV	USD	VG	AVAILABLE	DTC	DTC	20,000.0000	20,000.0000		
VGG9160X1078	UMEWORLD LTD USD 0.0001	USD	VG	AVAILABLE	DTC	DTC	1,600.0000	1,600.0000		
ZAE000259701	SIBANYE STILLWATER LTD NPV	ZAR	ZA	AVAILABLE	YZA	YZA8	3.0000	3.0000		
ZAU000013799	AU MIN AFRICA PTY LTD NPV	USD	ZA	AVAILABLE	DTC	DTC	4,000.0000	4,000.0000		
	TOTA	L BY U	NITS - 91	9999 - AUZF ST	ATE OF X	xxxxx	306,883,479.8463	306,098,707.5457	816,053.5630	31,281.2624
	TOTAL BY AMOR	TIZED F	ACE - 9	9999 - AUZF ST	ATE OF X	OXXXXXX	24,432.7172	В		
10/4/2021 8:33:52	PM EDT				Page	266 of 266				









### 2. Custody Valuation

Like Custody Holdings, the Custody Valuation Report will also display the state's positions. In addition, this report will detail the share price and market value for each security. Pending and settled shares are separated into two reports. This report runs in real time too.

The following pages are examples of the above reports as seen on NEXEN®.

### **Custody Valuation - Entire Portfolio**

A V E N U					ody Valuation Asset Type		Rep	Report ID: ICUS0017 porting Currency: USD
	TATE OF XXXXXXXXX				Basis - 10/12/2021			
ISIN	Description	Ctry	Loc	Ccy	Units	Local Price	Market Value Local	Market Value Reporting Currency
					Amortized Face			
EQUITIES			В					
AUSTRALIAN DO	DLLAR ( Exchange Rate : 0.7357500000)							
AU000000LSA2	LACHLAN STAR LTD NPV	AU	YAS	AUD	40,000.0000	0.030000	1,200.00	882.90
CANADIAN DOLL	AR ( Exchange Rate : 0.8028580000)							
CA0115321089	ALAMOS GOLD INC NEW NPV	CA	DTC	CAD	3.0000	9.500000	28.50	22.88
CA0585861085	BALLARD PWR SYS INC NEW NPV	CA	DTC	CAD	22.0000	18.630000	409.86	329.06
CA17178G1046	CIELO WASTE SOLUTIONS CORP NPV	CA	DTC	CAD	16.0000	0.485000	7.76	6.23
CA21922J6043	CORNERSTONE CAP RES INC NPV	CA	DTC	CAD	10,000.0000	3.920000	39,200.00	31,472.04
CA2926717083	ENERGY FUELS INC NPV	CA	DTC	CAD	25.0000	9.320000	233.00	187.07
CA3805561006	GOLD BULL RES CORP NPV	CA	DTC	CAD	272.0000	0.215000	58.48	46.95
CA56501R1064	MANULIFE FINL CORP NPV	CA	DTC	CAD	5,307.0000	24.640000	130,764.48	104,985.33
CA68827L1013	OSISKO GOLD ROYALTIES LTD NPV	CA	DTC	CAD	367.0000	14.710000	5,398.57	4,334.29
CA74346M1095	PROMIS NEUROSCIENCES INC NPV	CA	YCA	CAD	89,000.0000	0.185000	16,465.00	13,219.06
CA74762L1067	QUANTITATIVE ALPHA TRADING INC NPV	CA	DTC	CAD	80.0000	0.009779	0.78	0.63
CA8911605092	TORONTO DOMINION BK ONT NPV	CA	DTC	CAD	14.0000	85.690000	1,199.66	963.16
CA89621C1059	TRILOGY METALS INC NEW NPV	CA	DTC	CAD	8.0000	2.330000	18.64	14.97
CA9774861095	WI2WI CORP NPV	CA	YCA	CAD	187,500.0000	0.050000	9,375.00	7,526.80
JE00BWH5YF45	ROYAL ROAD MINERALS LTD NPV	JE	YCA	CAD	8.0000	0.260000	2.08	1.67
	TOTAL BY UN				292,622.0000		203,161.81	163,110.14
A	TOTAL BY AMORTIZED FA	ACE - CA	ANADIAN	DOLLAR	0.0000			
EURO ( Exchange	e Rate: 1.1549000000)							
CA7507581048	RAILPOWER COM NPV	CA	YCA	EUR	200.0000	0.000431	0.09	0.10
CA8584971003	STELAX INDS LTD NPV	CA	DTC	EUR	75,020.0000	0.005500	412.61	476.52
DE0007100000	DAIMLER AG NPV	DE	DTC	EUR	1.0000	82.310000	82.31	95.06
US3838701023	GPS INDUST COM USD0.01	US	DTC	EUR	54,264.0000			
A		TOTAL	BY UNITS	- EURO	129,485.0000		495.01	571.68
A	TOTAL BY	AMORTI	ZED FACE	- EURO	0.0000			
HONG KONG DO	LLAR ( Exchange Rate : 0.1285220000)							
BMG524181036	KERRY LOGISTICS NETWORK LTD HKD 0.5	ВМ	YHK	HKD	125.0000	18.380000	2.297.50	295.28
BMG524401079	KERRY PROPERTIES LTD HKD 1.0	BM	YHK	HKD	250.0000	22.000000	5,500.00	706.87
HK0008011667	PCCW LTD NPV	HK	YHK	HKD	5.0000	4.000000	20.00	2.57
	TOTAL BY UNIT	S - HON	IG KONG	DOLLAR	380.0000	_	7.817.50	1,004,72
	TOTAL BY AMORTIZED FAC	E - HON	IG KONG	DOLLAR	0.0000		,,,,,,,,,	.,
UNITED STATES	DOLLAR ( Exchange Rate : 1.0000000000)							
BMG3156P1032	ASA GOLD A COM STK NPV USD	BM	DTC	USD	201.0000	20.070000	4.034.07	4.034.07
BMG9618F1075	WHITE MOUNTAINS INSURANCE G USD 1.0	BM	DTC	USD	1.0000	1.087.990000	1.087.99	1,087,99

- A Sorted by Asset Type
- B Location of Shares





## Custody Valuation Continued – Entire Portfolio

AVE	N U				Valuation set Type		Rep	Report ID: ICUS0017 orting Currency: USD
999999 - AUZF S1	ATE OF XXXXXXXXXXXXX			1.0	sis - 10/12/2021			
ISIN	Description	Ctry	Loc	Ссу	Units	Local Price	Market Value Local	Market Value Reporting Currency
100000000000000000000000000000000000000		110	DEC	1100	Amortized Face	-0.010000		40.000.00
US98850P1093	YUM CHINA HLDGS INC USD 0.01	US	DTC	USD	223.0000	58.340000	13,009.82	13,009.82
US9888501031	ZAHAV INC	US	DTC	USD	4.0000	0.000017	7.33	m 00
US98986T1088 X9X9USDDGCM3	ZYNGA INC USD 0.000006 DREYFUS GOVT CM INST 289	US	GSF	USD	1.0000	7.330000	12.277.04	7.33 12.277.04
X9X9USDDGCM3		10.507700				1.000000		
	TOTAL BY UNITS -	UNITED	STATES	DOLLAR	3,806,666.5720		12,656,311.61	12,656,311.61
	TOTAL BY AMORTIZED FACE -	UNITED	STATES	DOLLAR	0.0000			
	TO	TAL BY	UNITS -	EQUITIES	4,269,153.5720		-	12,821,881.05
	TOTAL BY AMO	ORTIZED	FACE -	EQUITIES	0.0000			
MISC DEBT								
UNITED STATES	OOLLAR ( Exchange Rate : 1.0000000000)							
US09625U1097	BLUEKNIGHT ENERGY PARTNERS L P	US	DTC	USD	21.0000	3.250000	68.25	68.25
US29273V1008	ENERGY TRANSFER LP	US	DTC	USD	483.0000	9.900000	4,781.70	4,781.70
US2937921078	ENTERPRISE COM UNITS REP LIM PART I	US	DTC	USD	1.0000	23.990000	23.99	23.99
US4511001012	ICAHN ENTERPRISES L P	US	DTC	USD	393.0000	54.700000	21,497.10	21,497.10
	TOTAL BY UNITS -	UNITED	STATES	DOLLAR	898.0000	_	26,371.04	26,371.04
	TOTAL BY AMORTIZED FACE -	UNITED	STATES	DOLLAR	0.0000			
	тот	AL BY U	INITS - MI	SC DEBT	898.0000		_	26,371.04
	TOTAL BY AMOR	TIZED	FACE - MI	SC DEBT	0.0000			
	TOTAL BY UNITS - ACCOUNT 999999 - A	UZF ST	TATE OF	XXXXXXX	4,270,051.5720	A	В	12,848,252.09
TOTAL	BY AMORTIZED FACE - ACCOUNT 999999 - A	UZF ST	TATE OF	XXXXXXX	0.0000			

- A Total Share Amount for Settled Shares
- B Total Market Value for Securities Held as of Report Date



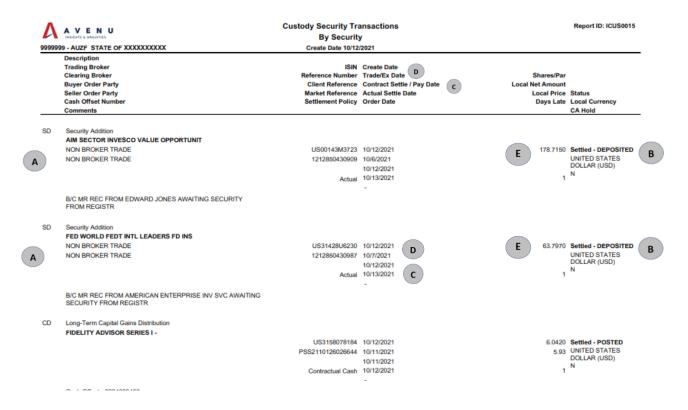


### 3. Custody Security Transactions

NEXEN® is a useful tool for the state in obtaining the status of transfers, deposits, sales, and even corporate actions.

This report gives the state the flexibility of obtaining any transactions that have settled or are pending in the account. The transactions can be obtained as of a specific date, within a specific date range or real time. The data is kept for 24 months.

The following pages are examples of the above report as seen on NEXEN®.



- A Report is Sorted by Transaction Type (SD, CD, CA, DV, B, etc.)
- B Location of Settlement
- c Settle Date
- Trade Date
- E Shares Settled





### **Cash Reporting**

NEXEN® provides various reports for cash:

#### **Settled Cash Statements**

The Settled Cash Statement report is a high-level view of trade and settlement date holdings by location for a selected date range (real-time and historical). It shows all asset types, including cash investment vehicles referred to as sweeps. In contrast, the Projected Cash Statement report shows current day and up to five future business days.

#### **Settled Cash Balances**

The Settled Cash Balances report provides beginning and ending balances, net activity, exchange rate and location information for the point in time date (real time or historical) selected. It shows all cash types, including cash investment vehicles referred to as sweeps and free delivery / receipt transactions.

#### **Cash and Security Transactions**

The Cash and Security Transactions report is a high-level view that shows all of the cash and custody activity together. Related cash and custody transactions are grouped together. This report's design allows you to search for information based on cash or custody specific activities. It shows all transaction types, including cash investment vehicles, referred to as sweeps. This report can be run in Real-Time and for historical transactions for the last two years.

### **Cash Inquiry**

The Cash Inquiry report provides a high-level view that displays all of the cash, custody and user-entered net settlement adjustments activity. You can filter for information based on cash or net settlement adjustment specific activities. It shows all transaction types and can be run in real-time, previous day and five future business days.

The following pages are examples of the above reports as seen on NEXEN®





### **Settled Cash Statements**

Δ	A V E N U	All Balances	Settled Cash S - Consolidate Cash		counts	Reportin	Report ID: ICAS0010 ng Currency: USD
999999	AUZF STATE OF XXXXXXXX		9/30/2021 - 9/3				
Tran Type	Description Trading Broker Clearing Broker		ISIN Reference Number Client Reference Event ID	Trade / Ex Date Settle / Pay Date Cash Post Date Cash Value Date	Shares/Par Amortized Units Local Price/Rate Local Principal Local Income	Local Amount	Reporting Equivalent
			Settlement Policy				
A	Dividend ARES CAP CORP USD 0.001 Gross: 199.67 RecDte: 9/15/2021		US04010L1035 PSS2109146186720	9/14/2021 9/30/2021 9/30/2021 9/30/2021	487.0000 0.4100000000	199.67	199.67
•			0212854553 Contractual Cash		199.67		
DV	Dividend  BECTON DICKINSON + CO USD 1.0  Gross: 88.81 RecDte: 9/9/2021	A	US0758871091 PSS2109076134951	9/8/2021 9/30/2021 9/30/2021 9/30/2021	107.0000 0.8300000000	88.81	88.81
			0212832586 Contractual Cash	515012021	88.81		
DV	Dividend BLACKROCK SBI USD0.001		US09249E1010	9/14/2021 9/30/2021	737.0000	54.98	54.90
	Gross: 54.98 RecDte: 9/15/2021		PSS2109146224123	9/30/2021 9/30/2021	0.0746000000	A	
			0215044514 Contractual Cash		54.98		
οV	Dividend CDK GLOBAL INC		US12508E1010	8/31/2021 9/30/2021	36.0000	5.40	5.40
	Gross: 5.40 RecDte: 9/1/2021		PSS2108306201600	9/30/2021 9/30/2021	0.1500000000		
			0214048405 Contractual Cash		5.40		

- A Details by Transaction
  - Transaction Type
  - Security Name
  - Security ID
  - Share Amount
  - Rate and Cash Received





### **Settled Cash Balances**

#### Report ID: ICAS0008 **Settled Cash Balances** A V E N U Reporting Currency: USD All Balances - Consolidate Cash and Sweep - All Accounts 9/30/2021 - 9/30/2021 Net Activity Local 2,958.33 2,996.00 Period Summary UNITED STATES DOLLAR (USD) AUZF STATE OF XXXXXXXXX - 999999999 9/30/2021 26 7,377.33 7,866.44 1.0000000000 7,377.33 489.11 7,866.44 26 7,377.33 489.11 7,866,44 7,377.33 489.11 BACK VALUED AMOUNT Α TOTAL CASH AND SWEEP 10,339.34 523.39 10,862.73 В

AVENU				Settled Cash Balar			Papartir	Report ID: ICAS0008
999999 - AUZF STATE OF	xxxxxxx	•	All Balances - Cons	9/30/2021 - 9/30/202	•	ints	Reportii	ig Currency. USD
Date	Count	Beginning Balance Local	Net Activity Local	Ending Balance Local	Exchange Rate Reporting Currency	Beginning Balance Reporting Currency	Net Activity Reporting Currency	Ending Balance Reporting Currency
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00
NEW ISRAELI SHEKEL (IL	S) AUZF STAT	E OF XXXXXXXX - 9999	999999					
9/30/2021	0	0.00	0.00	0.00	0.3099669885	0.00	0.00	0.00
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00
NEW ISRAELI SHEKEL (IL	S) AUZF STAT	E OF XXXXXXXX - 9999	999999					
9/30/2021	0	0.00	0.00	0.00	0.3099669885	0.00	0.00	0.00
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00
NEW ZEALAND DOLLAR	(NZD) AUZF ST	ATE OF XXXXXXX - 99	999999					
9/30/2021	0	0.00	0.00	0.00	0.6898500000	0.00	0.00	0.00
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00
NEW ZEALAND DOLLAR	(NZD) AUZF ST	ATE OF XXXXXXX - 99	9999999					
9/30/2021	0	0.00	0.00	0.00	0.6898500000	0.00	0.00	0.00
Period Summary		0.00	0.00	0.00		0.00	0.00	0.00
POUND STERLING (GBP)	AUZF STATE (	OF XXXXXXX - 9999999	99					
9/30/2021	0	0.00	0.00	0.00	1.3483500000	0.00	0.00	0.00
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00
POUND STERLING (GBP)	AUZF STATE (	OF XXXXXXXX -9999999	999					
9/30/2021	0	0.00	0.00	0.00	1.3483500000	0.00	0.00	0.00
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00

- Beginning Balance Details
- **Ending Balance Details**





12

### **Cash & Security Transactions**

A A	AUZF STATE OF XXXXXXXXX	Cash And Security Posting I 10/14/2021 - 10	Date		Report ID: ICAS001 Reporting Currency: USD	
	e Description	10/14/2021 - 10	7/14/2021 Trade / Ex Date	Shares/Par/Amount	Local Amount	Reporting
	nt Cash Detail Transaction Type	ISIN	Settle / Pay Date	Local Price/Rate	Eocal Alliount	Reporting
-quivale.	Trading Broker	Reference Number	Cash Post Date	Local Principal		
	Clearing Broker	Client Reference	Cash Value Date	Local Income		
	Linked Transaction Description	Event ID	Transaction Status Post Timestams			
		Market Reference Settlement Policy		В		
	FREE TRANSACTIONS FOR PERIOD	•				
<b>A</b> )	Security Addition		10/12/2021	250.0000	0.00	0.00
	SECURITY DEPOSIT	AU000000GRV0	10/14/2021			
	GREENVALE MINING LTD NPV	1212840179034	10/14/2021			
	THE BANK OF NEW YORK MELLON (IRVTUS3NIBK)	GSP 117992	10/14/2021			
	CITIBANK LIMITED MELBOURNE (CITIAU3X)		2021-10-13			
		Actual	19:33:39.4822 51		<b>c</b> )	
A	Merger		10/14/2021	193.0000	0.00	0.0
	CORPORATE ACTION	CA0324272057	10/14/2021			
	ANACORTES MNG CORP NPV	1212874006558	10/14/2021			
		PSS1212874006558	10/14/2021 2021-10-14			
		0214092786	13:09:08.5065			
		PSS1212874006558	87			

	V E N U	Cash And Security Posting	Date		Report ID: ICAS0011 Reporting Currency: USD	
	Description	10/14/2021 - 1	Trade / Ex Date	Shares/Par/Amount	Local Amount	Reporting Equivalent
тап туре	Cash Detail Transaction Type	ISIN	Settle / Pay Date	Local Price/Rate	Local Amount	Reporting Equivalent
	Trading Broker	Reference Number	Cash Post Date	Local Principal		
	Clearing Broker	Client Reference	Cash Value Date	Local Income		
	Linked Transaction Description	Event ID	Transaction Status Post Timestamp	Local Income		
		Market Reference Settlement Policy				
DV	Dividend	•	9/28/2021	8.647.0000	10.268.31	10.268.31
	CASH DIVIDEND - CR	US7181721090	10/14/2021	1.1875000000	,	,=
	PHILIP MORRIS INTL INC NPV	PSS2110136075853	10/14/2021			
	Gross 10,268.31 RecDte: 9/29/2021		10/14/2021	10,268.31		
A	PSS #: 2110136075853 UNITS/QNTY: 8,647.0000 SEDOL #: B2PKRQ3 ISIN #: US7181721090 EVENT ID: 0215404243	0215404243	2021-10-13 16:48:40.9298 99	В		
	DESC: PHILIP MORRIS INTL INC DIV SRC RATE: 1.187500000 EX DT: 21SEP28 RECORD DT: 21SEP29 PAY DT: 21OCT14 CCY: USD GRSS: 10,268.3100 WTH: 0.0000 AMOR BAL: 0.0000 PRFC: 0.0000 CUFC: 0.0000	0				
DV	Dividend		9/28/2021	8,647.0000	540.44	540.44
	CASH DIVIDEND - CR	US7181721090	10/14/2021	0.0625000000		
	PHILIP MORRIS INTL INC NPV	PSS2110146172691	10/14/2021			
	Gross 540.44 RecDte: 9/29/2021		10/14/2021	540.44		
	PSS #: 2110146172691 UNITS/QNTY: 8,647.0000 SEDOL #: B2PKRQ3 ISIN #: US7181721090 EVENT ID: 0215404243	0215404243	2021-10-14 16:21:25.2414		( <b>c</b>	
	DESC: PHILIP MORRIS INTL INC DIV SRC RATE: 0.062500000 EX DT: 21SEP28 RECORD DT: 21SEP29 PAY DT: 21OCT14 CCY: USD GRSs: 540.4400 WTH: 0.0000 AMOR RAI: 0.0000 PEPEC: 0.0000 CLIEC: 0.0000	0	3			

- A Transaction Description Includes Rate and Number of Shares
- B Trade Date, Record Date and Payable Date for all Dividends and Payments
- c Information Related to Shares Received for Transaction Type





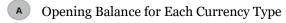
### **Cash Inquiry**



Cash Inquiry- Detail Prior Day 10/14/2021 As of 10/14/2021

Report ID: ICAS0021 Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXX		As of 10/14/2021				
Opening Balance					Opening Balance 0.00	Reporting Equivalent Opening Balance 0.00
South African Rand (ZAR) AUZF STATE OF XXXXXXX	XX-999999999 Exchan	ge Rate 0.0683964119				
				A	Opening Balance	Reporting Equivalent Opening Balance
Opening Balance					0.00	0.00
Swedish Krona (SEK) AUZF STATE OF XXXXXXXX -	9999999999 Exchange R	ate 0.1160840216				
					Opening Balance	Reporting Equivalent Opening Balance
Opening Balance					0.00	0.00
Swedish Krona (SEK) AUZF STATE OF XXXXXXXXX -	9999999999 Exchange I	Rate 0.1160840216				Reporting Equivalent
Opening Balance					Opening Balance 0.00	Opening Balance
Swiss Franc (CHF) AUZF STATE OF XXXXXXXXX - 99	99999999 Exchange Rat	e 1.0834823121			0.00	0.00
		- 11000				Reporting Equivalent
Opening Balance				A	Opening Balance 0.00	Opening Balance 0.00
Swiss Franc (CHF) AUZF STATE OF XXXXXXXXX - 99	99999999 Exchange Rat	e 1.0834823121				
					Opening Balance	Reporting Equivalent Opening Balance
Opening Balance					0.00	0.00
United States Dollar (USD) AUZF STATE OF XXXXXX	XXX-999999999 Exch	ange Rate 1.0000000000				
					Opening Balance	Reporting Equivalent Opening Balance
Opening Balance					2,021.48	2,021.48
Settled Transactions Transaction Type		Update Date - Timestamp		Shares/Par	Amount I	Reporting Equivalent Amount
	ISIN	Reference Number Event ID	Posted Date Value Date	Amortized Units	Amount	reporting Equivalent Amount
CORPORATE ACTION  DFA INVESTMENT DIMENSIONS GROUP		10/14/2021 10:19 AM		0.55	-21.03	-21.03
	US2332035615	1212874005391 0216535757	10/14/2021	0.00		
		0216535757	10/14/2021			
		Total CORPO	PRATE ACTION:		-21.03	-21.03
DIVIDEND  DFA INVESTMENT DIMENSIONS GROUP		10/14/2021 10:18 AM		395.55	21.03	21.03
	US2332035615	PSS2110146111177	10/14/2021	0.00		
		0216535757	10/14/2021			
A		Cash Inquiry- Deta	il			Report ID: ICAS0021
A V E N U		Prior Day 10/14/202	:1		Re	porting Currency: USD
PHILIP MORRIS INTL INC NPV		As of 10/14/2021 10/14/2021 04:12 PM		101.00	6.31	6.31
THE MORE INC.	US7181721090	PSS2110146170854	10/14/2021	0.00	0.01	0.01
		0215404243	10/14/2021			
PHILIP MORRIS INTL INC NPV	US7181721090	10/14/2021 04:10 PM PSS2110146165245	10/14/2021	0.00	-126.25	-126.25
			10/14/2021			
NORDIC AMERICAN TANKER LTD 0.01 USD	BMG657731060	10/14/2021 10:16 AM PSS2109226102955	10/14/2021	445.00 0.00	4.45	4.45
	BMG007731000	0214323960	10/14/2021	0.00	( <b>c</b> )	
TAIWAN SEMICONDUCTOR M TWD 10.0 ADR		10/13/2021 08:00 PM		132.00	51.23	51.23
	US8740391003	PSS2109156147295 0210976027	10/14/2021	0.00		
PHILIP MORRIS INTL INC NPV		10/13/2021 08:00 PM	TOT THE EUR	0.00	126.25	126.25
	US7181721090	PSS2109276169396	10/14/2021 10/14/2021	0.00		
			10/14/2021			
		1	otal DIVIDEND:		1,000.41	1,000.41
			d Transactions	В	1,016.93	1,016.93
		Projected I	Ending Balance		21,553.12	21,553.12



**Ending Cash Balance** 

Cash Deposited into the Account for Specified Transaction Type





14

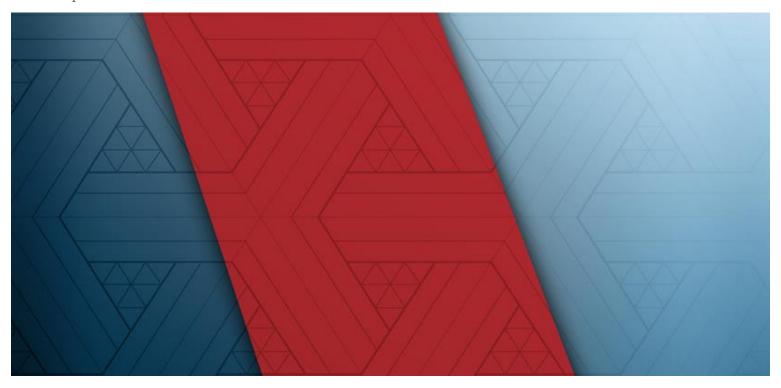
### Extranet Reference Guide



# The Extranet Reference Guide

An Online Portal for Managing Your Unclaimed Securities Portfolio

September 2021







### 1. Preface

The Extranet is an on-line portal through which authorized staff can coordinate automated transfer requests, respond to voluntary corporate actions, submit research requests along with other capabilities. Via the secure Extranet, authorized users have the ability to transact electronically to initiate transfers, wires, receipt of securities and cash and to inquire about any particular security or deposit.

Avenu has automated the transfer request process through the Extranet for Avenu's new Clearview Connection suite of software solutions, including UPS2000, by generating a file on the system upon final claim approval. Each day, all approved securities (including mutual funds) claims that require re-registration to owners are included on a file (Excel) that is automatically delivered securely to the Extranet or SFTP site. The manual process of entering securities transfers or claims one by one is eliminated. The Extranet includes a quality assurance review as it provides the initiator with the transaction request. This has eliminated nearly all posting errors.

©2021 Avenu Insights & Analytics, LLC. All rights reserved. Avenu® and Avenu and Design® are trademarks of Avenu Insights & Analytics, LLC. in the United States and/or other countries.

The contents of this manual are considered to be Avenu private data and are provided for the exclusive use of the state. The contents herein may not be reproduced without the specific written permission of Avenu Insights & Analytics, LLC. This document is for informational purposes only and does not constitute a contract or an offer to contract.

Other company trademarks are also acknowledged.

Document Version: 5.1 (September 2021, Avenue Insights & Analytics, LLC.)





# 2. Table of Contents

1.	Preface	2
2.	Table of Contents	3
3.	Navigating the System	4
4.	Web Library	5
5.	FTP Delivery	6
6.	State Home	7
	State Home - NWT	8
	State Home - Research	9
	State Home – Liquidation	10
7.	Corporate Actions	11
8.	Uploads – File	





# 3. Navigating the System

After logging on to the Extranet via our web-based system, <a href="www.unclaimedproperty.com">www.unclaimedproperty.com</a> the user will be presented with an easy-to-use side navigation bar that provides access to all sub-sections of the Extranet. Access to the different sections within the site will be controlled by a unique user login ID and password as determined by your state administrator.

Web Library FTP Delivery State Home Uploads Corporate Actions

Logout

**Web Library:** Allows the user to navigate

E-Library archives.

**FTP Delivery:** Allows the user to navigate the

FTP Delivery section.

**State Home:** Allows the user to navigate the

State Home section.

**Uploads:** Allows the user to upload files

such as transfer or sell requests.

**Corporate Actions:** Allows the user to navigate the

Corporate Actions section.

**Logout:** Logs the user out and ends the

session.

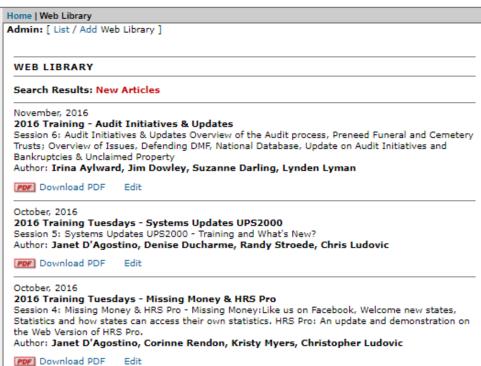




# 4. Web Library

Avenu has a section of the website containing archived articles and reference information that may be useful to the state/organization. Avenu also uploads a listing of DRS eligible securities on a monthly basis that can be downloaded by clients. The first screen shots below shows an example of what is displayed when navigating to the Web Library for the DRS profile and the second screen shot shows a listing of archived articles.









# 5. FTP Delivery

Many states have elected to receive reports or files electronically. Rather than sending a file via email, Avenu has developed an FTP capability that the state/organization may utilize to download reports. This reduces the delay in uploading the information to the state database and the possibility of losing files.

Once a file is downloaded, it is automatically moved from the Main Directory to the Archive directory. The Main Directory will always be displayed upon entering the FTP Delivery section. If an item is downloaded and moved to Archive in error, a user may retrieve it by selecting the **Archive** link displayed below and downloading it from this location. Files are maintained in Archive for 90 days and then they are automatically deleted.

lome   FTP Delivery			
	Select Organization:		FTP Deliver
	UPLOAD	Choose File No file ch	Illinoi osen UPLOAD
Name	Size	Last Modified	[ARCHIVE]
IL101161019.TXT	[MOVE TO ARCHIVE	] 2508 01/	16/2020 08:16:54 PM
	Back T	Тор	





### 6. State Home

The State Home section allows an authorized user to submit transfer requests or re-registrations, liquidation instructions and research requests. This allows the user and the vendor to track all requests with a tracking number that is assigned once all of the information has been inputted and submitted. The user may want to take a screen print of the information submitted with the tracking number or record the tracking number for their records.

A new feature of the State Home section which was developed for a more detailed audit trail allows the state/organization to have a separate user review the information submitted\*\*. Once the information is submitted by one user, an email containing all of the information submitted is sent to a separate user (email address is required).

\*\*This replicates the process of one individual creating a letter and another individual reviewing and signing which provides authorization.

When the user enters the State Home section of the website, the following screen will be displayed:

#### Home | State Home

#### State Home:

Forms:

- NWT/DRP
- Research
- Liquidation





# State Home - NWT

A user has the ability to enter new NWT/DRP, Research and Liquidation forms from this location. The following individual forms or requests are displayed based on user selection:

- 1. NWT/DRP
- 2. Research
- 3. Liquidation

### 1. NWT/DRP Form: Please fill in the fields and click Submit

State Home: NWT  Nominee Name: Account Number: Tax ID: State Address1: State Address2: State Address3: State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address2 City * State * Zip Code * Issue Name * CUSIP # * Number of Shares * Question (eg. mm/dd/yyyy) Claim # DTC Number Receiving Broker Broker Account Number	Home   State Home   NWT	
Account Number:  Tax ID:  State Address1: State Address3: State City: State State: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address1 * Address2 City *  State * Zip Code *  Issue Name * CUSIP # * Number of Shares *  Question (e.g. mm/dd/yyyy) Claim # DTC Number Receiving Broker Broker Account Number	State Home : NWT	
Account Number:  Tax ID:  State Address1: State Address2: State Address3: State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address1 * Address2 City * State * Zip Code * Issue Name * CUSIP # * Number of Shares * Number of Shares * Question in the state of the state o		
Account Number:  Tax ID:  State Address1: State Address2: State Address3: State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address1 * Address2 City * State * Zip Code * Issue Name * CUSIP # * Number of Shares * Number of Shares * Question in the state of the state o	Nominee Name:	
Tax ID: State Address1: State Address2: State Address3: State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address1 * Address2 City * State * Zip Code * Issue Name * CUSIP # * Number of Shares * Number of Shares * Question Receiving Broker  Broker Account Number		
State Address2: State Address3: State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address1 * Address2 City * State * Zip Code * Issue Name * CUSIP # * Number of Shares * Number of Shares * Quality		
State Address3: State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Stock	State Address1:	
State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Submitter ID * Registration Name *  Social Security # * Address1 * Address2 City * State * Zip Code * Issue Name * CUSIP # * Number of Shares * Question (eg. 8.000) Date Reported * Claim # DTC Number Receiving Broker Broker Account Number	State Address2:	
State City: State State: State Zip:  Note: All fields except Claim # are required.  Form Type * Stock	State Address3:	
Note: All fields except Claim # are required.  Form Type * Stock   Submitter ID *  Registration Name *   Social Security # *  Address1 *  Address2  City *  State *   Zip Code *  Issue Name *  CUSIP # *  Number of Shares *   Date Reported *   Claim #  DTC Number  Receiving Broker  Broker Account Number	State City:	9
Note: All fields except Claim # are required.  Form Type * Stock   Submitter ID *  Registration Name *    Social Security # *   Address1 *   Address2   City * State *   Zip Code *   Issue Name *   CUSIP # *   Number of Shares *   Number of Shares *   DTC Number   Receiving Broker   Broker Account Number	State State:	
Form Type * Stock V Submitter ID *  Registration Name *  Social Security # *  Address1 *  Address2  City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  Number of Shares *  Date Reported *  Claim #  DTC Number  Receiving Broker  Broker Account Number	State Zip:	Control of the Contro
Form Type * Stock V Submitter ID *  Registration Name *  Social Security # *  Address1 *  Address2  City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  Number of Shares *  Date Reported *  Claim #  DTC Number  Receiving Broker  Broker Account Number	Note:	All fields except Claim # are required.
Submitter ID *  Registration Name *  Social Security # *  Address1 *  Address2  City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  Number of Shares *  Date Reported *  CISIN #  DTC Number  Receiving Broker  Broker Account Number		
Registration Name *  Social Security # *  Address1 *  Address2  City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  Number of Shares *  (eg. 8.000)  Date Reported *  (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number		
Social Security # *  Address1 *  Address2  City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  Date Reported *  DTC Number  Receiving Broker  Broker Account Number		
Address1 * Address2 City * State * Zip Code *  Issue Name * CUSIP # * Number of Shares *  Date Reported *  Claim #  DTC Number  Receiving Broker  Broker Account Number	negistration name	
Address2  City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  (eg. 8.000)  Date Reported *  (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	Social Security # *	
City *  State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  (eg. 8.000)  Date Reported *  (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	Address1 *	
State *  Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  (eg. 8.000)  Date Reported *  (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	Address2	
Zip Code *  Issue Name *  CUSIP # *  Number of Shares *  (eg. 8.000)  Date Reported *  (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	City *	
Issue Name *  CUSIP # *  Number of Shares *  (eg. 8.000)  Date Reported *  (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	State *	~
CUSIP # *  Number of Shares *  (eg. 8.000)  Date Reported *  (leg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	Zip Code *	
Number of Shares * (eg. 8.000)  Date Reported * (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	Issue Name *	
Date Reported * (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	CUSIP # *	
Date Reported * (eg. mm/dd/yyyy)  Claim #  DTC Number  Receiving Broker  Broker Account Number	Number of Shares *	(eg. 8.000)
Claim #  DTC Number  Receiving Broker  Broker Account Number	Date Reported *	
Receiving Broker  Broker Account Number		
Broker Account Number	DTC Number	
Broker Account Number	Receiving Broker	
		SUBMIT





# State Home - Research

2. Research Form: Please fill in the fields and click Submit

Home   State Home   Research						
State Home : Research	1					
Nominee Name:						
Account Number:						
Tax ID:						
State Address1:	•					
State Address2:						
State Address3:						
State City:						
State State:						
State Zip:						
	Note: All fields except Claim # are required.					
Submitter ID *	The rest of the re					
CUSIP #						
Security Name						
Escheatment Date	(eg. mm/dd/yyyy)					
Number of Shares	(eg. 8.000)					
Explanation						
	SUBMIT					





# State Home – Liquidation

### 3. Form: Please fill in the fields and click Submit

Home   State Home   Liquidation							
State Home : Liquidation							
Nominee Name:							
Account Number:	•						
Tax ID:							
State Address1: State Address2:							
State Address3:							
State City: State State:							
State Zip:							
State Zip:							
No	te: All fields except Claim # are required.						
Form Type *	Stocks						
Submitter ID *							
Registration Name *							
Social Security #							
Address1							
Address2							
City							
State							
Zip Code							
Issue Name							
CUSIP # *							
Number of Shares *	(eg. 8.000)						
Date Reported *	(eg. mm/dd/yyyy)						
Claim #							
	SUBMIT						

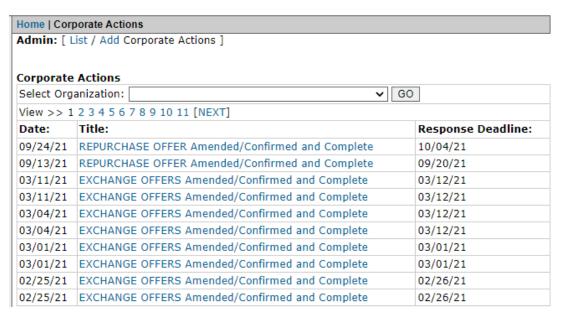




# 7. Corporate Actions

The Corporate Actions section allows the user to view and respond to all voluntary corporate actions. Each day, voluntary corporate actions are loaded to the system with information such as cusip, name of security, deadline for a response, description of the action and options available for the user to choose\*.

Upon entering the corporate actions section, the following screen will be displayed:



The user has the ability to see all voluntary Corporate Actions associated with the user's state/organization.

\*Currently, only voluntary corporate actions are available on-line. Avenu will be posting all corporate actions, voluntary and involuntary for the state to review.





# **Corporate Actions**

By clicking on a specific Corporate Action, the user will see all information associated with the action such as: the name of the security (title), cusip number, response deadline, posting and expirations dates, the rate, a description of the action (term) and the options available. The following is an example of what will be displayed for the user.

Web Library FTP Delivery State Home Uploads Corporate Actions

Logout

Home | Corporate Actions | Detail

Corporate Actions Detail

Date: 09/29/21 Title: NON OFFICIAL OFFER Amended/Confirmed and Complete

Security Description: SALESFORCE COM INC USD 0.001
CUSIP: 79466L302 Response Deadline: 10/14/21
Payable Date: Expiration Date: 10/15/21

Rate: N/A Terms: THE FOLLOWING PREVIOUSLY ANNOUNCED CORPORATE EVENT

HAS NOW BEEN UPDATED/COMPLETED EVENT TYPE: NON-OFFICIAL OFFER OFFICIAL CORPORATE ACTION EVENT REFERENCE: US125958436 START-

DATE: 06-Apr-2021 \*END DATE: 15-Oct-2021 EXPIRY DATE (COMPANY/REGISTRAR): 15-Oct-2021 EXPIRY TIME

(COMPANY/REGISTRAR): 17-00.00.000000 ACCRUED INTEREST
INDICATOR: No RESTRICTION FLAG: No DEADLINE INFORMATION:
PLEASE BE ADVISED THAT THE RESPONSE DEADLINE FOR YOUR LENDING
POSITION MAY BE EARLIER THAN YOUR CUSTODY POSITION OPTION AND
PAYOUT DETAILS: 001-ACCEPT THE CASH OFFER DEFAULT OPTION

INDICATOR: NO CUSDAR OPTION STATUS: Active \*MARKET DEADLINE DATE: 15-Oct-2021 WITHDRAWL ALLOW INDICATOR: YES \*REVOCABILITY END DATE: 15-Oct-2021 CASH OFFER DEBIT CREDIT

"REVOCABLITY END DATE: 15-OCC-2021 CASH OFFER DEBIT CREDIT INDICATOR: CREDIT CASH OFFER PRICE CURRENCY: USD CASH OFFER PRICE: 240.0 002-TAKE NO ACTION DEFAULT OPTION INDICATOR: YES CUSDAR OPTION STATUS: Active FREE FORMAT TEXT OF EVENT:.

- ACCEPT THE CASH OFFER
- TAKE NO ACTION (DEFAULT)

Submit

The list of options associated with this corporate action will be displayed with a description of what each option is. The user selects the option that the state/organization has elected to take. A confirmation of this option selected will be sent via email to the user. If the user does not respond, the default option will be taken. In the instance where the state/organization always elects the default option, we would recommend that the user access the corporate action and choose the default rather than just allowing the system to assign the default. This indicates that the user has read and understands the actions.





# 8. Uploads – File Transfer Instructions

This section allows users to upload or download transfer, liquidation or other files to/from Avenu electronically.

INSTRUCTIONS: Use the BROWSE button below to locate the file on your local disk that you wish to upload, then click UPLOAD FILE to complete the upload:

File Upload: Choose File No file chosen Upload File

#### To Add a File to this Site

- Click the "Choose File" Button
- Your Browser will open a "Choose a File" window displaying the contents of your hard drive. Use standard navigation to find and select the file you want to upload.
- The file name will appear in the "File Name" filed. Click the "Open" Button.
- Your Browser will close the "Choose a File" window and fill in the file name and path in the "Upload" field.
- Click the "Upload File" Button.
- The upload application will copy the file from your system to the upload directory and make it available for the Organization you selected.

#### To Get a File from this Site

- Move your mouse over the name of the file you want to download.
- Right click the file name. Your browser will open up an options box. Select "Save Link As"
- Your browser will open up a Select "Save As" window. Use standard navigation to identify the directory in which you want to save the file.
- Make sure that the name in the "File Name" filed is the one you want to use when saving the file.
- Note that the "Organization Name" is appended to the file name. The application performs this function when it originally received the file. If you will be returning this file to the site at a later date, you may want to rename it at some point so that the "Organization Name" is not appended more than once.
- After you have selected your preferred directory and file name click the "Save" button.





- Your Browser may open a "File Download" window to display the status of the download. When complete you will see a "Download Complete" window.
- Click "Close".





# Avenu Reports

# Class Actions Report .PDF Format



#### **Settled Class Actions Pending Claims Summary**

Report ID: ICSS00002

#### Claims Filing Deadline Date between 7/31/2023 and 1/27/2024

Class Action Account Number	Account Name	Notice Date Account Open	Exclusion Date Status Date	Claim Due Account Status	Period Begin Claim Status	Period End Comments	Currency * Projected	Gross Settlement Recognized Loss
ARCONIC INC., Secur	rities Litigation	N/A	7/19/2023	8/21/2023	11/4/2013	6/27/2017	USD	74,000,000.0000
xxxxx	STATE NAME	6/9/2016	6/1/2023	OPEN	PREPARATI ON IN			0
WELLS FARGO & CO (18CWHO)	MPANY, Securities Litigation	N/A	7/27/2023	8/21/2023	11/3/2016	8/3/2017	USD	300,000,000.0000
		NO	SELECTED ACCC	UNTS AFFECTED				
ARCONIC INC., Secur	rities Litigation	N/A	7/19/2023	8/21/2023	11/4/2013	6/27/2017	USD	74,000,000.0000
xxxxx	BNY MELLON ACCOUNT	1/1/1981	6/1/2023	CLOSED	NOT-FILED I	ONF NO ELIGIBLE	TRANSACTIONS	0
ARCONIC INC., Secur	rities Litigation	N/A	7/19/2023	8/21/2023	11/4/2013	6/27/2017	USD	74,000,000.0000
		NO	SELECTED ACCC	UNTS AFFECTED				
WELLS FARGO & CO (18CV03948WHO)	MPANY, Securities Litigation	N/A	7/27/2023	8/21/2023	11/3/2016	8/3/2017	USD	300,000,000.0000
XXXXX	STATE NAME	6/9/2016	5/31/2023	OPEN	NOT-FILED I	ONF NO ELIGIBLE	TRANSACTIONS	0
TACTILE SYSTEMS T	ECHNOLOGY. INC, Securities	N/A	8/2/2023	8/23/2023	5/7/2018	6/8/2020	USD	5,000,000.0000
		NO	SELECTED ACCC	UNTS AFFECTED				
SUNLANDS TECHNO	LOGY GROUP, Securities Litigation	N/A	9/6/2023	8/28/2023	2/23/2018	9/18/2018	USD	6,200,000.0000
		NO	SELECTED ACCC	UNTS AFFECTED				
KRAFT HEINZ COMPA	ANY, Fair Fund	N/A	N/A	8/31/2023	2/26/2016	2/21/2019	USD	62,000,000.0000
		NO	SELECTED ACCC	UNTS AFFECTED				

<sup>\*</sup>Projected Recognized Loss amount is not the final proceeds to be received by the client for the specified class action event/account. It is the potential recognized loss value calculated by BNYM's vendor for class action processing. The Projected Recognized Loss amount is an estimate, and may vary from the final Court approved/analyzed recognized loss proceeds received.

# Custody Valuation Report .PDF Format

Custody Valuation
By Asset Type
Settled Basis - 3/4/2020

Report ID ICUS0017
Reporting Currency USD

				Units			
ISIN Description	Ctry Inc	Loc	Ссу	Amortized Face	Local Price	Market Value Local	Market Value Reporting Currency
DEBT UNITED STATES DOLLAR (Exchange Rate: 1.0000000000)							
US81988XAA19 SHARP DO BRASIL S A I 9.625 300CT05	BR	DTC	USD	50,000.0000			
OCC 1000/AATO GITAKE DO BINAGE O'ATO.020 0000 100				, 			
TOTAL BY	IOTAL AMORTI	BY UNITS ZED FACE		50,000.0000 0.0000			0.00
EQUITIES							
CANADIAN DOLLAR (Exchange Rate: 0.7455450000)							
CA15101Q1081 CELESTICA INC NPV	CA	DTC	CAD	342.0000	15.880000	5,430.96	4,049.03
<b>EURO</b> (Exchange Rate: 1.1123000000)							
US1727371080 CIRCUIT CITY STORES INC USD 0.5	US	DTC	EUR	25.0000			
US5502783039 LUMINENT M COM USD0.001	US	DTC	EUR	100,000.0000			
US86825Q1040 SUPERIOR O COM STK USD0.01	US	DTC	EUR	250.0000	0.028000	7.00	7.79
	TOTAL E	BY UNITS	- EURO	100,275.0000			
TOTAL BY	AMORTIZ	ED FACE	- EURO	0.0000		7.00	7.79
SWISS FRANC (Exchange Rate: 1.0326310000)							
CH0244767585 UBS GROUP AG CHF 0.1	СН	DTC	CHF	2,134.0000	13.160000	28,083.44	28,999.83
UNITED STATES DOLLAR (Exchange Rate: 1.0000000000)							
CH0102993182 TE CONNECTIVITY LTD 2.6	СН	DTC	USD	32.0000	62.630000	2,004.16	2,004.16
GB00B5BT0K07 AON PLC USD 0.01	GB	DTC	USD	13.0000	107.790000	1,401.27	1,401.27
IE00BBGT3753 MALLINCKRODT PLC USD 0.2	ΙE	DTC	USD	3.0000	54.650000	163.95	163.95
IE00BD845X29 ADIENT PLC USD 0.001	ΙE	DTC	USD	1.0000	44.200000	44.20	44.20
IE00BLS09M33 PENTAIR PLC USD 0.01	ΙE	DTC	USD	3.0000	54.700000	164.10	164.10
IE00BTN1Y115 MEDTRONIC PLC USD 0.1	ΙE	DTC	USD	30.0000	82.140000	2,464.20	2,464.20
IE00BY7QL619 JOHNSON CONTROLS INTERNATI USD 0.01	IE	DTC	USD	12.0000	40.880000	490.56	490.56
IE00BY9D5467 ALLERGAN PLC USD 0.0033	ΙE	DTC	USD	7.0000	195.000000	1,365.00	1,365.00
NL0011031208 MYLAN NV EUR 0.01	NL	DTC	USD	40.0000	35.000000	1,400.00	1,400.00
PR25811P8521 DORAL FINL CORP USD 0.01	PR	DTC	USD	2.0000	0.051950	0.10	0.10
PR2987161011 EUROBANCSH COM STK USD0.01	PR	DTC	USD	270.0000	0.000100	0.03	0.03
PR3186727065 FIRST BANCORP P R USD 0.1	PR	DTC	USD	1,165.0000	4.910000	5,720.15	5,720.15

Disclaimer - The pricing information contained within this report is unaudited and may not reflect the most recent security prices.

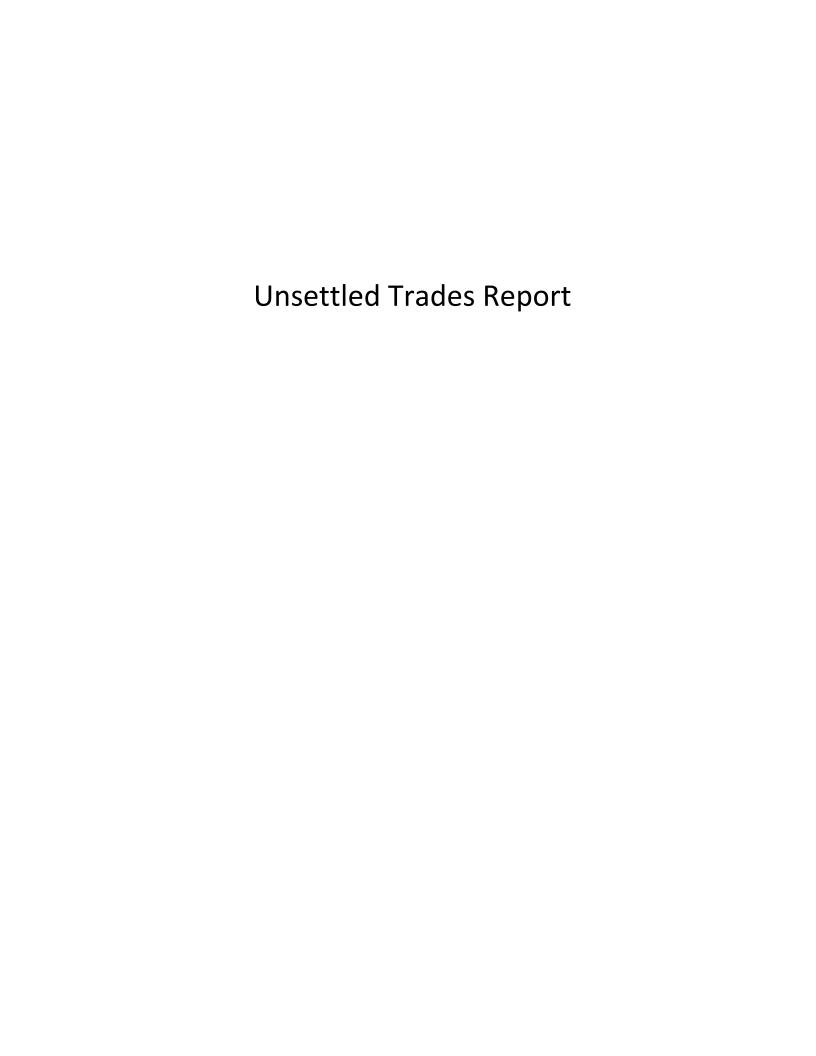


# Custody Valuation By Asset Type Settled Basis - 3/4/2020

Report ID ICUS0017
Reporting Currency USD

				Units			
ISIN Description	Ctry Inc	Loc	Ссу	Amortized Face	Local Price	Market Value Local	Market Value Reporting Currency
US81371U1043 SECURE TEC COM USD0.01	US	DTC	USD	20.0000	0.010000	0.20	0.20
US8284086092 SILVERLINE TECHNOLOGIES LTD NPV ADR	IN	DTC	USD	1.0000	1.600000	1.60	1.60
US8445448090 SOUTHMARK CORP USD 0.01	US	DTC	USD	4.0000	0.001000		
US85207U1051 SPRINT CORP USD 0.01	US	DTC	USD	1.0000	6.130000	6.13	6.13
US85916J4094 STEREOTAXIS INC USD 0.001 DEFAULT	US	DTC	USD	32.0000	0.640000	20.48	20.48
US8627731081 STRATEGIC COM USD0.001	US	DTC	USD	225.0000	0.000100	0.02	0.02
US86800C1045 SUNTECH PO SPONS ADR EA REPR 1 ORD	KY	DTC	USD	70.0000	0.035200	2.46	2.46
US8769932059 TAX FREE PUERTO RICO TARGET RESTR	PR	NYV	USD	2,924.0000	1.000000	2,924.00	2,924.00
US8786951058 TECHNOLOGY USD0.001	US	NYV	USD	440.0000	0.262500	115.50	115.50
US90206R1032 2-INFINITY COM INC USD 0.001	US	DTC	USD	1,000.0000	0.000500	0.50	0.50
US9092143067 UNISYS CORP USD 0.01	US	DTC	USD	40.0000	10.350000	414.00	414.00
US9100471096 UNITED CONTL HLDGS INC USD 0.01	US	DTC	USD	20.0000	57.230000	1,144.60	1,144.60
US92242T1016 VECTRUS INC USD 0.01	US	DTC	USD	16.0000	16.450000	263.20	263.20
US9253261005 VERTIENTES CAMAGUEY SUGAR C USD 6.5	US	NYVS	USD	550.0000	0.010000	5.50	5.50
US9293671007 WW ENERGY COM STK USD0.0001	US	DTC	USD	2.0000			
US94107F1012 WASTECH INC COM USD0.01	US	DTC	USD	500.0000	0.010000	5.00	5.00
TOTAL BY UNITS - TOTAL BY AMORTIZED FACE -				39,293.4780 0.0000	_	206,551.14	206,551.14
то	TAL BY (	JNITS - E	QUITIES	142,044.4780			
TOTAL BY AMO	RTIZED	FACE - E	QUITIES	0.0000			239,607.79
TOTAL BY UNITS - ACCOUNT XXXXXX - AUZF	STATE	NAME	_	192,044.4780			
TOTAL BY AMORTIZED FACE - ACCOUNT XXXXXX		STATE NAME	=	0.0000			239,607.79

Disclaimer - The pricing information contained within this report is unaudited and may not reflect the most recent security prices.





#### **Unsettled Trades**

Report ID ICUS0018

#### Real-Time 1/8/2020 11:50:00 AM EST

	Description Trading Broker Clearing Broker Buyer Order Party Seller Order Party Trade Matching Status	ISIN Reference Number Client Reference Depository Reference Market Reference Settlement Policy	Contract Settle Date	Shares/Par Local Net Amt Local Price	Local Currency
SD	Security Addition  BPI ENERGY HOLDINGS INC  FIRST CLEARING, LLC  FIRST CLEARING, LLC	CA0559341031 1163010205943 26931837.6		166.0000	Failing - SETTLEMENT FAILURE UNITED STATES DOLLAR (USD) 26876390.338 B/C A, REC FROM FIRST CLEARING AWAITING SECURITIES FROM CPY 1163010101840
	AWSH	Actual			
SD	AWAITING SECURITIES FROM CPY Security Addition CAMPBELL R COM NPV FIRST CLEARING, LLC FIRST CLEARING, LLC	CA1344226099 1163010206055 26931837.19		20.0000	Failing - SETTLEMENT FAILURE UNITED STATES DOLLAR (USD) 26876390.352 B/C A, REC FROM FIRST CLEARING AWAITING SECURITIES FROM CPY 1163010101883
	AWSH	Actual			
en.	AWAITING SECURITIES FROM CPY				
SD	NORTEL NETWORKS CORP NEW NPV OPTIONSXPRESS, INC. OPTIONSXPRESS, INC.	CA6565685089 1163090300390 27016545.129		1.0000	Pending - VERIFIED  UNITED STATES DOLLAR (USD)  B/C A RECEIVE FROM OPTIONXPRESS
		Actual			
SD	Security Addition  NOVANTA INC NPV  NATL FINANCIAL SERVICES LLC  NATL FINANCIAL SERVICES LLC	CA67000B1040 1162990284984 26925435.589		13.0000	Failing - VERIFIED  UNITED STATES DOLLAR (USD)  B/C A, REC FROM FIDELITY AWAITING SECURITIES FROM CPY 1162990130269
	AWSH	Actual			
	AWAITING SECURITIES FROM CPY				



Description

SD

SW

**Trading Broker** 

**Clearing Broker** 

**Buyer Order Party** 

**Seller Order Party** 

**Trade Matching Status** 

OPTIONSXPRESS, INC.

OPTIONSXPRESS, INC.

RAYMOND, JAMES & ASSOC., INC.

**Unsettled Trades** Report ID ICUS0018

Real-Time 1/8/2019 11:50:00 AM EST

ISIN Reference Number

**Client Reference** 

Depository Reference Trade Date

Market Reference Contract Settle Date

Settlement Policy Order Date

Shares/Par Status

**Local Price Comments** 

Local Net Amt Local Currency

Security Addition USM15CNT9972 1/8/2020

**CONTRA BACKWEB TECHNOLOGIES NPV** 1163090300360 1/8/2020

27016545.121

300.0000 Pending - VERIFIED

UNITED STATES DOLLAR (USD)

**B/C A RECEIVE FROM OPTIONXPRESS** 

Actual

499.0720 Shares/Par **TOTAL SECURITY DEPOSIT (7)** 

Security Withdrawal USM15CNT9972 10/25/2019 -600.0000 Failing - VERIFIED

**CONTRA BACKWEB TECHNOLOGIES NPV** 1163000246904 10/25/2019

RAYMOND, JAMES & ASSOC., INC.

UNITED STATES DOLLAR (USD) B/C C SALE OF SHARES DOC

26935128

Actual

TOTAL XXXXXX - STATE NAME( 242 ) 4,325,418.3410 Shares/Par

> REPORT TOTAL (242) 4,325,418.3410 Shares/Par

# Securities Liquidation Report PDF Format



# **Custody Security Transactions**

By Security

Actual Settle Date 12/1/2019 - 12/31/2019

Report ID ICUS0015

XXXXXX - STATE NAME Description **CUSIP/CINS Trading Broker ISIN Create Date Clearing Broker** Reference Number Trade/Ex Date Shares/Par **Buver Order Party** Client Reference Contract Settle/Pay Date **Local Net Amount Seller Order Party** Local Price Status Market Reference Actual Settle Date Cash Offset Number **Settlement Policy Order Date Days Late Local Currency** Comments Sale- Mutual Fund order 746853100 12/2/2019 -227.0000 Settled - ACTUAL 1.090.72 **SETTLEMENT PUTNAM PRE SBI NPV** US7468531006 12/1/2019 4.8300881000 UNITED STATES DOLLAR (USD) 1163070106776 12/4/2019 **RAYMOND JAMES & ASSOC INC** RAYMOND JAMES & ASSOC INC GTN1611020006458 12/4/2019 Actual Cash Offset - XXXXX08400 SPRO//RVA 63 1/01/19 1163070076550 S Sale 878520204 12/2/2019 -5.0000 Settled - ACTUAL 28.81 SETTLEMENT US8785202040 12/1/2019 **TECHNICOLO NPV ADR** 5.7900000000 UNITED STATES DOLLAR (USD) 1163070106738 12/4/2019 **RAYMOND JAMES & ASSOC INC** GTN1611020006452 12/4/2019 **RAYMOND JAMES & ASSOC INC** Actual Cash Offset - XXXXX08400 SPRO//RVA 70 1/01/19 1163070076565 Shares Liquidated includes number of shares, date, price, S Settled - ACTUAL Sale 882508104 12/2/2019 1,174.07 SETTLEMENT **TEXAS INSTRS INC USD 1.0** US8825081040 12/1/2019 commission, net proceeds and 69.09000000000 UNITED STATES DOLLAR (USD) 1163070106723 12/4/2019 0000 RAYMOND JAMES & ASSOC INC more. **RAYMOND JAMES & ASSOC INC** GTN1611020006448 12/4/2019

Actual



Description

Comments

**Trading Broker** 

**Clearing Broker** 

**Buyer Order Party** 

**Seller Order Party** 

**Cash Offset Number** 

# **Custody Security Transactions**

By Security

Actual Settle Date 12/1/2019 - 12/31/2019

**CUSIP/CINS** 

**ISIN Create Date** 

Reference Number Trade/Ex Date

Client Reference Contract Settle/Pay Date

Market Reference Actual Settle Date

Settlement Policy Order Date

Shares/Par Local Net Amount

Local Price Status

Days Late Local Currency

Report ID ICUS0015

Cash Offset - XXXXX08400 SPRO// AVENU UNCLAIMED PROPERTY CLEARING AVERAGE PRICE TRADE 2255 RVA 71 11/01/16 1163070076560

TOTAL SELL (1)

TOTAL TEXAS INSTRS INC USD 1.0 (1)

TOTAL XXXXXX - STATE NAME

(3)

-17.0000 Shares/Par

-17.0000 Shares/Par

-249.0000 Shares/Par



### **Mutual Fund Sales**

AVENU XXXXXX - STATE NAME

Description

# **Custody Security Transactions**

By Security

Actual Settle Date 12/1/2019 - 12/31/2019

**Trading Broker** 

**Clearing Broker** 

**Buver Order Party** 

**Seller Order Party** 

Cash Offset Number

Comments

**CUSIP/CINS** 

**ISIN Create Date** 

Reference Number Trade/Ex Date

Client Reference Contract Settle/Pay Date

Market Reference Actual Settle Date

**Settlement Policy Order Date** 

Shares/Par

**Local Net Amount** 

**Local Price Status** 

**Days Late Local Currency** 

-107.1730 Settled - ACTUAL 1.955.91 SETTLEMENT

18.2500256000 UNITED STATES DOLLAR (USD)

Report ID ICUS0015

Sale- Mutual Fund order

AIM EQUITY INVSC CHRTR FD A

001413103 12/2/2019

US0014131033 12/1/2019

1163070082128 12/2/2019

26968011 12/2/2019

Actual

Cash Offset - XXXXX08400

1163060158808 10-31-19 SALE REQUEST SALE OF SHARE 1163060158808 10-31-19 SALE REQUEST

SALE OF SHARE

Sale- Mutual Fund order

S

AIM EQUITY INVSC DVSFD INV

Mutual Fund Sale -Includes price/share, net/gross proceeds and more

001413194 12/2/2019

US0014131942 12/1/2019

1163070082055 12/2/2019

TSR1611018827027 12/2/2019

Actual

-60.3620 Settled - ACTUAL 1,129.37 SETTLEMENT

18.7099499000 UNITED STATES DOLLAR (USD)

0

Cash Offset - XXXXX08400

1163060195152 10-31-19 SALE REQUEST SALE OF 1163060195152 10-31-19 SALE REQUEST SALE OF

SHARES UNEXECUTED DOC 26968011

TOTAL XXXXXX - STATE NAME(2)

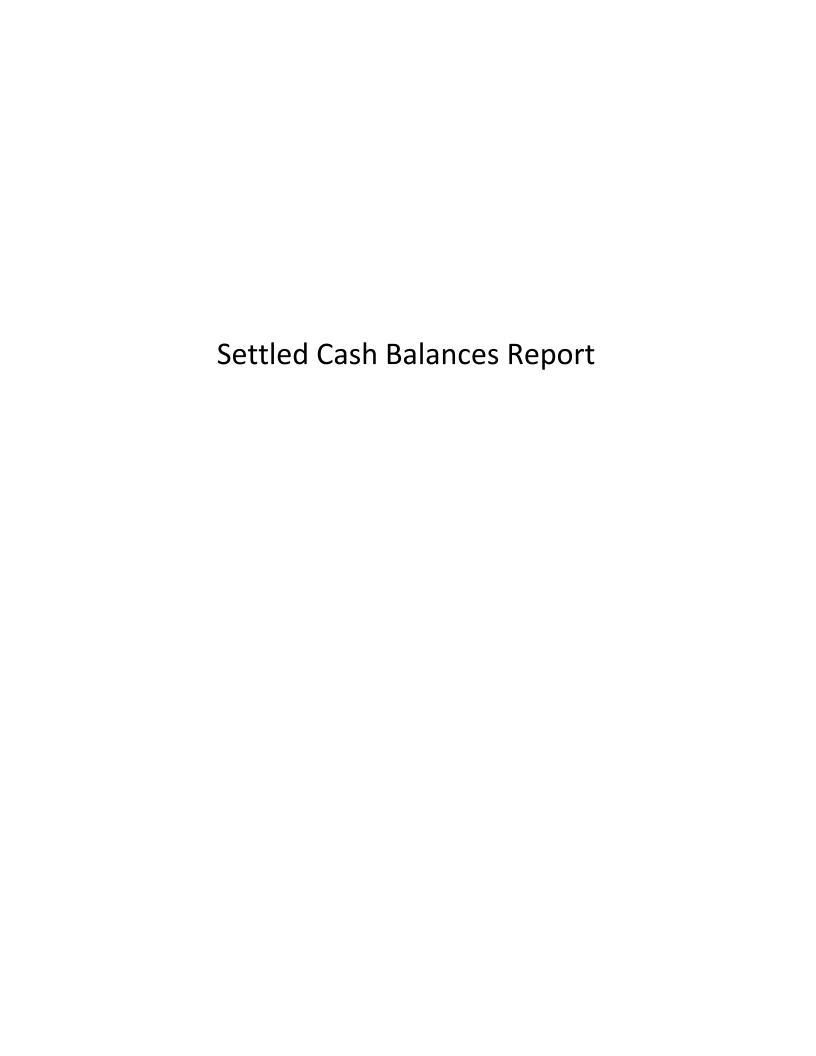
-167.5350 Shares/Par

List of Assets Report .XLS

# LIST OF ASSETS



P <b>r</b> ice Date	Location Name	CUSIP CINS	Security Short Description	Units	Local Price	Market Value ISIN Local	TICKER	QUICK SEDOL	VALOREN I	<b>M</b> oo <b>d</b> ys Rating	S&P Rating
4/28/2020	STIF LOCATIONS/CASH HELD	X9USDDGCM	DREYFUS GOVT CM INST 289	774,235.1800	1.000000	774,235.18 X9X9USDDGCM3		9A0NZKE	•	tating	
4/28/2020	CIBC MELLON TRUST COMPANY	00831V205	AFTERMATH SILVER LTD NPV	3,951.0000	0.225000	888.98 CA00831V2057	AAG/H CN	BDFS6H8			
4/28/2020	CIBC MELLON TRUST COMPANY	10567D204	BRAVADA GOLD CORP NEW NPV	60.0000	0.090000	5.40 CA10567D2041	BVA CN	BKY7Y60	024064614		
4/28/2020	CIBC MELLON TRUST COMPANY	16890P103	CHINA GOLD INTL RES CORP LTD NPV	10,000.0000	0.740000	7,400.00 CA16890P1036	CGG CN	2750488	011547765		
4/28/2020	CIBC MELLON TRUST COMPANY	35968C604	FULL METAL MINERALS LTD NPV	2,158.0000	0.010000	21.58 CA35968C6045	FMM CN	BSL8718	026043720		
4/28/2020	CIBC MELLON TRUST COMPANY	38871F102	GRAPHITE ONE INC NPV	701.0000	0.235000	164.74 CA38871F1027	GPH CN	BJ9N154			
4/28/2020	CIBC MELLON TRUST COMPANY	85255T109	STAGE HOLDCO LTD NPV	42.0000	1.000000	42.00 CA85255T1093		BJ2FRD7			
4/28/2020	CIBC MELLON TRUST COMPANY	902166107	TYHEE GOLD CORP NPV	4,000.0000	0.000001	0.01 CA9021661074	TDC/H CN	2447575	012433210		
	CLEARSTREAM BANKING FRANKFURT	D4024H102	KHD HUMBOLDT WEDAG INTERNATIONA NPV	253.0000	1.410000	356.73 DE0006578008	KWG GR	4570060	000340920		
4/28/2020	DBS SINGAPORE	Y1775U107	CREATIVE TECHNOLOGY LTD/SINGAPO NPV	30.0000	2.150000	64.50 SG1A98006814	CREAF SP	6207582	000824820		
4/28/2020	DEPOSITORY TRUST CPNY	26822LBH6	E-470 PUB HWY AUTH COLO 0.0 01SEP22	5,000.0000	94.566000	4,728.30 US26822LBH69		BGSBD96	019065011 A	<b>A2</b>	Α
	DEPOSITORY TRUST CPNY	03062D100	AMERICAS GOLD + SILVER CORP NPV	70.0000	2.911168	203.78 CA03062D1006	USA CN	BK7CQN3			
4/28/2020	DEPOSITORY TRUST CPNY	05208W108	AURYN RES INC	35.0000	1.510000	52.85 CA05208W1086	AUG CN	BFPNLY9	022593569		
4/28/2020	DEPOSITORY TRUST CPNY	058586108	BALLARD PWR SYS INC NEW NPV	1,400.0000	14.340000	20,076.00 CA0585861085	BLDP CN	2072717	004889034		
	DEPOSITORY TRUST CPNY	067901108	BARRICK GOLD CORP NPV	6.0000	37.730000	226.38 CA0679011084	ABX CN	2024644	000337680		
4/28/2020	DEPOSITORY TRUST CPNY	15135U109	CENOVUS ENERGY INC NPV	10.0000	4.380000	43.80 CA15135U1093	CVE CN	B57FG04	010704160		
4/28/2020	DEPOSITORY TRUST CPNY DEPOSITORY TRUST CPNY	217621101	COPPERBANK RES CORP NPV ENBRIDGE INC NPV	8,633.0000	0.040000	345.32 CA2176211019	CBK CN ENB CN	BSL0M31	025864587		
4/28/2020 4/28/2020	DEPOSITORY TRUST CPNY	29250N105 32076V103	FIRST MAJESTIC SILVER CORP NPV	599.0000 1.0000	42.590000 11.370000	25,511.41 CA29250N1050 11.37 CA32076V1031	FR CN	2466149 2833583	000962293 002723324		
4/28/2020	DEPOSITORY TRUST CPNY	45690A107	INFINITE ORE CORP NPV	1,173.0000	0.080343	94.24 CA45690A1075	ILI CN	BK95TH5	002723324		
4/28/2020	DEPOSITORY TRUST CPNY	46050R107	INTERNATIONAL TOWER HILL MINES NPV	1,798.0000	0.680000	1,222.64 CA46050R1029	ITH CN	B65XBX5	011680936		
4/28/2020	DEPOSITORY TRUST CPNY	496902404	KINROSS GOLD CORP CAD NPV	391.0000	9.630000	3,765.33 CA4969024047	KCN	B03Z841	001977416		
	DEPOSITORY TRUST CPNY	51811C105	LAST MILE HLDGS LTD NPV	10.0000	0.085000	0.85 CA51811C1059	MILE CN	BLHDDT8	001377410		
4/28/2020	DEPOSITORY TRUST CPNY	557903101	MADISON PAC PPTYS INC NPV	1.0000	3.330000	3.33 CA5579031017	MPC CN	2246750	000898983		
4/28/2020	DEPOSITORY TRUST CPNY	56501R106	MANULIFE FINL CORP NPV	7,342.0000	16.690000	122,537.98 CA56501R1064	MFC CN	2492519	001002859		
	DEPOSITORY TRUST CPNY	601132202	MILLROCK RES INC NPV	4,800.0000	0.185000	888.00 CA6011322022	MRO CN	BRHX9V4	025883771		
4/28/2020	DEPOSITORY TRUST CPNY	66510M204	NORTHERN DYNASTY MINERALS LTD NPV	462.0000	0.830000	383.46 CA66510M2040	NDM CN	2637848	000330948		
4/28/2020	DEPOSITORY TRUST CPNY	682310875	ONCOLYTICS BIOTECH INC NPV	10.0000	2.470000	24.70 CA6823108759	ONC CN	BG4R989			
	DEPOSITORY TRUST CPNY	724112107	PIPESTONE ENERGY CORP NPV	4.0000	0.490000	1.96 CA7241121077	PIPE CN	BH42KD3			
4/28/2020	DEPOSITORY TRUST CPNY	74264L208	PRISM RES INC NPV	168.0000	0.022500	3.78 CA74264L2084	PRS/H CN	2319920	001764864		
4/28/2020	DEPOSITORY TRUST CPNY	811916105	SEABRIDGE COM NPV	4.0000	19.730000	78.92 CA8119161054	SEA CN	2246459	000908106		
4/28/2020	DEPOSITORY TRUST CPNY	82621E106	SIENNA RES INC NPV	12.0000	0.045000	0.54 CA82621E1060	SIE CN	BJ90VZ5	023524615		
4/28/2020	DEPOSITORY TRUST CPNY	87807B107	TC ENERGY CORP NPV	45.0000	65.280000	2,937.60 CA87807B1076	TRP CN	BJMY6G0			
4/28/2020	DEPOSITORY TRUST CPNY	896812104	TRIUMPH GOLD CORP NPV	3,000.0000	0.205000	615.00 CA8968121043	TIG CN	BD31H87			
4/28/2020	DEPOSITORY TRUST CPNY	962879102	WHEATON PRECIOUS METALS CORP NPV	4.0000	55.530000	222.12 CA9628791027	WPM CN	BF13KN5			
	DEPOSITORY TRUST CPNY	98462Y100	YAMANA GOLD INC NPV	25.0000	6.640000	166.00 CA98462Y1007	YRICN	2219279	001657932		
4/28/2020	DEPOSITORY TRUST CPNY	858497100	STELAX INDS LTD NPV	2,500.0000	0.005500	13.75 CA8584971003	LAX FP	2139559	000485643		
	DEPOSITORY TRUST CPNY	D1668R123	DAIMLER AG NPV	672.0000	30.410000	20,435.52 DE0007100000	DAI GR	5529027	000945657		
	DEPOSITORY TRUST CPNY	H42097107	UBS GROUP AG CHF 0.1	64.0000	10.140000	648.96 CH0244767585	UBSG SW	BRJL176	024476758		
4/28/2020	DEPOSITORY TRUST CPNY	806857108	SCHLUMBERG COM USD0.01	215.0000	16.150000	3,472.25 AN8068571086	SLB US	2779201	000555100		
	DEPOSITORY TRUST CPNY	G0585R106	ASSURED GUARANTY LTD USD 0.01	60.0000	30.490000	1,829.40 BMG0585R1060	AGO US	B00V7H8	001832273		
	DEPOSITORY TRUST CPNY DEPOSITORY TRUST CPNY	G3156P103 G65773106	ASA GOLD A COM STK NPV	150.0000	14.230000	2,134.50 BMG3156P1032	ASA US	B046PT7 2113876	002004320		
	DEPOSITORY TRUST CPNY	G65773106 G7738W106	NORDIC AMERICAN TANKER LTD 0.01 USD SFL CORP LTD USD 0.01	18.0000 50.0000	7.340000 11.080000	132.12 BMG657731060 554.00 BMG7738W1064	NAT US SFL US	BJXT857	000415309		
4/28/2020	DEPOSITORY TRUST CPNY	G8649T109	SYNCORA HOLDINGS LTD USD 0.01	10.0000	0.320000	3.20 BMG8649T1099	SYCRF US	B19VTG9	004474766		
	DEPOSITORY TRUST CPNY	G9001E102	LIBERTY LATIN AMERICA LTD USD 0.01	11.0000	10.690000	117.59 BMG9001E1021	LILA US	BD9Q3P5	004474700		
	DEPOSITORY TRUST CPNY	G9001E102	LIBERTY LATIN AMERICA LTD USD 0.01	34.0000	10.360000	352.24 BMG9001E1286	LILAK US	BD9Q3Q6			
4/28/2020	DEPOSITORY TRUST CPNY	P47725109	GLOBAL ENVIRONMENTAL ENER USD 0.002	1,743.0000	0.000700	1.22 BSP477251099	GEECF US	2676506	002087096		
	DEPOSITORY TRUST CPNY	38068N306	GOLD RESV INC NPV	100.0000	1.536153	153.62 CA38068N3067	GDRZF US	BK9DTW4	00=00:000		
	DEPOSITORY TRUST CPNY	86222Q806	STORNOWAY DIAMOND CORP NPV	100.0000	0.002600	0.26 CA86222Q8065	SWY CN	B06MGW3	012507233		
4/28/2020	DEPOSITORY TRUST CPNY	H84989104	TE CONNECTIVITY LTD 2.6	109.0000	73.650000	8,027.85 CH0102993182	TEL US	B62B7C3	010299318		
	DEPOSITORY TRUST CPNY	G5480U104	LIBERTY GLOBAL PLC USD A	68.0000	18.415000	-	LBTYA US	B8W6766	021612464		
	DEPOSITORY TRUST CPNY	G5480U120	LIBERTY GLOBAL PLC USD C SHARE	204.0000	17.590000	3,588.36 GB00B8W67B19	LBTYK US	B8W67B1	021612671		
4/28/2020	DEPOSITORY TRUST CPNY	G87110105	TECHNIPFMC PLC USD 1.0	20.0000	7.960000	159.20 GB00BDSFG982	FTIUS	BDSFG98			
4/28/2020	DEPOSITORY TRUST CPNY	G9402V109	VALARIS PLC USD 0.1	545.0000	0.401100	218.60 GB00BJVJZD68	VAL US	BJVJZD6			
4/28/2020	DEPOSITORY TRUST CPNY	G1151C101	ACCENTURE PLC USD 0.000023	34.0000	178.360000	6,064.24 IE00B4BNMY34	ACN US	B4BNMY3	010478724		
4/28/2020	DEPOSITORY TRUST CPNY	G29183103	EATON CORP PLC USD 0.01	444.0000	83.100000	36,896.40 IE00B8KQN827	ETN US	B8KQN82	020100637		
	DEPOSITORY TRUST CPNY	G5785G107	MALLINCKRODT PLC USD 0.2	9.0000	3.660000	32.94 IE00BBGT3753	MNK US	BBJTYC4	021654907		
	DEPOSITORY TRUST CPNY	G0084W101	ADIENT PLC USD 0.001	16.0000	13.970000	223.52 IE00BD845X29	ADNT US	BD845X2			
	DEPOSITORY TRUST CPNY	G96629103	WILLIS TOWERS WATSON P USD 0.000305	18.0000	174.930000	3,148.74 IE00BDB6Q211	WLTW US	BDB6Q21	030948740		
4/28/2020	DEPOSITORY TRUST CPNY	G6700G107	NVENT ELECTRIC PLC USD 0.01	18.0000	19.090000	343.62 IE00BDVJJQ56	NVT US	BDVJJQ5			



# Settled Cash Balances All Balances - Consolidate Cash and Sweep - All Accounts 12/01/2019 - 12/31/2019

Report ID ICAS0008
Reporting Currency USD

Date	Count	Beginning Balance Local	Net Activity Local	Ending Balance Local	Exchange Rate Reporting Currency	Beginning Balance Reporting Currency	Net Activity Reporting Currency	Ending Balance Reporting Currency
ARGENTINE PESO (ARS)	STATE NAME	- XXXXXXXX						
12/3/2019	0	0.00	0.00	0.00	0.0656922318	0.00	0.00	0.00
12/4/2019	0	0.00	0.00	0.00	0.0658653054	0.00	0.00	0.00
12/5/2019	0	0.00	0.00	0.00	0.0658653054	0.00	0.00	0.00
12/6/2019	0	0.00	0.00	0.00	0.0655845220	0.00	0.00	0.00
12/7/2019	0	0.00	0.00	0.00	0.0656922318	0.00	0.00	0.00
12/10/2019	0	0.00	0.00	0.00	0.0658327847	0.00	0.00	0.00
12/11/2019	0	0.00	0.00	0.00	0.0658870037	0.00	0.00	0.00
12/12/2019	0	0.00	0.00	0.00	0.0659608851	0.00	0.00	0.00
12/13/2019	0	0.00	0.00	0.00	0.0661419406	0.00	0.00	0.00
12/14/2019	0	0.00	0.00	0.00	0.0661922885	0.00	0.00	0.00
12/17/2019	0	0.00	0.00	0.00	0.0657030223	0.00	0.00	0.00
12/18/2019	0	0.00	0.00	0.00	0.0657527040	0.00	0.00	0.00
12/19/2019	0	0.00	0.00	0.00	0.0657732467	0.00	0.00	0.00
12/20/2019	0	0.00	0.00	0.00	0.0658653054	0.00	0.00	0.00
12/21/2019	0	0.00	0.00	0.00	0.0660066006	0.00	0.00	0.00
12/24/2019	0	0.00	0.00	0.00	0.0662142029	0.00	0.00	0.00
12/25/2019	0	0.00	0.00	0.00	0.0658870037	0.00	0.00	0.00
12/26/2019	0	0.00	0.00	0.00	0.0656868379	0.00	0.00	0.00
12/27/2019	0	0.00	0.00	0.00	0.0657408168	0.00	0.00	0.00
12/28/2019	0	0.00	0.00	0.00	0.0656922318	0.00	0.00	0.00
12/31/2019	0	0.00	0.00	0.00	0.0658924306	0.00	0.00	0.00
Period Summary	0	0.00	0.00	0.00		0.00	0.00	0.00
ARGENTINE PESO (ARS)	STATE NAME-	- xxxxxxxx						
12/3/2019	0	0.00	0.00	0.00	0.0656922318	0.00	0.00	0.00
12/4/2019	0	0.00	0.00	0.00	0.0658653054	0.00	0.00	0.00
12/5/2019	0	0.00	0.00	0.00	0.0658653054	0.00	0.00	0.00

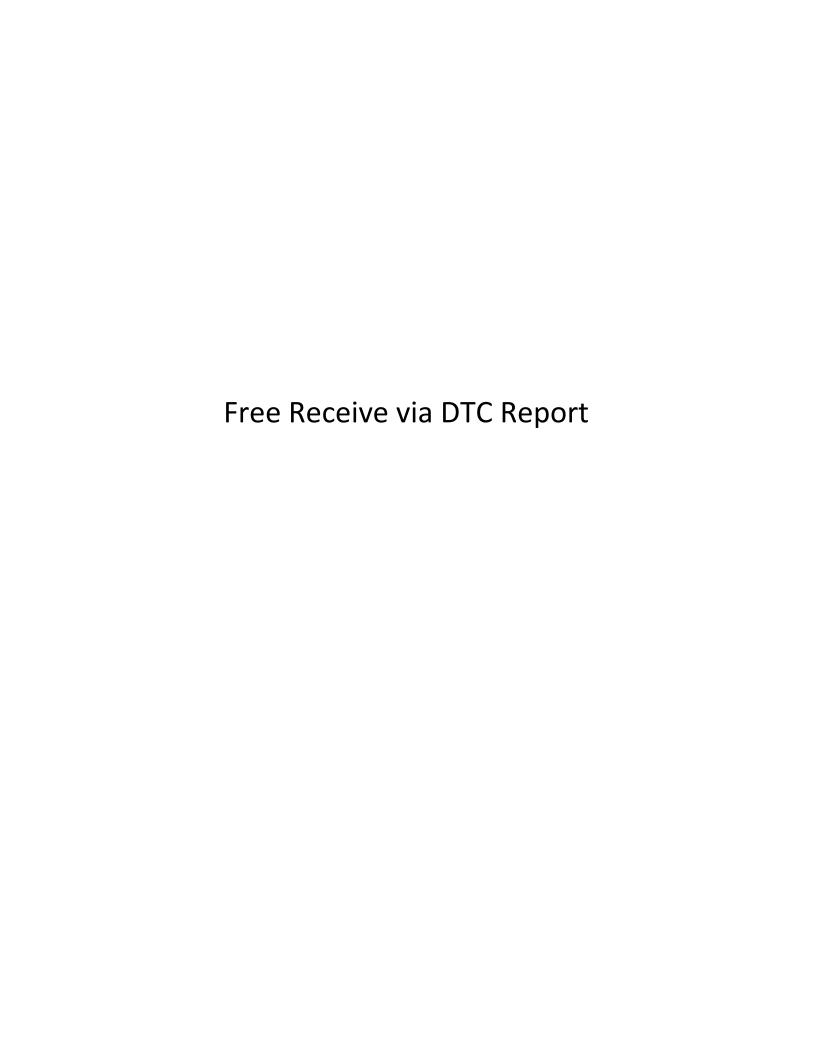


# **Settled Cash Balances** All Balances - Consolidate Cash and

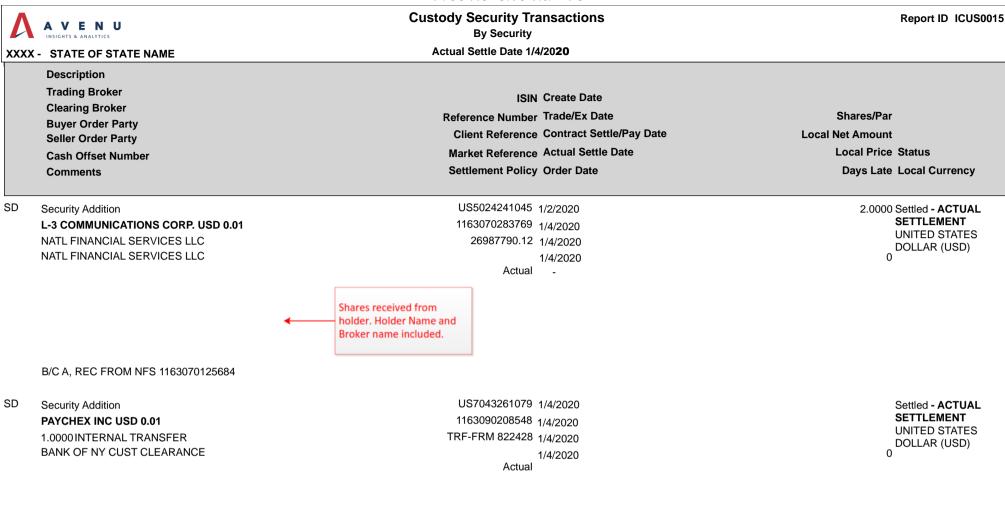
Report ID ICAS0008 Reporting Currency USD

Sweep - All Accounts 12/1/2019 - 12/31/2019

Date	Count	Beginning Balance Local	Net Activity Local	Ending Balance Local	Exchange Rate Reporting Currency	Beginning Balance Reporting Currency	Net Activity Reporting Currency	Ending Balance Reporting Currency
12/4/2019	0	0.00	0.00	0.00	1.0000000000	0.00	0.00	0.00
12/5/2019	0	0.00	0.00	0.00	1.0000000000	0.00	0.00	0.00
12/6/2019	0	0.00	0.00	0.00	1.0000000000	0.00	0.00	0.00
12/7/2019	0	0.00	0.00	0.00	1.0000000000	0.00	0.00	0.00
12/10/2019	0	0.00	0.00	0.00	1.0000000000	0.00	0.00	0.00
12/11/2019	0	0.00	0.00	0.00	1.0000000000	0.00	0.00	0.00
12/12/2019	1	0.00	4.49	4.49	1.0000000000	0.00	4.49	4.49
12/13/2019	0	4.49	0.00	4.49	1.0000000000	4.49	0.00	4.49
12/14/2019	0	4.49	0.00	4.49	1.0000000000	4.49	0.00	4.49
12/17/2019	0	4.49	0.00	4.49	1.0000000000	4.49	0.00	4.49
12/18/2019	0	4.49	0.00	4.49	1.0000000000	4.49	0.00	4.49
12/19/2019	0	4.49	0.00	4.49	1.0000000000	4.49	0.00	4.49
12/20/2019	0	4.49	0.00	4.49	1.0000000000	4.49	0.00	4.49
12/21/2019	1	4.49	55.94	60.43	1.0000000000	4.49	55.94	60.43
12/24/2019	0	60.43	0.00	60.43	1.0000000000	60.43	0.00	60.43
12/25/2019	0	60.43	0.00	60.43	1.0000000000	60.43	0.00	60.43
12/26/2019	0	60.43	0.00	60.43	1.0000000000	60.43	0.00	60.43
12/27/2019	0	60.43	0.00	60.43	1.0000000000	60.43	0.00	60.43
12/28/2019	0	60.43	0.00	60.43	1.0000000000	60.43	0.00	60.43
12/31/2019	0	60.43	0.00	60.43	1.0000000000	60.43	0.00	60.43
Period Summary	2	0.00	60.43	60.43		0.00	60.43	60.43
TOT	AL CASH AND	SWEED				3,773.74	211.65	3,985.39



### Free Receive via DTC



B/C A XFER TO XXXXX 049480516-20161101 1163090108127 Shares received from holder via DTC. Avenu Report- Internal Transfer with report ID number for easy reconciliation.

### Free Recieve via DTC



# **Custody Security Transactions**

By Security

Actual Settle Date 1/4/2020

Description

**Trading Broker** 

**Clearing Broker** 

**Buyer Order Party Seller Order Party** 

Cash Offset Number

Comments

Security Addition

**XENIA HOTE COM USD0.01** 

**ONATL FINANCIAL SERVICES LLC** 

NATL FINANCIAL SERVICES LLC

SD

**ISIN Create Date** 

Reference Number Trade/Ex Date

Client Reference Contract Settle/Pay Date

Market Reference Actual Settle Date

**Settlement Policy Order Date** 

Shares/Par Local Net Amount

Local Price Status

**Days Late Local Currency** 

Report ID ICUS0015

B/C A, REC FROM NFS 26987790.14 1163090090949

TOTAL SECURITY DEPOSIT (1)

TOTAL STANDARD E COM USD0.01 (1)

US9840171030 1/2/2020

1163070283852 1/4/2020

26987790.15 1/4/2020

1/4/2020

Actual -

2,000.0000 Shares/Par

2,000.0000 Shares/Par

270.000 Settled - ACTUAL SETTLEMENT

UNITED STATES DOLLAR (USD)

n

B/C A, REC FROM NFS 1163070125709

TOTAL XXXXXX- AUZF STATE OF XXX(6)

2,476.0000 Shares/Par



#### Free Receive - via DRS

AVENU

Description

# **Custody Security Transactions**

By Security

Actual Settle Date 12/31/2019 - 12/31/2019 XXXXXX - STATE OF STATE NAME

**CUSIP/CINS** 

**Trading Broker** 

**ISIN Create Date Clearing Broker** Reference Number Trade/Ex Date

**Buver Order Party** Client Reference Contract Settle/Pay Date **Local Net Amount Seller Order Party** 

Local Price Status Market Reference Actual Settle Date Cash Offset Number

**Settlement Policy Order Date Days Late Local Currency** Comments

SD Security Addition

46625H100 12/28/2019 JPMORGAN CHASE + CO USD 1.0 US46625H1005 12/28/2019 1163020203255 12/28/2019 JPMORGAN CHASE BANK

JPMORGAN CHASE BANK JP MORGAN 12/31/2019

Actual

B/C A, REC FROM JP MORGAN CHASE /IAS/B/C A, REC FROM JP MORGAN /IAS/CHASE SPRO//B/C A,

REC FROM JP MORGAN

Security Addition

SD

**UNION ELEC CO 4.5 CUM PFD** 

AMEREN SERVICES COMPANY/DRS

AMEREN SERVICES COMPANY/DRS

906548508 12/31/2019

US9065485081 12/31/2019 1163050316378 12/31/2019

12/31/2019

Actual

REC VIA DRS PER HOLDER NOTICE AWAITING **SECURITIES FROM CPY 1163050130339** 

Shares received from Holder/Transfer Agent via DRS

TOTAL XXXXXX- AUZF STATE OF XXX (2)

5.0000 Shares/Par

Report ID ICUS0015

3.0000 Settled - ACTUAL SETTLEMENT

2.0000 Settled - ACTUAL

**SETTLEMENT** 

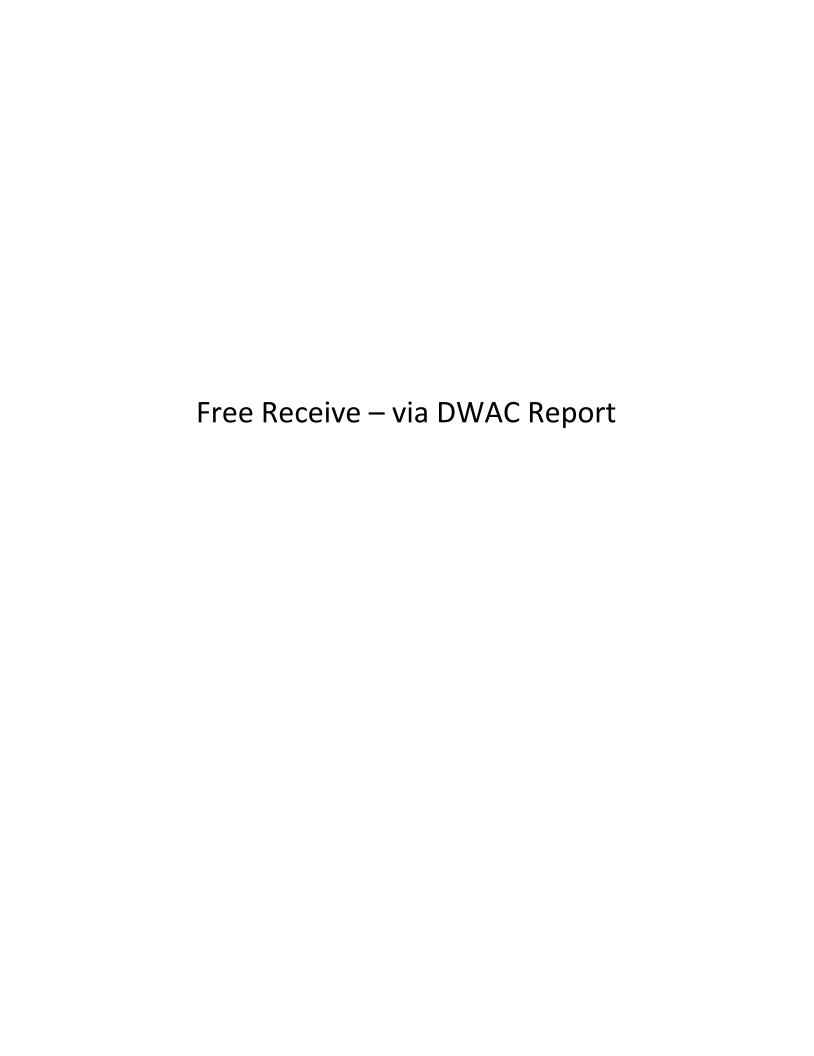
**UNITED STATES** 

DOLLAR (USD)

**UNITED STATES** 

DOLLAR (USD)

Shares/Par



## **RECEIPT OF DWAC**

AVENU XXXXXX - STATE NAME

Description

# **Custody Security Transactions**

By Security

Actual Settle Date 9/26/2019 - 1/7/2020

**CUSIP/CINS** 

**Trading Broker** 

**Clearing Broker** 

**Buyer Order Party** 

**Seller Order Party** 

**Cash Offset Number** 

Comments

**ISIN Create Date** 

Reference Number Trade/Ex Date

Client Reference Contract Settle/Pay Date

Market Reference Actual Settle Date

**Settlement Policy Order Date** 

Shares/Par

**Local Net Amount** 

**Local Price Status** 

**Days Late Local Currency** 

65.0000 Settled - ACTUAL SETTLEMENT

**UNITED STATES** 

DOLLAR (USD)

Report ID ICUS0015

SD Security Addition

**ARCHER DANIELS MIDLAND CO NPV** 

DWAC-DTC DEPOSITS/WITHDRAWALS DWAC-DTC DEPOSITS/WITHDRAWALS 039483102 9/26/2019

US0394831020 9/26/2019

1162700208079 9/26/2019

NRF1609262261400 9/26/2019

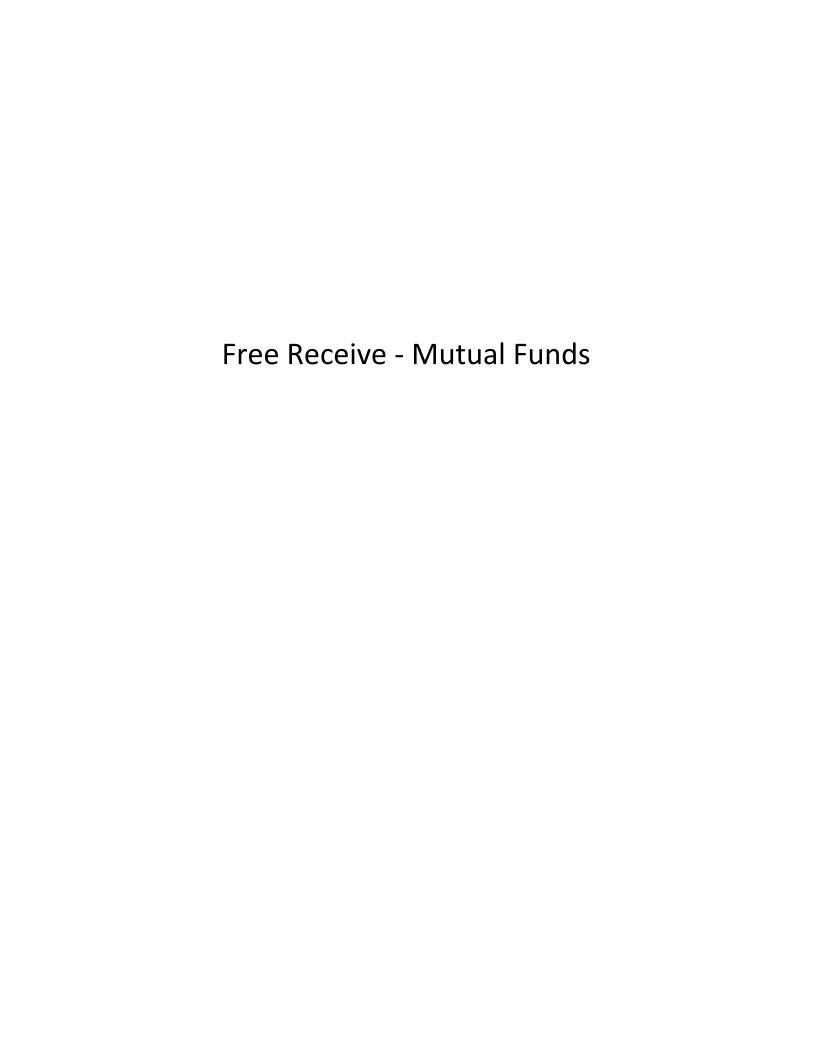
Actual

Shares Received from Holder via DWAC

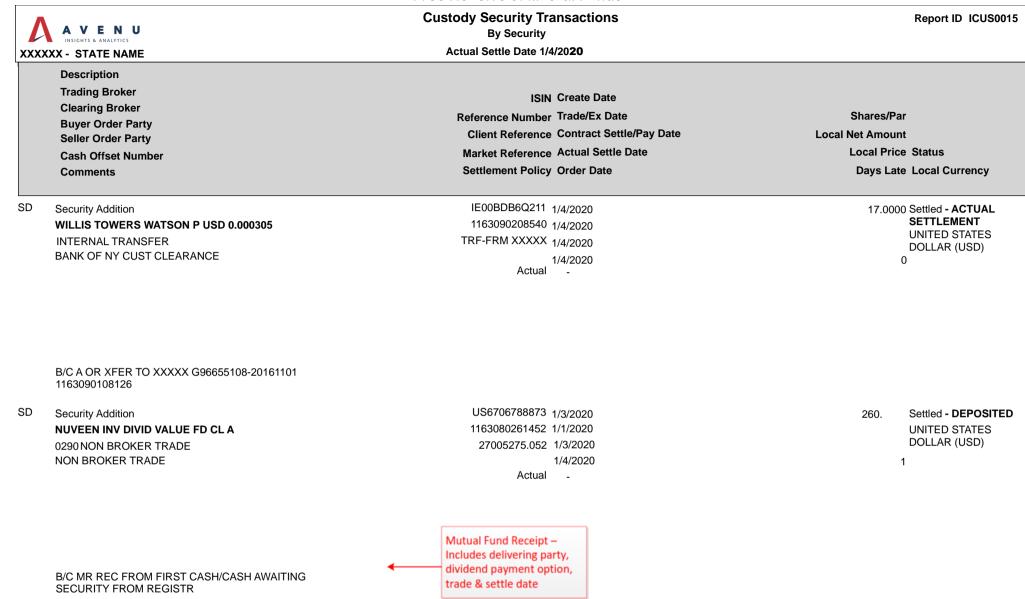
/IAS/B/C A RECEIVE DWAC FRM HICKORY /IAS/BANK TRUST 1162700121253

TOTAL XXXXXX - STATE NAME (1)

65.0000 Shares/Par



#### Free Receive of Mutual Funds



TOTAL XXXXXX - STATE(2) 277.0290 Shares/Par

Receipt of Physical Certificate Report **Receipt of Physical Certificate** 

AVENU XXXXXX- STATE NAME

> Description **Trading Broker**

**Clearing Broker** 

**Buyer Order Party** 

**Seller Order Party** 

**Cash Offset Number** 

# **Custody Security Transactions**

By Security

Actual Settle Date 1/4/2020

**ISIN Create Date** 

Reference Number Trade/Ex Date

Client Reference Contract Settle/Pay Date

Market Reference Actual Settle Date

**Settlement Policy Order Date** 

Shares/Par

**Local Net Amount** 

**Local Price Status** 

**Days Late Local Currency** 

SD Security Addition

**ENVIROTECHNOLIGIES, INC USD .001** 

CUSTOMER CUSTOMER

Comments

US29413C2026 1/3/2020

1163090141149 1/3/2020

27012828.26 1/3/2020

1/4/2020

7.0000 Settled - ACTUAL SETTLEMENT

**UNITED STATES** DOLLAR (USD)

Report ID ICUS0015

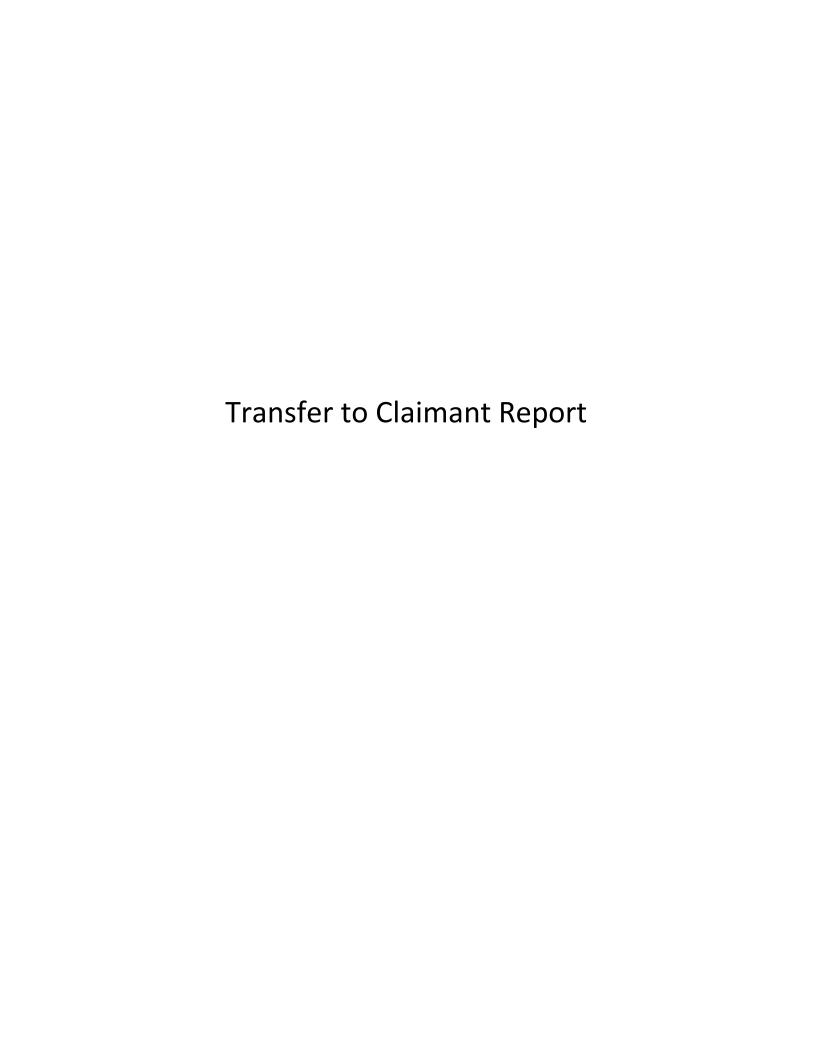
Actual

REC BY AVENU FROM NFS 020620516/111116 26987790.109 ES0757 1163090090979

Shares received from holder. Holder name and certificate # included.

TOTAL XXXXXX- STATE NAME (1)

7.0000 Shares/Par



# Re-Reg

AVENU XXXXXX - STATE NAME

# **Custody Security Transactions**

By Security

Actual Settle Date 1/4/2020

Description

**Trading Broker** 

**Clearing Broker** 

**Buyer Order Party** 

**Seller Order Party** 

Cash Offset Number

Comments

**ISIN Create Date** 

Reference Number Trade/Ex Date

Client Reference Contract Settle/Pay Date

Market Reference Actual Settle Date

**Settlement Policy Order Date** 

Shares/Par

**Local Net Amount** 

**Local Price Status** 

**Days Late Local Currency** 

SW Security Withdrawal

**SHORE BANCSHARES INC USD 0.01** 

SHIP TO CUSTOMER-STMT ONLY

SHIP TO CUSTOMER-STMT ONLY

US8251071051 10/28/2019

1163020153768 10/28/2019

172318 10/28/2019

1/4/2020

Actual

-7.0000 Settled - ACTUAL SETTLEMENT **UNITED STATES** 

DOLLAR (USD)

Report ID ICUS0015

CL 172318 JOHN SMITH, 999 MAIN ST SAN DEIGO CA 99999 AVENU

SW Security Withdrawal

3M CO USD 0.01

SHIP TO CUSTOMER-STMT ONLY

SHIP TO CUSTOMER-STMT ONLY

Shares Re-Issued to Claimant. Claimant name & address omitted in example. Claim number can be added.

US88579Y1010 10/28/2019

1163020154295 10/28/2019

177723 10/28/2019

1/4/2020

Actual

-2.0000 Settled - ACTUAL

SETTLEMENT

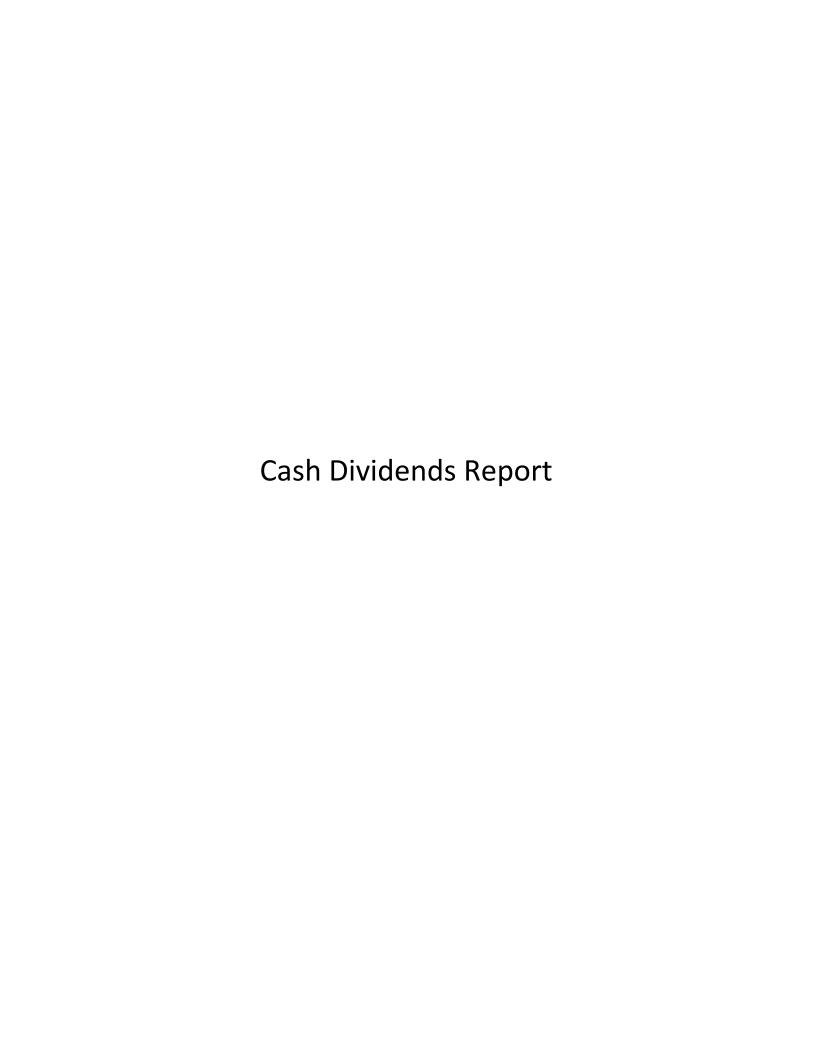
**UNITED STATES** 

DOLLAR (USD)

CL 177723 JANE ANDERSON, 100 HANCOCK STREET, QUINCY MA 02171 AVENU

TOTAL XXXXXX- STATE NAME (2)

-9.0000 Shares/Par



# AVENU XXXXXX - STATE NAME

# Cash Dividends **Cash And Security Transactions** Posting Date

Report ID ICAS0011 Reporting Currency USD

12/1/2019 - 12/31/2019

|--|

#### UNITED STATES DOLLAR (USD) AUZF STATE NAME - XXXXXXXXX

1/4/	2019 - Posted <b>Exchange Rate 1.0000000000</b>					
DIV	DEND					
DV	Dividend CRH PLC EUR 0.3 Gross 0.82 RecDte: 9/9/2019 Source W/H -0.16	G25508105 IE0001827041 PSS1611020000627	9/9/2019 12/4/2019 12/4/2019 12/4/2019	4.0000 0.2051633500 0.66	0.66	0.66
	PSS #: 1611020000627 UNITS/QNTY: 4.0000  SEDOL #: 0182704 ISIN #: IE0001827041 EVENT ID: 0112443205  DESC: CRH PLC DIV SRC RATE: 0.2051633500  EX DT: 19SEP08 RECORD DT: 19SEP09 PAY DT: 20JAN04  CCY: USD GRSS: 0.8200 WTH: 0.1600  AMOR BAL: 0.0000 PRFC: 0.0000 CUFC: 0.0000	0112443205				
DV	Dividend GLEN BURNI COM USD1 Gross 14.40 RecDte: 10/24/2019 PSS #: 1610196060930 UNITS/QNTY: 144.0000 SEDOL #: 2690153 ISIN #: US3774071019 EVENT ID: 0115248584	377407101 US3774071019 PSS1610196060930 0115248584	10/20/2019 124/2019 12/4/2019 12/4/2019	144.0000 0.1000000000 14.40	14.40	14.40

DESC: GLEN BURNI COM USD1 DIV SRC RATE: 0.1000000000

EX DT: 19OCT20 RECORD DT: 19OCT24 PAY DT: 19NOV04

CCY: USD GRSS: 14.4000 WTH: 0.0000

AMOR BAL: 0.0000 PRFC: 0.0000 CUFC: 0.0000

#### DV Dividend

#### **COLUMBIA F AMT-FREE CONN INTER MUNI**

Gross 1.06 RecDte: 8/31/2019

PSS #: 1611046018899 UNITS/QNTY: 41.7940

SEDOL #: BWK1TF4 ISIN #: US19765N4016 EVENT ID: 0113349658

DESC: COLUMBIA F AMT-FREE CO DIV SRC RATE: 0.0000000000

EX DT: 19AUG31 RECORD DT: 19AUG31 PAY DT: 19AUG31

CCY: USD GRSS: 1.0600 WTH: 0.0000

AMOR BAL: 0.0000 PRFC: 0.0000 CUFC: 0.0000

Cash Dividend includes
number of shares, date,
payment rate and more

8/31/2019

8/31/2019

12/4/2019

8/31/2019\*

19765N401

0113349658

US19765N4016

PSS1611046018899

SUBTOTAL DIVIDEND (3) 16.12 16.12

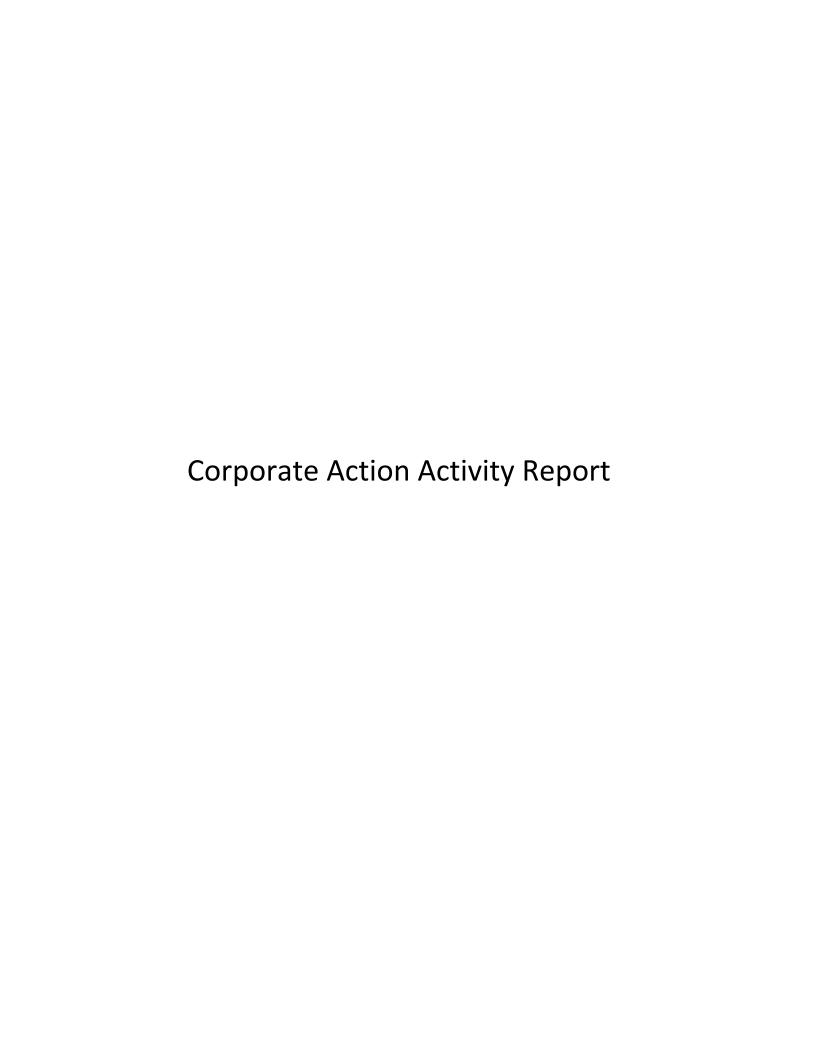
1.06

1.06

41.7940

1.06

<sup>\*</sup>Back Valued Transaction



Corporate Action Report PDF **Custody Security Transactions** AVENU By Security Actual Settle Date 1/4/2020 XXXXXX- STATE NAME Description **Trading Broker ISIN Create Date Clearing Broker** Reference Number Trade/Ex Date Shares/Par **Buver Order Party** Client Reference Contract Settle/Pay Date **Local Net Amount Seller Order Party** Local Price Status Market Reference Actual Settle Date Cash Offset Number **Settlement Policy Order Date Days Late Local Currency** Comments CA Receipt of Rights 10/31/2019 180.0000 Settled - ACTUAL 1163054005692 1/1/2020 SG1DC4000002 CHARISMA ENERGY SERVIC RITS 22NOV19 (SGD) 1/1/2020 1/4/2020 Actual Corporate Action Activity - Includes rate, C/DECL// SG2B54957198 114485890 C/DECL// type, payable date, SG2B54957198 114485890 ORIG EVENT: event ID and more SG2B54957198 NEW CODE: RATIO: 000001.000000/000010.000000 CA US0138175072 1/4/2020 Name Change -3.705.0000 Settled - ACTUAL **ALCOA INC USD 1.0** 1163094004290 1/1/2020 1/4/2020 1/4/2020

SETTLEMENT **UNITED STATES** DOLLAR (USD) Actual

C/DECL// US0138175072 115377487 C/DECL// US0138175072 115377487 ORIG EVENT: US0138175072 NEW CODE: RATIO: 000001.000000/000001.000000

CA Spinoff/Demerger **ALCOA CORP USD 0.01** 

00 EXCHANGE UNDER REORGANIZATION **EXCHANGE UNDER REORGANIZATION** 

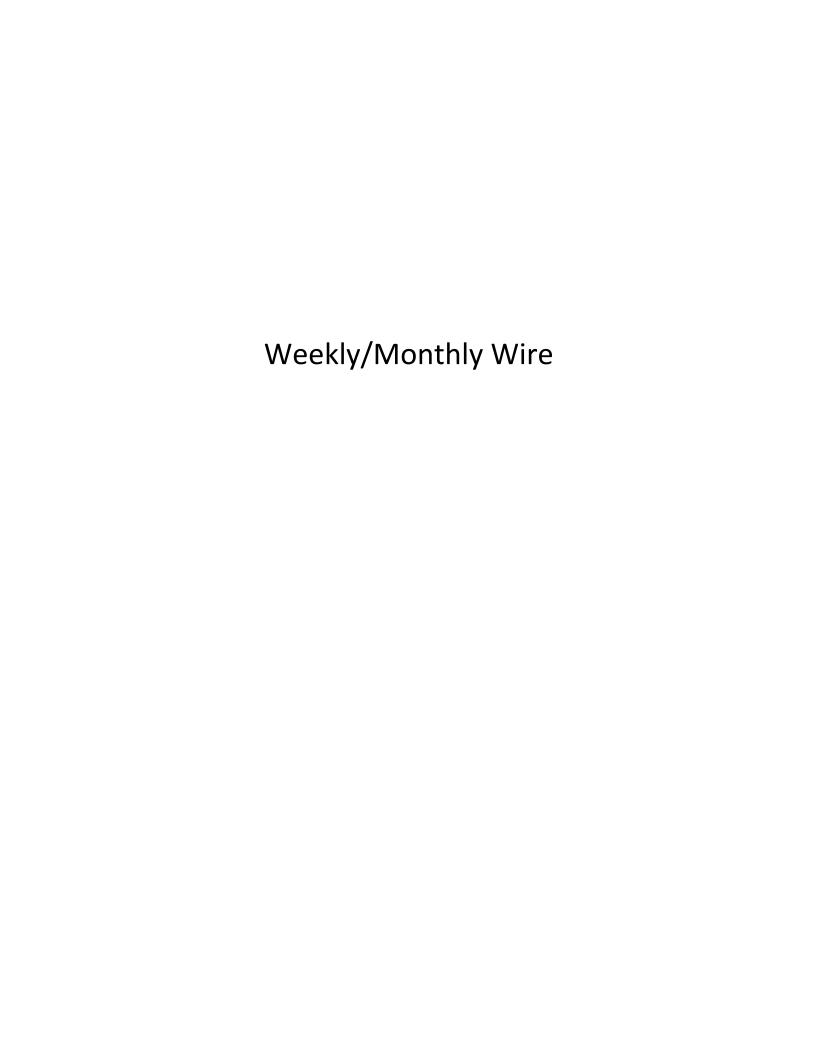
US0138721065 10/31/2019 1163054007461 1/1/2020 1/4/2020 1/4/2020 Actual

Settled - ACTUAL 1.235.00 **SETTLEMENT UNITED STATES** DOLLAR (USD)

Report ID ICUS0015

SETTLEMENT

SINGAPORE DOLLAR





#### Weekly/Monthly Sale Wire Report - Sample

Actual CUSIP/CINS Security Short Descript	on Shares / Par	Local Local Pr	incipal Commissio	n Local Income	Miscellaneous	Foreign	Local Amount Transaction Type Name	Transaction Description 1	Transaction Description 2
Settle Date	Price		mount	Amount	Fees	Exchange Fees			
12/29/2019 52469H115 LEGG MASON CLEARBI			349.18 \$ (14.37		\$ -	\$ -		1181780289545	SALE 6-22-18 SALE OF SHARES
12/16/2019 4812C2601 JP MORGAN INVESTOR			298.57 \$ (69.54	) \$ -	\$ -	\$ -		1181940123132	SALE 7-11-18 SALE OF SHARES
12/16/2019 641224100 NEUBERGER GENESIS		62.03 \$ 29,8	326.51 \$ (67.32	) \$ -	\$ -	\$ -	\$ 29,759.19 SELL	1181940123861	SALE 7-11-18 SALE OF SHARES
12/5/2019 939330106 WASHINGTON MUTUAL		44.28 \$ 3,2	289.30 \$ (10.40	) \$ -	\$ -	\$ -		GSP #:1181860157475 UNITS/QNTY: 74.2840	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 939330106 WASHINGTON MUTUAL		44.28 \$ 2	204.62 \$ (0.65	) \$ -	\$ -	\$ -		GSP #:1181860160230 UNITS/QNTY: 4.6210	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 19765P638 COLUMBIA FUNDS SER		20.02 \$ 27,0	20.29 \$ (188.95	) \$ -	\$ -	\$ -		GSP #:1181860160890 UNITS/QNTY: 1,349.6650	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746704105 PUTNAM DIVERSIFIED		7.04 \$	138.19 \$ (2.75	) \$ -	\$ -	\$ -		GSP #:1181860161539 UNITS/QNTY: 19.6290	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746745108 PUTNAM EQUITY INCO		24.44 \$ 2,	110.39 \$ (12.09	) \$ -	\$ -	\$ -		GSP #:1181860162098 UNITS/QNTY: 86.3500	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746745108 PUTNAM EQUITY INCO	E FUND SHS -A0.357 \$ 2	24.44 \$	8.73 \$ (0.05	) \$ -	\$ -	\$ -	\$ 8.68 SELL	GSP #:1181860163361 UNITS/QNTY: 0.3570	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746745108 PUTNAM EQUITY INCO	E FUND SHS -A10.882 \$ 2	24.44 \$ 2	265.96 \$ (1.52	) \$ -	\$ -	\$ -		GSP #:1181860164060 UNITS/QNTY: 10.8820	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746745108 PUTNAM EQUITY INCO	E FUND SHS -A26.048 \$ 2	24.44 \$ (	36.61 \$ (3.65	) \$ -	\$ -	\$ -	\$ 632.96 SELL	GSP #:1181860164413 UNITS/QNTY: 26.0480	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746778109 PUTNAM GLOBAL HEAL	TH CARE FUND, -168.471 \$ 5	51.14 \$ 8,6	315.61 \$ (23.59	) \$ -	\$ -	\$ -	\$ 8,592.02 SELL	GSP #:1181860164670 UNITS/QNTY: 168.4710	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 746778109 PUTNAM GLOBAL HEAL	TH CARE FUND, -37.072 \$ 5	51.14 \$ 1,8	395.86 \$ (5.19	) \$ -	\$ -	\$ -	\$ 1,890.67 SELL	GSP #:1181860165002 UNITS/QNTY: 37.0720	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 74926P803 RBC FUNDS TRUST - R		24.10 \$	86.66 \$ (0.50	) \$ -	\$ -	\$ -	\$ 86.16 SELL	GSP #:1181860166091 UNITS/QNTY: 3.5960	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 74926P803 RBC FUNDS TRUST - R	C ENTERPRISE -0.770 \$ 2	24.10 \$	18.56 \$ (0.11	) \$ -	\$ -	\$ -	\$ 18.45 SELL	GSP #:1181860167612 UNITS/QNTY: 0.7700	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 921935102 VANGUARD W COM US	01 -3.212 \$ 4	40.98 \$	131.63 \$ (0.45	) \$ -	\$ -	\$ -	\$ 131.18 SELL	GSP #:1181860168018 UNITS/QNTY: 3.2120	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019 921935102 VANGUARD W COM US	-2869.568 \$ 4	40.98 \$ 117,	594.90 \$ (401.74	) \$ -	\$ -	\$ -	\$ 117,193.16 SELL	GSP #:1181860168420 UNITS/QNTY: 2,869.5680	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/16/2019 125325506 CGM TRUST - CGM FOO	US FUND SHS -253.119 \$ 4	43.44 \$ 10,9	95.49 \$ (35.44	) \$ -	\$ -	\$ -		SALE 6-22-18 SALE OF SHARES	TRADE DT:18JUN27 CONT SET DT:18JUL16 CALL/MAT DT:
12/17/2019 12601V109 CMTSU LIQ INC USD 0.0		0.00 \$	0.64 \$ (0.01	) \$ -	\$ -	\$ -	\$ 0.63 SELL	SPRO//MXA 17 07/13/18	1181970059381
12/17/2019 37426X204 GET REAL USA INC USI	0.0001 -1.000 \$	0.06 \$	0.06 \$ (0.01	) \$ -	\$ -	\$ -	\$ 0.05 SELL	SPRO//MXA 18 07/13/18	1181970059378
12/17/2019 65343N108 NEXGEN MNG INC USD	0.00001 -9424.000 \$	0.05 \$	171.20 \$ (0.01	) \$ -	\$ -	\$ -	\$ 471.19 SELL	SPRO//MXA 19 07/13/18	1181970059350
12/17/2019 949090104 WELBILT INC USD 0.01	-7.000 \$ 2	23.56 \$	164.92 \$ (0.98	) \$ -	\$ -	\$ -	\$ 163.94 SELL	SPRO//RVA 11 07/13/18	1181970059365
12/17/2019 961684107 WESTWATER RES INC	JSD 0.001 -1.000 \$	0.38 \$	0.38 \$ (0.14	) \$ -	\$ -	\$ -	\$ 0.24 SELL	SPRO//RVA 12 07/13/18	1181970059362
12/9/2019 03211P301 AMPLIPHI BIOSCIENCE	CORP USD 0.01 -3.000 \$	1.12 \$	3.36 \$ (0.4)	2) \$ -	\$ -	\$ -	\$ 2.94 SELL	SPRO//RVA 21 07/05/18	1181860116081
12/9/2019 746909100 PUTNAM MAS SBI NPV	-706.000 \$	4.59 \$ 3,2	240.61 \$ (98.84	) \$ -	\$ -	\$ -	\$ 3,141.77 SELL	SPRO//RVA 23 07/05/18	1181860116084
12/9/2019 746922103 PUTNAM MUN COM SBI	NPV -3.000 \$ 1	11.66 \$	34.98 \$ (0.42	) \$ -	\$ -	\$ -	\$ 34.56 SELL	SPRO//RVA 24 07/05/18	1181860116086
12/9/2019 812578102 SEATTLE GE COM USD	.001 -52.000 \$ 6	67.99 \$ 3,5	35.49 \$ (7.28	) \$ -	\$ -	\$ -	\$ 3,528.21 SELL	SPRO//RVA 25 07/05/18	1181860116088
12/9/2019 949746101 WELLS FARGO + CO NI	W USD 1.666 -4.000 \$ 5	55.35 \$ 2	221.41 \$ (0.56	) \$ -	\$ -	\$ -	\$ 220.85 SELL	SPRO//RVA 26 07/05/18	1181860116091
12/9/2019 925550105 VIAVI SOLUTIONS INC I	SD 0.001 -10.000 \$ 1	10.06 \$	100.63 \$ (1.40	) \$ -	\$ -	\$ -	\$ 99.23 SELL	SPRO//RVA 27 07/05/18	1181860116090
12/17/2019 023135106 AMAZON COM INC USD	0.01 -4.000 \$1,80	05.43 \$ 7,2	221.72 \$ (0.56	) \$ -	\$ -	\$ -	\$ 7,221.16 SELL	SPRO//RVA 4 07/13/18	1181970059375
12/17/2019 46138G706 INVESCO EX SOLAR ET	-1.000 \$ 2	23.28 \$	23.28 \$ (0.14	) \$ -	\$ -	\$ -	\$ 23.14 SELL	SPRO//RVA 6 07/13/18	1181970059370
12/17/2019 759892201 RENREN INC USD 0.001	ADR -31.000 \$	2.39 \$	74.09 \$ (4.34	) \$ -	\$ -	\$ -	\$ 69.75 SELL	SPRO//RVA 7 07/13/18	1181970059372
12/17/2019 87968A104 TELLURIAN INC NEW U	D 0.01 -6.000 \$	98.02 \$	48.12 \$ (0.84	) \$ -	\$ -	\$ -	\$ 47.28 SELL	SPRO//RVA 8 07/13/18	1181970059368
12/17/2019 89854H102 TTEC HLDGS INC USD		35.30 \$ 4,2	236.00 \$ (16.80	) \$ -	\$ -	\$ -		SPRO//RVA 9 07/13/18	1181970059358
12/9/2019 656811106 NORTH AMERN CONST		5.80 \$	52.20 \$ (1.26	) \$ -	\$ -	\$ -		SPRO// CNDT STATE LOCAL SOLUTIONS	UNCLAIMED PROPERTY
12/17/2019 09368L100 BLOCKCHAIN INDS INC	JSD 0.001 -200.000 \$	4.31 \$ 8	362.00 \$ (28.00	) \$ -	\$	\$ -		SPRO// CNDT STATE LOCAL SOLUTIONS	UNCLAIMED PROPERTY
12/17/2019 24373L102 DEEP GREEN WASTE +				\$ -	\$ 0.15	\$ 3.30		SPRO// CNDT STATE LOCAL SOLUTIONS	UNCLAIMED PROPERTY
12/17/2019 92846K100 VITA MOBILE SYS INC N		0.03 \$	3.00 \$ (0.01		\$ -	\$ -		SPRO// CNDT STATE LOCAL SOLUTIONS	UNCLAIMED PROPERTY
12/17/2019 98420U109 XPRESSPA GROUP INC	NPV -40.000 \$	0.30 \$	12.05 \$ (5.60	) \$ -	\$ -	\$ -	\$ 6.45 SELL	SPRO// CNDT STATE LOCAL SOLUTIONS	UNCLAIMED PROPERTY
							\$ 230,787.50		





# Weekly/Other Proceeds Wire Report - Sample Report

Actual	CUSIP/CINS	Security Short Description	Shares / Par	Local	Local P	rincipal Com	mission	Local Income	Miscellane	eous	Forei	gn L	Local Amount Transaction Type Name	Transaction Description 1	Transaction Description 2
Settle Date			F	Price/Rate		Amount		Amount	F	Fees E	Exchange Fe	es			
12/6/2019	31641P302	FIDELITY SYSTEMATIC INVT PLANS	0.941 \$	-	\$	(40.65) \$	-	\$ -	\$	- \$	-	9	\$ (40.65) CORPORATE ACTION	C/DECL// US31641P3029 138894108	C/DECL// US31641P3029 138894108
12/5/2019	353496805	FRANKLIN CUSTODIAN FUNDS - FRANKLIN	0.129		\$	(0.30) \$	-	\$ -	\$	- \$	-		\$ 0.30) CORPORATE ACTION	C/DECL// US3534968058 149933669	C/DECL// US3534968058 149933669
12/18/2019	353612682	FRANKLIN I BALANCED FD A	0.002 \$	-	\$	(0.03) \$	-	\$ -	\$	- \$	-	9	\$ (0.03) CORPORATE ACTION	C/DECL// US3536126820 150527561	C/DECL// US3536126820 150527561
12/2/2019	354014102	FRANKLIN M COM USD0.01	0.020 \$	- 3	\$	(0.02) \$	-	\$ -	\$	- \$	-	9		C/DECL// US3540141021 149655680	C/DECL// US3540141021 149655680
12/2/2019	416645596	THE HARTFORD MUTUAL FUNDS, INC	0.150 \$	- 3	\$	(3.68) \$	-	\$ -	\$	- \$	-	9	\$ (3.68) CORPORATE ACTION	C/DECL// US4166455968 149656027	C/DECL// US4166455968 149656027
12/3/2019		INVESCO SE CLASS IB	2.942 \$	ş -	\$	(19.80) \$	-	\$ -	\$	- \$	-	9	\$ (19.80) CORPORATE ACTION	C/DECL// US46131G4064 149933834	C/DECL// US46131G4064 149933834
12/12/2019		GLAXOSMITHKLINE PLC 25P ADR	1.000 \$	0.50	\$	- \$	-	\$ 0.50	\$	- \$	-	9	\$ 0.50 DIVIDEND	PSS #: 1805096075612 UNITS/QNTY: 1.0000	SEDOL #: 2374112 ISIN #: US37733W1053 EVENT ID: 0145628242
		BK OF AMER COM USD0.01	132.000 \$		\$	- \$	-	\$ 15.84		- \$	-	9	\$ 15.84 DIVIDEND	PSS #: 1805306079309 UNITS/QNTY: 132.0000	SEDOL #: 2295677 ISIN #: US0605051046 EVENT ID: 0145647639
		PEPSICO INC USD 0.017	3.000 \$	0.93	\$	- \$	-	\$ 2.78		- \$	-	9	\$ 2.78 DIVIDEND	PSS #: 1805306092757 UNITS/QNTY: 3.0000	SEDOL #: 2681511 ISIN #: US7134481081 EVENT ID: 0146270822
		PRINCIPAL COM USD0.01	42.000 \$	0.52	\$	- \$	-	\$ 21.84		- \$	-	9	\$ 21.84 DIVIDEND	PSS #: 1806046016649 UNITS/QNTY: 42.0000	SEDOL #: 2803014 ISIN #: US74251V1026 EVENT ID: 0145664920
		DXC TECHNOLOGY CO USD 0.01	62.000 \$	0.19	\$	- \$	-	\$ 11.78	\$	- \$	-	9	\$ 11.78 DIVIDEND	PSS #: 1806046111071 UNITS/QNTY: 62.0000	SEDOL #: BYXD7B3 ISIN #: US23355L1061 EVENT ID: 0147286359
12/5/2019		PULTE GROUP INC	541.000 \$		\$	- \$	-	\$ 48.69	\$	- \$	-	9	\$ 48.69 DIVIDEND	PSS #: 1806056056935 UNITS/QNTY: 541.0000	SEDOL #: 2708841 ISIN #: US7458671010 EVENT ID: 0146764669
12/2/2019		FIRST HORIZON NATL CORP USD 0.625	5.000 \$		\$	- \$	-	\$ 0.60	\$	- \$	-	\$	\$ 0.60 DIVIDEND	PSS #: 1806066085307 UNITS/QNTY: 5.0000	SEDOL #: 2341484 ISIN #: US3205171057 EVENT ID: 0145621265
12/2/2019	124857202	CBS CORPOR CLASS B COM STK USD 0.0	159.000 \$		\$	- \$	-	\$ 28.62	\$	- \$	-	9	\$ 28.62 DIVIDEND	PSS #: 1806066137254 UNITS/QNTY: 159.0000	SEDOL #: B0SRLH6 ISIN #: US1248572026 EVENT ID: 0147350873
12/5/2019			24.810 \$		\$	- \$	-	\$ -	\$	- \$	-	9	\$ (18.88) FOREIGN EXCHANGE	PSS1805230005012	EXCH RATE: 1.31425510000 THEIRS TRADE DT :29JUN18
12/5/2019			-18.880 \$	1.31	\$	24.81 \$	-	\$ -	\$	- \$	-	9	\$ 24.81 FOREIGN EXCHANGE	PSS1805230005012	EXCH RATE: 1.31425510000 OURS TRADE DT :29JUN18
		FEDERAL HOME LN MTG 6.5195 15JUL21	20000.000 \$	0.00	\$	- \$	-	\$ 0.16	\$	- \$	-	9	\$ 0.16 INTEREST	PSS #: 1806146213965 UNITS/QNTY: 20,000.0000	SEDOL #: ISIN #: US312903SA62 EVENT ID: 0147010204
12/16/2019		BANK AMER CORP SUB INT 6.05 15FEB38	150000.000 \$	0.01	\$	- \$	-	\$ 756.25	\$	- \$	-	9	\$ 756.25 INTEREST	PSS #: 1806296109021 UNITS/QNTY: 150,000.0000	SEDOL #: B2PZHY6 ISIN #: US06050XA944 EVENT ID: 0146928328
12/16/2019	36207UKJ6	GNMA I + II - SI 442297 7.0 15JAN27	25000.000	0.00	\$	- \$	-	\$ 0.51	\$	- \$	-	9	\$ 0.51 INTEREST	PSS #: 1806296354572 UNITS/QNTY: 25,000.0000	SEDOL #: ISIN #: US36207UKJ69 EVENT ID: 0146674276
		GNMA I + II - SI 352054 6.5 15OCT23	25000.000		\$	- \$	-	\$ 0.62	\$	- \$	-	9		PSS #: 1806296580764 UNITS/QNTY: 25,000.0000	SEDOL #: ISIN #: US36203LBX91 EVENT ID: 0146695674
12/12/2019	26842F103	E-DIRECT INC NPV	1344.000 \$	-	\$	- \$	-	\$ -	\$	- \$	-	9	\$ - INTERNAL MOVEMENT	1181920119206	
12/12/2019	26842F103	E-DIRECT INC NPV	-1344.000 \$	-	\$	- \$	-	\$ -	\$	- \$	-	9	\$ - INTERNAL MOVEMENT	DTC ARF # 20171009DTC 9002	AWAITING SECURITY FROM REGISTR
12/5/2019	918231101	VHGI HLDGS INC USD 0.0001	100000.000 \$	-	\$	- \$	-	\$ -	\$	- \$	-	9	\$ - INTERNAL MOVEMENT	DTC ARF # 20171009DTC 9010	1181860102907
12/5/2019	918231101	VHGI HLDGS INC USD 0.0001	-100000.000 \$	- 6	\$	- \$	-	\$ -	\$	- \$	-	9	\$ - INTERNAL MOVEMENT	DTC ARF # 20171009DTC 9010	AWAITING SECURITY FROM REGISTR
			0.000 \$	-	\$	- \$	-	\$ 0.34	\$	- \$	-	9	\$ 0.34 OTHER	CR INTEREST-ACCOUNT 9124838400	
			0.000 \$	- 3	\$	- \$	-	\$ 0.01	\$	- \$	-	9	\$ 0.01 OTHER	CR INTEREST-ACCOUNT 9124838401	
12/16/2019	312903SA6	FEDERAL HOME LN MTG 6.5195 15JUL21	20000.000 \$	- 6	\$	2.65 \$	-	S -	\$	- \$	-	9	\$ 2.65 PAY DOWN	PSS #: 1806146214035 UNITS/QNTY: 20,000.0000	SEDOL #: ISIN #: US312903SA62 EVENT ID: 0147010204
12/16/2019	36207UKJ6	GNMA I + II - SI 442297 7.0 15JAN27	25000.000	- 6	\$	0.88 \$	-	\$ -	\$	- \$	-	9	\$ 0.88 PAY DOWN	PSS #: 1807096182918 UNITS/QNTY: 25,000.0000	SEDOL #: ISIN #: US36207UKJ69 EVENT ID: 0146674276
12/16/2019	36203LBX9	GNMA I + II - SI 352054 6.5 15OCT23	25000.000	-	\$	1.56 \$	-	\$ -	\$	- \$	-	9	\$ 1.56 PAY DOWN	PSS #: 1807096230584 UNITS/QNTY: 25,000.0000	SEDOL #: ISIN #: US36203LBX91 EVENT ID: 0146695674
12/29/2019	G1151C101	ACCENTURE PLC USD 0.000023	21.000 \$	-	\$	- S	-	S -	S	- \$	-	9	\$ - SECURITY DEPOSIT	B/C A REC FROM MORGAN STANLEY	AWAITING SECURITIES FROM CPY
12/29/2019	G51502105	JOHNSON CONTROLS INTERNATI USD 0.01	56.000		s	- Š	-	Š -	Š	- s	-	9	\$ - SECURITY DEPOSIT	B/C A REC FROM MORGAN STANLEY	AWAITING SECURITIES FROM CPY
		QIAGEN NV EUR 0.01	296.000		Š	- \$	-	s -	s	- Š	-	9	\$ - SECURITY DEPOSIT	B/C A REC FROM MORGAN STANLEY	AWAITING SECURITIES FROM CPY
12/5/2019	896887106	TROILUS GOLD CORP NPV	-2.000 S		\$	- \$		s -	s	- \$	_	9	\$ - SECURITY WITHDRAWAL	6/29/19 SALE, PROCEEDS POST	SEPERATE
		JP MORGAN STRG INCM CL A	-1150.501 \$		s	- \$	_	s -	s	- \$	-	9		CL 1018837. LUCINDA J MAR 27	4TH ST RENTON MA 98056 W-9 NOT
12/29/2019		CAP INC BU SBI NPV	-167.149 \$		\$	- \$	-	š -	š	- Š	_	S		CL 11881, CAROL LIMIAS 32	6TH AVE NW SEATTLE WA 98117 W-9
		COSTCO WHOLESALE CORP NEW USD 0.005	-1100.000 \$	_	\$	- \$	_	š -	s	- \$	-	Š	- SECURITY WITHDRAWAL		A/C 5680992
.2,.2,2013		COUNCIL SOM NEW COD 0.000			Ψ			*	-	Ψ		-	025.00		

\$ 835.08

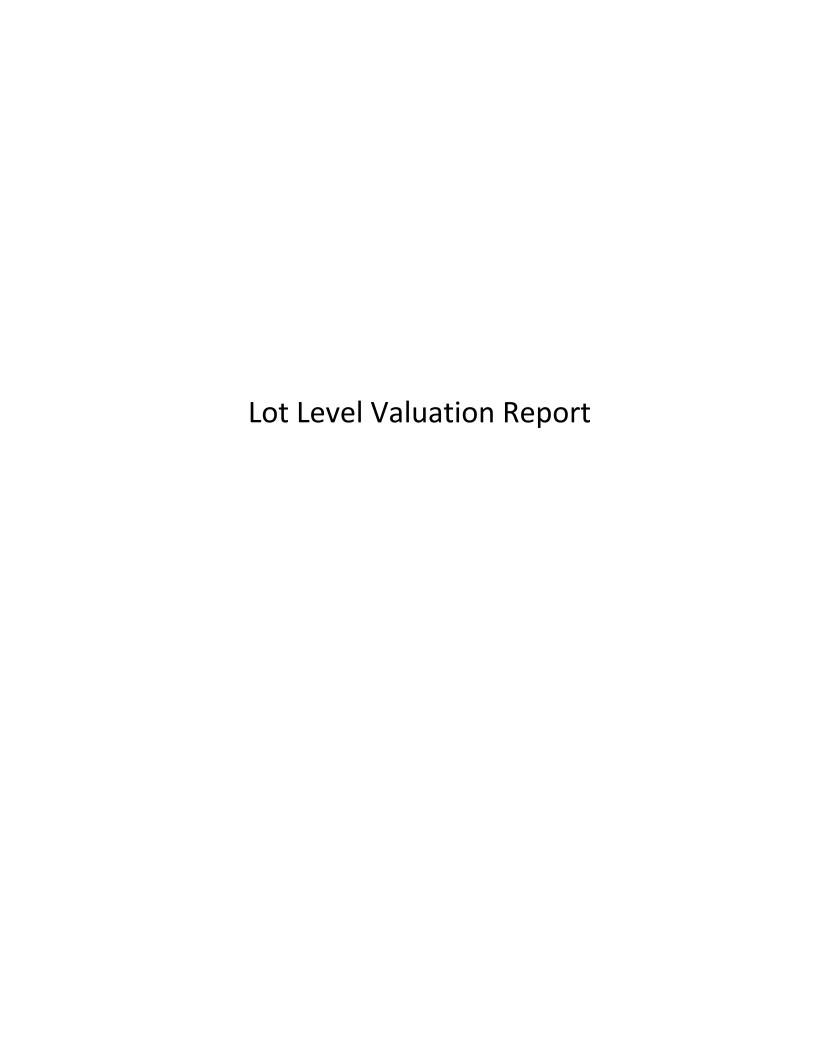


# Position – Unable to Trade Report



# Position - Unable to Trade Report Days Units CUSIP Location Comments

			Position - Unable to Th	aue Keport	
AC#	Security Description	Davs	Units CUSIP	Location	Comments
XXXXXX	ACT TELECONFERENCING INC ADEX MINING INC	381.00 786.00	810.000 000955104	NYC NYC	private company - no market chilled for deposit has value cannot sell
XXXXXX	ALL STATE PROPERTIES HOLDINGS	1.660.00	540.000 006903207 1.000 016663205	NYCR	RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
	ALTAIR NANOTECHNOLOGIES INC NPV	88.00	223.0000 021373303	DTC	RESTRICTED - RATIMOND JAMES CANNOT SELL THEM RESTRICTED FROM TRADING PER BROKER
XXXXXX	ANDALAY SOLAR INC USD 0.001	94.00	75.0000 021373303	DTC	RESTRICTED FROM TRADING FER BROKER  RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
XXXXXX	ARETE INDS INC NPV	101.00	3.0000 033335106	DTC	RESTRICTED - RAYMOND JAMES CANNOT SELL THEM  RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
XXXXXX	ATLANTIC WIND & SOLAR INC	324.00	72.000 040090303	DTC	restricted from trading per raymond james
XXXXXX	ATLANTIC WIND & SOLAR INC	324.00	18.000 049127103	DTC	restricted from trading per raymond james
XXXXXX	ATLANTIC WIND & SOLAR INC	324.00	32.000 049127103	DTC	restricted from trading per raymond james
XXXXXX	ATLANTIC WIND & SOLAR INC	324.00	1.000 049127103	DTC	restricted from trading per raymond james
XXXXXX	AURORA GOLD CORP USD 0.001	94.00	30.0000 051642205	DTC	RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
XXXXXX	AVITAR INC NEW USD 0.01	94.00	1.0000 051042205	DTC	restricted from trading per raymond james
XXXXXX	B-FAST CORP	381.00	570.000 055413108	DTC	restricted from trading per raymond james
	BETTWORK INDS INC USD 0.001	94.00	1.0000 033413108	DTC	restricted from trading per raymond james
XXXXXX	BIG BUCK B COM USD0.01	86.00	24.0000 087700101	DTC	restricted from trading per raymond james
XXXXXX	BIOSYNERGY INC NPV	72.00	4,000.0000 090917105	DTC	restricted from trading per raymond james
	BRIGHTROCK GOLD CORP USD 0.001	99.00	1.0000 109476101	DTC	restricted from trading per raymond james
XXXXXX	CGE ENERGY INC USD 0.01	99.00	140.0000 109476101	DTC	restricted from trading per raymond james
XXXXXX	CAMPBELL R COM NPV	1,526.00	10.0000 125286104	YCA	
				DTC	cant be sold has no value on foreign marekt
XXXXXX	CARRIOVASCULAR RIOTHERAREUTICS	304.00	170.000 137648101	NYC	this security is restricted from trading
XXXXXX	CARDIOVASCULAR BIOTHERAPEUTICS	157.00	780.000 141607101		no quotes for this security - will most likely sell as worthless delisted
XXXXXX	CLEARSTORY SYSTEMS INC	414.00	1,000.000 185066107	DTC	restricted from trading per raymond james
XXXXXX	COMMONWEALTH EDISON CO LEGENDED CON		1,965.00 202795720	DTCR	cant be sold. No market. Subsidiary of Exelon.
XXXXXX	CONECTISYS CORP	99.00	20.000 206827305	DTC	restricted from trading per raymond james
XXXXXX	CROSSWIND RENEWABLE ENERG USD 0.001	99.00	1.0000 227692100	DTC	restricted from trading per raymond james
XXXXXX	CYBER DIGITAL INC	319.00	600.000 232441105	DTC	restricted from trading per raymond james
XXXXXX	EVEROCK INC	414.00	55,754.000 300398401	DTC	restricted from trading per raymond james
XXXXXX	EVEROCK INC	451.00	2,500.000 300398401	DTC	restricted from trading per raymond james
XXXXXX	FEDERAL CASTERS CORP	157.00	400.000 313200107	NYC	cant deposit to DTC and this has value cannot sell
XXXXXX	FEDERAL SCREW WKS USD 1.0		43.0000 313819104	DTC	restricted from selling per raymond james
XXXXXX	FIRST INDEPENDENCE CORP DETROIT MICH	3,299.00	451.000 320539208	NYC	CANT SELL NO MARKET worthless
XXXXXX	FLAMEMASTE COM USD0.01	101.00	112.0000 338490204	DTC	restricted from trading per raymond james
XXXXXX	GT LEGEND AUTOMOTIVE HLDG USD 0.001	71.00	3.0000 362369100	DTC	restricted from trading per raymond james
XXXXXX	GENERAL FINANCE + DEVELOPM RESTR		3.0000 368992855	NYV	this is a worthless security
XXXXXX	GLOBAL NET COM NPV	80.00	50.0000 379382104	DTC	restricted from trading per raymond james
XXXXXX	GOLD DYNAM USD 0.001	94.00	1,900.0000 380584102	DTC	restricted from trading per raymond james
XXXXXX	GOLD ROCK HLDGS INC USD 0.001	80.00	1.0000 380709303	DTC	restricted from trading per raymond james
XXXXXX	GOLDSANDS DEV CO USD 0.001	71.00	1,100.0000 381454107	DTC	restricted from trading per raymond james
XXXXXX	GREAT BASIN ENERGIES INC USD 0.01	72.00	2,000.0000 390123107	DTC	restricted from trading per raymond james
XXXXXX	GREAT BASIN GOLD LTD NPV	88.00	214.0000 390124105	DTC	restricted from trading per raymond james
XXXXXX	GREEN STAR PRODS INC USD 0.001	71.00	5,000.0000 393411103	DTC	restricted from trading per raymond james
XXXXXX	HAT TRICK BEVERAGE INC	319.00	50,000.000 418756102	DTC	has been designated as restricted from selling
XXXXXX	HEMP INC	324.00	3.000 423703206	DTC	restricted from trading per raymond james
XXXXXX	HEMP INC	413.00	101.000 423703206	DTC	restricted from trading per raymond james
XXXXXX	HIRU CORP	456.00	60,000.000 433570108	DTC	RESTRICTED FROM SELLING PER RAYMOND JDAMES
XXXXXX	HOP-ON INC	456.00	400,000.000 439338203	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES
XXXXXX	HORIZON GROUP PROPERTIES, L.P RESTR		119.0000 440994911	NYV	this is a private company and can't sell
XXXXXX	HOP-ON INC COM NPV	456.00	400,000.0000 439338203	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES
XXXXXX	HYSTER-YALE MATLS HANDLING USD 0.01		1.0000 449172204	NYVT	can this be deposited/sold? Worthless
XXXXXX	ICOA INC USD 0.0001	786.00	1.0000 449292309	DTC	has value - cannot sell restricted
XXXXXX	IVANHOE ENERGY INC NPV	71.00	4.0000 465790509	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES
XXXXXX	JAYHAWK ENERGY INC USD 0.001	80.00	125.0000 472100106	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES
XXXXXX	JUNIPER GROUP INC USD 0.001		7,500.0000 481905875	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES
XXXXXX	KENILWORTH SYS CORP USD 0.01	86.00	1.0000 489084202	DTC	restricted from trading
XXXXXX	LBO CAP CORP USD 0.0001	72.00	42,000.0000 501792303	DTC	restricted from trading per raymond james
XXXXXX	LONE STAR GOLD INC USD 0.001	94.00	47.0000 542281100	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES
XXXXXX	LOUD TECHN COM STK NPV	87.00	50.0000 545731200	DTC	restricted from trading per raymond james
XXXXXX	MANATI INDS INC USD 0.01	101.00	200.0000 562020107	DTC	RESTRICTED FROM SELLING PER RAYMOND JAMES



# LOT LEVEL VALUATION REPORT



Reporting Account Name	Reporting Account Number	CUSIP	Security Description	Ticke <b>r</b>	ISIN	Units	Base P <b>r</b> ice	Base <b>M</b> arket Reporte <b>d</b> Value Date
STATE OF NAME	AUZFXXXXXXXX	88579Y101	3M CO	MMM	US88579Y1010	24.000	153.650000	3,687.60 4/10/2018
STATE OF NAME	AUZFXXXXXXXX	81785L302	727 COMMUNICATIONS INC	SVNJ	US81785L3024	6.000	0.000000	0.00 11/19/2019
STATE OF NAME	AUZFXXXXXXXX	002824100	ABBOTT LABORATORIES	ABT	US0028241000	10.000	94.950000	949.50 10/18/2016
STATE OF NAME	AUZFXXXXXXXX	002824100	ABBOTT LABORATORIES	ABT	US0028241000	14.000	94.950000	1,329.30 8/19/2019
STATE OF NAME	AUZFXXXXXXXX	00287Y109	ABBVIE INC	ABBV	US00287Y1091	25.000	84.690000	2,117.25 4/6/2020
STATE OF NAME	AUZFXXXXXXXX	00287Y109	ABBVIE INC	ABBV	US00287Y1091	10.000	84.690000	846.90 11/14/2019
STATE OF NAME	AUZFXXXXXXXX	00287Y109	ABBVIE INC	ABBV	US00287Y1091	14.000	84.690000	1,185.66 11/14/2019
STATE OF NAME	AUZFXXXXXXXX	00326L100	ABERDEEN TTL DYN DIVID	AOD	US00326L1008	224.000	7.040000	1,576.96 3/30/2020
STATE OF NAME	AUZFXXXXXXXX		ABILITY HOLDING CORP	AYHC	US0035011032	681.000	0.000000	0.00 3/30/2020
STATE OF NAME	AUZFXXXXXXXX		ACCESS-POWER INC	ACCR	US00431N1081	3,100.000	0.000000	0.00 2/2/2016
STATE OF NAME	AUZFXXXXXXXX		ACCESS-POWER INC	ACCR	US00431N1081	15,000.000	0.000000	0.00 3/10/2015
STATE OF NAME	AUZFXXXXXXXX		ADVANCE AUTO PARTS INC	AAP	US00751Y1064	4.000	118.950000	475.80 10/31/2019
STATE OF NAME	AUZFXXXXXXXX		ADVANCE AUTO PARTS INC	AAP	US00751Y1064	69.000	118.950000	8,207.55 11/25/2019
STATE OF NAME	AUZFXXXXXXXX		ADVANCE AUTO PARTS INC	AAP	US00751Y1064	69.000	118.950000	8,207.55 10/2/2019
STATE OF NAME	AUZFXXXXXXXX		ADVANCED MICRO DEVICES INC	AMD	US0079031078	4.000	56.490000	225.96 10/4/2019
STATE OF NAME	AUZFXXXXXXXX		ADVANCED MICRO DEVICES INC	AMD	US0079031078	5,100.000	56.490000	288,099.00 12/12/2019
STATE OF NAME	AUZFXXXXXXXX		AF CAP WLRD GR & INC-A	CWGI	US1405431099	250.512	44.720000	11,202.90 12/27/2019
STATE OF NAME	AUZFXXXXXXXX		AF CAP WLRD GR & INC-A	CWGI	US1405431099	2.134	44.720000	95.43 12/12/2019
STATE OF NAME	AUZFXXXXXXXX		AF CAP WLRD GR & INC-A	CWGI	US1405431099	138.221	44.720000	6,181.24 12/12/2019
STATE OF NAME	AUZFXXXXXXXX		AF CAP WLRD GR & INC-A	CWGI	US1405431099	0.694	44.720000	31.04 10/15/2019
STATE OF NAME	AUZFXXXXXXXX		AF CAP WLRD GR & INC-A	CWGI	US1405431099	24.684	44.720000	1,103.87 9/3/2019
STATE OF NAME	AUZFXXXXXXXX		AFFILIATED RESOURCES CORP	AFFL	US00827A1088	750.000	0.000000	0.00 9/30/2019
STATE OF NAME	AUZFXXXXXXXXX		AGNICO EAGLE MINES LTD	AEM	CA0084741085	18.000	60.820000	1,094.76 10/31/2019
STATE OF NAME	AUZFXXXXXXXX		ALCOA CORP	AA	US0138721065	8.000	7.370000	58.96 11/29/2019
STATE OF NAME	AUZFXXXXXXXX		ALEXANDRIA ADVANTAGE WARRANTY	AAWC	US01479R1005	3.000	0.002000	0.00 12/31/2019
STATE OF NAME	AUZFXXXXXXXX		ALEXANDRIA ADVANTAGE WARRANTY	AAWC	US01479R1005	3.000	0.002000	0.00 12/31/2019
STATE OF NAME	AUZFXXXXXXXX		ALEXANDRIA ADVANTAGE WARRANTY	AAWC	US01479R1005 US01479R1005			0.00 11/3/2019
STATE OF NAME	AUZFXXXXXXXX		ALEXCO RESOURCE CORP	AXU		1.000 300.000	0.002000 1.540000	462.00 10/1/2019
STATE OF NAME	AUZFXXXXXXXX		ALLIANCE DATA SYSTEMS CORP	ADS	CA01535P1062 US0185811082			
						4.000	41.390000	165.56 4/13/2020
STATE OF NAME STATE OF NAME	AUZFXXXXXXXX AUZFXXXXXXXXX		ALLIANZGI TECHNOLOGY-A ALLSCRIPTS HEALTHCARE SOLUTION	RAGT MDRX	US0189194725	76.061	56.760000	4,317.22 4/16/2020
			ALLSCRIPTS HEALTHCARE SOLUTION	MDRX	US01988P1084	121.000	6.680000	808.28 4/20/2020
STATE OF NAME	AUZFXXXXXXXX				US01988P1084	121.000	6.680000	808.28 4/27/2020
STATE OF NAME	AUZFXXXXXXXX		ALLSTATE CORP/THE	ALL	US0200021014	444.000	103.090000	45,771.96 4/9/2020
STATE OF NAME	AUZFXXXXXXXX		ALTRIA CROUP INC	MO	US02209S1033	1.000	39.750000	39.75 4/13/2020
STATE OF NAME	AUZFXXXXXXXX		ALTRIA GROUP INC ALTRIA GROUP INC	MO	US02209S1033 US02209S1033	16.000	39.750000	636.00 4/14/2020
STATE OF NAME	AUZFXXXXXXXX			MO		16.000	39.750000	636.00 4/17/2020
STATE OF NAME	AUZFXXXXXXXX		AMAZON.COM INC	AMZN	US0231351067	39.000	2,376.000000	92,664.00 4/20/2020
STATE OF NAME	AUZFXXXXXXXX		AMEDICACING	AMCP	US0233751082	249.598	31.090000	7,760.00 4/21/2020
STATE OF NAME	AUZFXXXXXXXX		AMEDISYS INC	AMED	US0234361089	38.000	191.990000	7,295.62 4/22/2020
STATE OF NAME	AUZFXXXXXXXX		AMER FND FNDMNTL INVST-A	ANCF	US3608021024	363.378	53.860000	19,571.54 4/23/2020
STATE OF NAME	AUZFXXXXXXXX		AMER FND FNDMNTL INVST-A	ANCF	US3608021024	152.392	53.860000	8,207.83 4/24/2020
STATE OF NAME	AUZFXXXXXXXX		AMER FND FNDMNTL INVST-A	ANCF	US3608021024	38.561	53.860000	2,076.90 4/27/2020
STATE OF NAME	AUZFXXXXXXXX		AMER FND GRW FD OF AM-A	AGTH	US3998741066	335.042	48.970000	16,407.01 12/28/2018
STATE OF NAME	AUZFXXXXXXXX		AMER FND GRW FD OF AM-A	AGTH	US3998741066	190.026	48.970000	9,305.57 10/11/2016
STATE OF NAME	AUZFXXXXXXXX		AMER FND GRW FD OF AM A	AGTH	US3998741066	47.164	48.970000	2,309.62 10/31/2019
STATE OF NAME	AUZFXXXXXXXX		AMER FND GRW FD OF AM-A	AGTH	US3998741066	13.042	48.970000	638.67 11/1/2019
STATE OF NAME	AUZFXXXXXXXX		AMER FND GRW FD OF AM-A	AGTH	US3998741066	27.328	48.970000	1,338.25 10/2/2019
STATE OF NAME	AUZFXXXXXXXX		AMER FND INV CO OF AM-A	AIVS	US4613081086	604.420	35.170000	21,257.46 11/15/2019
STATE OF NAME	AUZFXXXXXXXX		AMER FND INV CO OF AM-A	AIVS	US4613081086	175.964	35.170000	6,188.65 10/28/2019
STATE OF NAME	AUZFXXXXXXXX		AMER FND SMALLCAP WRLD-A	SMCW	US8316811012	484.828	51.190000	24,818.34 10/2/2019
STATE OF NAME	AUZFXXXXXXX	831681101	AMER FND SMALLCAP WRLD-A	SMCW	US8316811012	54.284	51.190000	2,778.80 10/16/2019

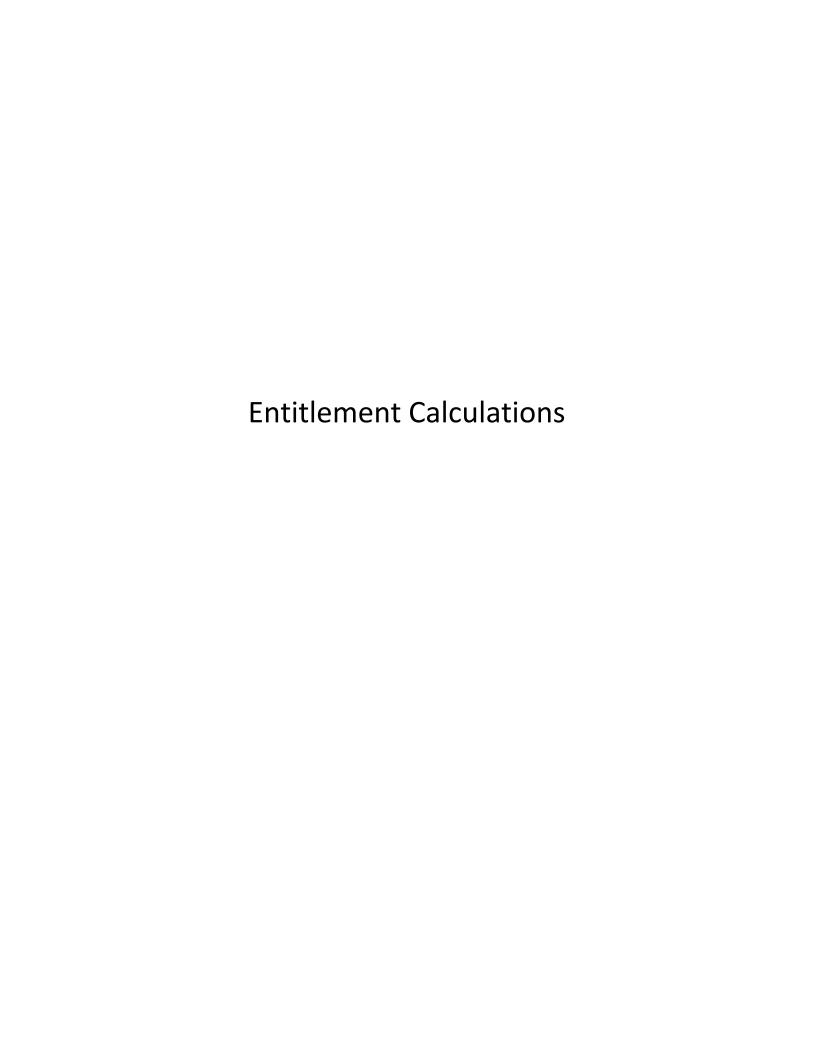


Worthless Report
.XLS Format

# Worthless Report

Account Numbe <b>r</b>	Account Name	Price Date	Location Name	CUSIP CINS	Security Short Description	Units Local Price Market Value Local		Market Value Reporting Currency	
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	384632AB1	GRAHAM-FIELD HEALTH PR 9.75 1 DFLT	50,000.0000	0.000000	0.00	0.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	383870102	GPS INDUST COM USD0.01	2,844.0000	0.000000	0.00	0.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	55970P203	MAGNUM D'O COM STK USD0.001	1,471.0000	0.000000	0.00	0.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	823213103	SHENGDATEC COM STK USD0.00001	20.0000	0.000000	0.00	0.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	314652108	FENWAY RES COM NPV	11,378.0000	0.000000	0.00	0.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	74728C307	QSOUND LAB COM NPV	50.0000	0.000000	0.00	0.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	78108N106	RTICA CORP COM NPV	2,991.0000	1.000000	2,991.00	2,991.00
XXXXX	AUZF STATE XXXXXXXX	6/30/2022	DEPOSITORY TRUST CPNY	G84385106	CHINA TECHNOLOGY GLOBAL CORP NPV	150.0000	0.000000	0.00	0.00
		·							

2,991.00



#### Claimant: First/Last Name CUSIP: 028837102

Original # of shares: 2.5470

Claim# 763855

4/22/1997



ISSUE NAME	TYPE	RECOI RATE DATE		SHARE BALANCE	CASH DIVIDEND	SHARE PRICE	SHARE DIVIDEND
Ending Balance				7.017	•		
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0 12/27/201	7 12/28/2017	7.017	\$ -	\$ -	0.000
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	1.15788 12/5/2017	12/6/2017	6.575	\$ 7.61	\$ 17.19	0.443
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	0.1389 12/28/201	6 12/31/2016	6.513	\$ 0.90	\$ 14.79	0.061
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Dividend	0.388 11/30/201	5 11/30/2015	6.343	\$ 2.46	\$ 14.43	0.171
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0 12/31/201	0 12/31/2010	6.343	\$ -	\$ -	0.000
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0 12/31/200	9 12/31/2009	6.343	\$ -	\$ -	0.000
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0 1/5/2009	1/5/2009	4.913	\$ -	\$ -	0.000
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	1.5716 12/30/200	1/5/2009	4.913	\$ 7.72	\$ 5.40	1.430
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	0.2976 12/26/200	7 1/2/2008	4.770	\$ 1.42	\$ 14.07	0.101
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Dividend	0.1252 12/26/200	7 1/2/2008	4.770	\$ 0.60	\$ 14.07	0.042
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Dividend	0.03995 12/28/200	12/28/2006	4.122	\$ 0.16	\$ 12.57	0.013
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	1.93606 12/28/200	12/28/2006	4.122	\$ 7.98	\$ 12.57	0.635
10/27/2004 Exchange cl	ass shares from C	CUISP 028837102 / cl	ass C to 028837870	/ class A rate	1:0.9962.		
				4.137	•		
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.543 12/28/200	12/31/2001	3.921	\$ 2.13	\$ 9.84	0.216
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.3 12/27/200		3.829		\$ 12.52	0.092
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.4 6/5/2000	6/6/2000	3.505		\$ 15.11	0.325
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.22 12/29/199		3.457		\$ 15.97	0.048
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.52 9/29/1999		3.093	1	\$ 12.91	0.364
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.046 12/17/199		2.864		\$ 13.08	0.229
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.22 12/29/199		2.816	,	\$ 12.97	0.048
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.35 11/13/199		2.547		\$ 12.77	0.269

#### There are No Dividend received from 2002 to 2005

Shares Liquidated 1/1/2018	
Under CUSIP 028837870	7.017
Liquidation Price:	\$18.00
Liquidation Proceeds Received:	\$126.31
Total Remittance Due:	\$144.31

Claimant:

Type:

Last/First Name

CUSIP: Original # of shares: 74441R508 120.0000 **759844** 



ISSUE NAME	TYPE	RATE	RECORD DATE	PAYMENT DATE	SHARE BALANCE	CASH DIVIDEND	SHARE PRICE	SHARE DIVIDEND
Ending Balance					123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02573	12/31/2010	12/31/2019	123.140	\$ 3.17		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			11/29/2019	123.140	1		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			10/31/2019	123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			09/30/2019	123.140	•		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend		- · · · · · · · · · · · · · · · · · · ·	08/30/2017	123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			06/31/2019	123.140	1		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			05/28/2019	123.140	•		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			05/31/2019	123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			04/30/2019	123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			03/29/2019	123.140	1		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			02/28/2019	123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			01/31/2019	123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend		12/31/2018		123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend		12/20/2018		123.140	1		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend		11/30/2018		123.140			
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			10/31/2018	123.140	•		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02281		9/28/2018	122.879	•	\$ 10.75	0.2607
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02281			122.879	1	1	0.2607
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02816	7/31/2018		122.360	•	\$ 10.79 \$ 10.76	0.3199
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02449			121.973		\$ 10.76	0.2841
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02552			121.473	1	\$ 10.76	0.2875
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02369	-, - ,		121.000		\$ 10.00	0.2669
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02592			121.419	•	\$ 10.76	0.2869
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02372				1		0.2511
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02253			120.878 120.603		\$ 10.85 \$ 10.91	0.2511
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			1/31/2018	120.603	•	\$ 10.91	0.2744
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			12/29/2017	120.329		\$ 10.98	0.2741
PRUDENTIAL SHORT-TERM CORPORAT	Dividend			11/30/2017	120.263		\$ 10.77	0.2630
I RODLINIIAL SHORT-TERM CORFORAL	Dividend	0.02411	11/30/2017	11/30/2017	120.000	φ 2.07	φ 11.00	0.2630

 Shares liquidated:
 123.140

 Dividends Paid in Cash:
 \$48.76

 Liq proceeds:
 \$1,321.29

 TOTAL:
 \$1,370.05

Claimant:

Last/First Name

CUSIP:

018918664

Original # of shares:

381.8883 11/18/2010

Type:

760495



ISSUE NAME	ТҮРЕ	RATE	RECORD Date	PAYMENT DATE	SHARE BALANCE	CASH DIVIDEND	SHARE PRICE	SHARE DIVIDEND
Ending Balance					312.231			

ALLIANZ FDS A- CUSIP 018918649

NO Dividend

312.231

Class effectived on 10/5/2018 CUSIP from 018918664 to 018918649, rate: 1 to 0.8175986

ALLIANZ FUDS C- CUSIP 018918664

381.8883

Shares liquidated under	312.231
CUSIP 018918649	
Liq proceeds:	\$8,945.42
Dividends Paid in Cash	\$0.00
TOTAL:	\$8,945.42

# Summary Entitlement Calculation Analysis



Claim#	Transaction Type	CUSIP	Security Name	Actual Settle Date	Units	P <b>r</b> ice	Liq Procee	<b>d</b> s L	₋iq Fee	Chec	k Amount
781317	Sell	05453N100	AWARE INC MASS USD 0.01	4/29/2019	-25.0000	\$ 3.10	\$ 77	.59	\$ (25.00)	\$	52.59
781316	Sell	030111207	AMERICAN SUPERCONDUCTOR CO USD 0.01	4/29/2019	-10.0000	\$11.32	\$ 113	.19	\$ (25.00)	\$	88.19
781899	Sell	654902204	NOKIA CORP CNY 1.0 ADR	4/30/2019	-50.0000	\$ 5.25	\$ 262	.49	\$ (25.00)	\$	237.49
781901	Sell	114340102	BROOKS AUTOMATION INC NEW USD 0.01	4/30/2019	-26.0000	\$31.34	\$ 814	.76	\$ (25.00)	\$	789.76
781902	Sell	872590104	T-MOBILE US INC USD 0.0001	4/16/2020	-10.0000	\$89.60	\$ 890	.98	\$ (25.00)	\$	865.98
781902	CIL	872590104	T-MOBILE US INC USD 0.0001	4/2/2019	-0.0509	\$82.60	\$ 4	.20	\$ -	\$	4.20
									TOTAL:	\$	<b>2</b> ,0 <b>3</b> 8. <b>21</b>

Please see below for Sprint's merger details:

04/02/2020 Stock merger: Holder received 0.10256 shares of Tmobile US INC cusip 872590104 per each share of Sprint Corp held.

Sprint shares requested to liquidate:	<b>9</b> 8.0000
Tmobile shares after merger (98*0.10256):	<b>1</b> 0.050 <b>9</b>
T <b>M</b> obile sha <b>r</b> es to be sol <b>d</b> :	10.0000
CIL for fractional shares (0.05088*\$82.60):	\$ 4. <b>2</b> 0

# SOC1 & SOC2 Reports

CONFIDENTIAL AND PROPRIETARY
NOT FOR PUBLIC DISCLOSURE



## Avenu Insights & Analytics

Unclaimed Property Clearinghouse Custody Operations System and Certain Aspects of the General Computer Control Environment

System and Organization Controls (SOC) for Service Organizations Report for the period of January 1, 2022 to September 30, 2022



An Independent Service Auditor Report issued by FORVIS, LLP

Avenu Insights & Analytics
SOC 1® Type 2 Report – SOC for Service Organizations: ICFR
Unclaimed Property Clearinghouse Custody Operations System and Certain Aspects of the General
Computer Control Environment

## **Table of Contents**

Section I: Report of Independent Service Auditors	1
Section II: Avenu Insights & Analytics' Assertion	4
Section III: Avenu Insights & Analytics' Description of its System and Controls	6
Section IV: Description of Avenu Insights & Analytics' Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results	18



## Section I: Report of Independent Service Auditors

To: Management of Avenu Insights & Analytics

#### Scope

We have examined Avenu Insights & Analytics' (the "Company") description of its Unclaimed Property Clearinghouse ("UPCH") Custody Operations System and Certain Aspects of the General Computer Control Environment (the "System") titled Avenu Insights & Analytics' Description of its System and Controls for processing user entities' transactions throughout the period January 1, 2022 to September 30, 2022 (the "description") and the suitability of the design and the operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in Avenu Insights & Analytics' Assertion (the "assertion"). The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Company uses the subservice organizations listed in the *Subservice Organizations* table in Section III of this report. The description in Section III of this report includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

## Service Organization's Responsibilities

In Section II of this report, the Company has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

#### Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 2022 to September 30, 2022.

# FORV/S

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, the suitability of the control objectives stated in the
  description, and the suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

#### **Inherent Limitations**

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

## **Description of Tests of Controls**

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV of this report.

#### **Opinion**

In our opinion, in all material respects, based on the criteria described in Avenu Insights & Analytics' assertion,

A The description fairly presents the System that was designed and implemented throughout the period, language

- A. The description fairly presents the System that was designed and implemented throughout the period January 1, 2022 to September 30, 2022.
- B. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2022 to September 30, 2022 and if the subservice organizations and user entities applied the complementary controls assumed in the design of Avenu Insights & Analytics' controls throughout the period January 1, 2022 to September 30, 2022.
- C. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2022 to September 30, 2022 if complementary subservice organization and user entity controls assumed in the design of Avenu Insights & Analytics' controls operated effectively throughout the period January 1, 2022 to September 30, 2022.

# FORV/S

#### **Restricted Use**

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the period January 1, 2022 to September 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

FORVIS, LLP

Tysons, VA

January 17, 2023



The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.



## Section II: Avenu Insights & Analytics' Assertion

We have prepared the description of Avenu Insights & Analytics' (the "Company") Unclaimed Property Clearinghouse ("UPCH") Custody Operations System and Certain Aspects of the General Computer Control Environment (the "System") entitled *Avenu Insights & Analytics' Description of its System and Controls* for processing user entities' transactions throughout the period January 1, 2022 to September 30, 2022 (the "description"), for user entities of the System during some or all of the period January 1, 2022 to September 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organizations and user entities of the System themselves, when assessing the risks of material misstatement of the user entities' financial statements.

The Company uses the subservice organizations listed in the *Subservice Organizations* table in Section III of this report. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if the complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

- A. The description fairly presents the System made available to user entities of the System during some or all of the period January 1, 2022 to September 30, 2022 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
  - 1. Presents how the System made available to user entities of the System was designed and implemented to process relevant user entity transactions, including, if applicable:
    - a. The types of services provided, including, as appropriate, the classes of transactions processed;
    - The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System;
    - c. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;
    - d. How the System captures and addresses significant events and conditions other than transactions:
    - e. The process used to prepare reports and other information for user entities;
    - f. Services performed by a subservice organization, if any, including whether the inclusive method or carve-out method has been used in relation to them;



- g. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls; and
- h. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- 2. Includes relevant details of changes to the service organization's system during the period covered by the description.
- 3. Does not omit or distort information relevant to the service organization's System, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.
- B. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 2022 to September 30, 2022 to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period. The criteria we used in making this assertion were that:
  - The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the Company;
  - 2. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
  - 3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

# Section III: Avenu Insights & Analytics' Description of its System and Controls

## A. Overview of Avenu Insights & Analytics

Headquartered in Centreville, Virginia, Avenu Insights & Analytics ("Avenu" or the "Company") has a long history of helping a variety of companies adapt to the changing needs for information management and their impact on service delivery. Avenu's software solutions for administration and revenue enhancement enable jurisdictions to provide a truly digital government that meets expectations of citizens, employees, and elected officials. The Company's focus and resources give customers more predictable revenue and costs and allow governments to sustain a high quality of life.

#### Services Provided

Avenu's Unclaimed Property & Treasury Custody Operations is a division of Avenu Insights & Analytics, LLC. Avenu Custody Group is a provider of unclaimed property collection and administration solutions, serving twenty-nine states, including the District of Columbia and Puerto Rico. Additionally, Avenu maintains and processes transactions for Insurance and Lottery programs for one state. Avenu is headquartered in Quincy, Massachusetts. Staffing consists of approximately 50 full-time employees and consultants.

Avenu provides securities custody services similar to those provided by banks or brokers on behalf of twentynine state clients including Puerto Rico and the District of Columbia. Avenu's Custody Group provides these services through a partnership with the Bank of New York Mellon (BNY Mellon), who acts as a sub-custodian since Avenu is neither a financial institution nor a direct member of the Depository Trust and Clearing Corporation (DTC). The scope of this report relates specifically to the state custody operations services that Avenu's Custody Group provides to its state clients.

Through BNY Mellon, Avenu holds securities and, as instructed by the states, values, sells, and reissues positions, including stock certificates or statements to claimants (also known as "owners"). Avenu provides the states with access to their positions and transactions through secure inquiry-only access in which they can also run monthly activity statements and view real time activities. Many positions are received in electronic format, although physical positions and statements continue to be received. For each state client, an account number/identifier is assigned through BNY Mellon's NEXEN® system.

Avenu maintains one BNY Mellon account for each state client, into which it receives positions through BNY Mellon's Global Security Processing (GSP) and NEXEN®. GSP is the internal operating system at BNY Mellon to which Avenu's users do not have access. NEXEN® is designed for BNY Mellon's outside clients and is the interface that Avenu's Custody Group uses to monitor and transact on behalf of its state clients. Avenu coordinates with BNY Mellon to execute the input of receipts, transfers, and liquidations requested by states and holders. These items remain in a pending status in NEXEN® until BNY Mellon settles each item as completed. The positions are then displayed as deposited or withdrawn from the state's account. BNY Mellon posts all DTC/physical/mutual fund activities, including corporate actions, into GSP.

## **B.** Scope of the Description

This description addresses only Avenu Insights & Analytics' Unclaimed Property Clearinghouse ("UPCH") Custody Operations System and Certain Aspects of the General Computer Control Environment (the "System") provided to user entities and excludes other services provided by Avenu Insights & Analytics. The description is intended to provide information for user entities of the System and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting, to be used in obtaining an understanding of the System and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of Avenu Insights & Analytics' UPCH Custody Operations System and Certain Aspects of the General Computer Control Environment.

## Information Systems Overview

Avenu utilizes the BNY Mellon NEXEN® system for both maintenance and the processing of free receipt, reregistration, liquidation, and transfer of securities. The NEXEN® system is BNY Mellon's online, real time accounting and management reporting application designed to automate a portion of a trust organization's accounting and reporting functions, provide a database of information for trust management and reporting, and allow outside clients to view account information.

Avenu uses this platform to maintain the assets for all state client unclaimed property programs. Additionally, the custody operation utilizes the extranet and liquidation portal to facilitate critical communication between Avenu and Its clients regarding instructions to liquidate or re-register shares. This portal feeds information regarding holdings directly from the NEXEN® platform to its clients. States also upload data with instructions through this method. For treasury accounts, including lottery and insurance processing, Avenu UPCH has an information services group that maintains the development and control of the internally-developed state treasury services system that resides on the AS400 and the internal network of Avenu UPCH. Records received related to account activity within NEXEN® are entered into the treasury system through the upload function.

#### C. Internal Control Framework

This section provides information about the five interrelated components of internal control at Avenu Insights & Analytics, including Avenu Insights & Analytics':

- Control environment,
- Risk assessment process,
- Monitoring activities,
- Information and communications, and
- Control activities.

#### 1. Control Environment

The control environment sets the tone of an organization and influences the control awareness of the organization. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to appropriate controls through management's actions supported by its policies, procedures, and organizational structure.

#### Commitment to Integrity and Ethical Values

Avenu has developed a formal ethics policy as part of the employee handbook which is available on its Intranet and contains rules about employee conduct. Employees are required to read and evidence their knowledge and receipt of Avenu's employee handbook upon hire and annually thereafter. Avenu offers its employees a number of channels through which potential breaches of ethical behavior may be reported.

## Oversight Responsibility of the Executive Management

The Company operates under the direction of its Chief Executive Officer ("CEO"), along with other senior executives ("Executive Team") that also serve as heads of the business units described within. The Executive Team holds itself accountable to the Company's ethics and conflict of interest policies and provides oversight of operations and activities. All areas are led by capable, experienced, and well-qualified individuals with years of experience applicable to their respective job responsibilities. Executives provide oversight of business units and are directly involved in the Company's operations.

#### Assignment of Authority and Responsibility

Executive management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures, under the ultimate oversight of the Executive Team. Management recognizes its responsibility for establishing and maintaining sound internal control and promoting integrity and ethical values to all personnel on a day-to-day basis.

#### Commitment to Competence

Avenu's values and commitment to competence begin with a commitment to engaging, developing, and supporting its people. This commitment starts with a clearly documented people selection process. Detailed job descriptions are created and maintained for each key position. Avenu's commitment to quality and competence is further evidenced by its approach to monitoring, evaluating, and supporting its people. The talent management process, along with staff training and development, helps ensure Avenu is providing its people with opportunities for professional growth.

#### Human Resource Policies and Practices

People are the key to Avenu's success, and the Human Resource ("HR") function is the organization driving programs to help ensure the Company engages, develops, and supports its people. The goal of the HR function is to build an organization of outstanding employees in an environment that encourages maximum engagement, development, and professional growth. Avenu is committed to respecting and supporting one another, regardless of physical differences, beliefs, or personal values. This commitment is expressed in Avenu's personnel policies and practices and begins with the recruiting process, which is the joint responsibility of the Operations' hiring managers and the Talent Acquisition Organization.

Avenu is an equal opportunity employer and is committed to providing a discrimination-free workplace. Employment decisions are based on each individual's skills and qualifications without regard to race, color, creed, religion, ancestry, national origin, age, gender/sex, marital status, sexual orientation, physical or mental disability, use of a guide dog or service animal, military/veteran status, citizenship status, genetic information, or any other category protected by law. This approach extends to every phase of the employment process including recruiting, hiring, training, promotion, compensation, benefits, transfers, and company-sponsored educational, social and recreational programs.

## 2. Risk Assessment Process

The service organization operates within an environment faced with a variety of risks from internal and external sources.

#### Risk Objectives

The risk assessment approach involves an iterative process for identifying and assessing risks to the achievement of objectives. This approach forms the basis for determining how risks will be addressed by management. Avenu recognizes that risk management is a critical component of internal controls affecting all levels of the organization. Management regularly assesses the risks of internal fraud and has taken measures to deter and prevent such actions from occurring. Management is also aware of the risks related to its Information Technology ("IT") infrastructure, such as security, network operations, and disaster recovery.

#### Identification and Analysis of Risks

Risk management is primarily the responsibility of individual business units which perform periodic risk assessments that identify and document significant risks facing Avenu, including any fraud risks. The results of these risk assessments determine how the business units develop and implement controls, operating procedures, and compliance processes for addressing and mitigating such risks. Avenu's policies require that any instances of suspected or actual fraud be brought to the immediate attention of senior management, the Chief Financial Officer, and Avenu's Legal department.

## 3. Monitoring Activities

Avenu employs a combination of ongoing and periodic monitoring activities to verify that controls are functioning effectively and that risks are appropriately mitigated.

#### **Ongoing Monitoring**

Avenu uses a variety of reports and monitoring mechanisms to help ensure controls are functioning as intended. Management regularly reviews and assesses business operations to verify that reporting and monitoring mechanisms used are effective in managing the operations of the business, controls, and related risks.

#### Monitoring of the Subservice Organizations

Avenu utilizes various subservice organizations to provide a) colocation Data Center services, b) custody and safekeeping of the securities it receives, and c) custodian services, including holding securities and maintaining accounts to support the System. Management monitors the services performed by the subservice organizations to help ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

#### 4. Information and Communication

Policies, procedures, and other information necessary to help achieve Avenu's business objectives are communicated through several means, including the Intranet, emails, newsletters, memoranda, meetings, and training sessions. Policies and procedures enforce the importance of adherence to and compliance with rules and regulations that govern business and operations. Policies and procedures are documented and are made available to employees on the Company Intranet.

Avenu has implemented various methods of communication to help ensure all employees understand their individual roles and responsibilities over transaction processing and controls and to help ensure significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees and the use of electronic mail messages to communicate timesensitive messages and information. Managers also hold periodic staff meetings as appropriate.

Avenu has also implemented various methods of communication to help ensure user entities understand the role and responsibilities they have in processing their transactions and to help ensure significant events are communicated to users in a timely manner. These methods include active participation in user meetings, as well as the designation of a client success manager ("CSM") who maintains contact with designated user representatives to inform them of new issues and developments. User organizations also are encouraged to communicate questions and problems to their liaison, and such matters are logged and tracked until resolved, with the resolution also reported to the user entity.

#### **D.** Control Activities

A variety of policies and procedures, including related control activities, have been developed to help ensure objectives are carried out and risks are mitigated. These control activities help ensure claims processing is administered in accordance with policies and procedures.

Control activities are performed at a variety of levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorizations, reconciliation, and IT controls. Duties and responsibilities, such as those related to the processing and recording of transactions, reconciliation activities, application development, compliance, and control monitoring, are allocated among personnel to help ensure that a proper segregation of duties is maintained.

A formal program is in place to periodically review and update policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and are communicated to associates.

#### 1. Physical Security

Control Objective 1: Controls provide reasonable assurance physical access to resources within Avenu Insights & Analytics facilities is restricted to appropriate personnel based on job function.

All external access points to the Avenu Insights & Analytics facilities are controlled through electronic card key readers. Card key access is limited to appropriate individuals based on job function. Visitors to the Avenu Insights & Analytics facilities are required to sign in at the front desk. The ability to implement changes to physical access rights at the Avenu Insights & Analytics facilities is limited to appropriate personnel based on job function to prevent unauthorized changes.

Physical access the Avenu Insights & Analytics facilities must be approved by management prior to the granting of access. Terminated employee access to the Avenu Insights & Analytics facilities is revoked within five business days of termination. Physical access to the Avenu Insights & Analytics facilities is reviewed on an annual basis by management to validate that employee access is commensurate with job responsibilities. Any issues identified are researched and resolved.

#### 2. Change Management - Network Infrastructure and Operating System

Control Objective 2: Controls provide reasonable assurance that network infrastructure and operating system changes are tested (if applicable) and approved prior to migration into the production environment.

Each change to network infrastructure and the operating system is applied and tested (if applicable) within development and/or testing environments which are separate from the production environment prior to migration into the production environment. Each change to network infrastructure and the operating system must be approved by a member of management prior to migration into the production environment. Access to promote changes into the production environment related to network infrastructure and the operating system is limited to appropriate personnel based on job function.

### 3. Change Management - Application and Database

Control Objective 3: Controls provide reasonable assurance that changes to the in-scope application (Escheatment System) and its related databases are tested (if applicable) and approved prior to migration into the production environment.

Each change to the in-scope application and its related databases is applied and tested (if applicable) within development and/or testing environments which are separate from the production environment prior to migration into the production environment. Each change to the in-scope application and its related databases must be approved by a member of management prior to migration into the production environment.

Access to promote changes into the production environment related to the in-scope application and its related databases is limited to appropriate individuals without development responsibilities. Version control software is in place to manage current versions of source code related to the in-scope application and its related databases.

## 4. Logical Security - Network Infrastructure and Operating System

Control Objective 4: Controls provide reasonable assurance that Administrative access to network infrastructure and operating system resources is restricted to appropriate personnel based on job function.

Valid user IDs and passwords are required to access the Company's network infrastructure and operating system resources. Password parameters to network infrastructure and operating system resources are configured to require:

- Expiration,
- Minimum length.
- History,
- Complexity, and
- Lockout after unsuccessful login attempts.

Administrative access to network infrastructure and operating system resources is restricted to appropriate personnel based on job function. Administrative access to network infrastructure and operating system resources is removed or disabled within five business days of the employee's termination date.

Requests to add Administrative access to network infrastructure and operating system resources are approved by the Senior Engineer of Servers, Storage, and Virtualization prior to access being granted.

## 5. Logical Security - Application and Database

Control Objective 5: Controls provide reasonable assurance that access, including Administrative and general user access, to the in-scope application (Escheatment System) and its related databases is restricted to appropriate personnel based on job function.

Valid user IDs and passwords are required to access the in-scope application and its related databases. Password parameters to the in-scope application and related databases are configured to require:

- Expiration,
- · Minimum length,
- History,
- · Complexity, and
- Lockout after unsuccessful login attempts.

Administrative access to the in-scope application and its related databases is restricted to appropriate personnel based on job function.

Requests to add access to the in-scope application and its related databases are approved by management prior to access being granted. Access to the in-scope application and its related databases is removed or disabled within five business days of the employee's/contractor's termination date. The Company performs an annual review of access to the in-scope application and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.

### 6. Receipt of Property

Control Objective 6: Controls provide reasonable assurance that physical property (cash/securities certificates) is received and properly credited to state accounts.

Each business day, package logs are used to record physically received checks and certificates and to monitor the transfer of the property to the custody unit. Physical checks received are logged within the check log sheet by the Operations Clerk, and the logging is verified by an Account Administrator. The check amounts are posted to the state's account via NEXEN®, which is reviewed by an Account Administrator.

Certificate transmittal logs are used to record physically received property (cash/securities) that is sent to BNY Mellon, and a confirmation of receipt is received from BNY Mellon to help ensure that property is properly credited to state accounts. An Account Administrator completes and signs off on each transmittal sheet indicating the control totals within the records received from the property holder(s) are balanced against the converted records within the system, including free receive transactions (certificates), to help ensure that property is properly credited to state accounts.

## 7. Delivering Transferring Securities

Control Objective 7: Controls provide reasonable assurance that Night Withdrawal Transfers (NWTs) are properly received and posted in accordance with state instructions.

Authorized state signatures are confirmed by an Account Administrator for each NWT request received via Avenu extranet or mail, and the unit manager of custody or an appropriate designee approves each NWT for trade entry. Each NWT is reviewed by an Account Administrator to confirm posting in accordance with state instructions. Any identified discrepancies are researched and resolved.

#### 8. Entitlement Calculations and Payments

Control Objective 8: Controls provide reasonable assurance that entitlement calculations and claim payments are prepared and processed in accordance with state instructions.

For participating states, remittance summary spreadsheets, including entitlement calculations and claim payments, are prepared by an Account Administrator and are reviewed by the unit manager of custody or an appropriate designee for accuracy. Any identified discrepancies are researched and resolved. For participating states, if cash is due to the owner and the state has elected Avenu to pay the owner (claimant), a check for the amount due is approved by the unit manager of custody or an appropriate designee and is forwarded to the owner upon settlement, in accordance with state instructions.

## 9. Liquidating Securities

Control Objective 9: Controls provide reasonable assurance that securities are liquidated with proper authorization by a state designee in accordance with state instructions.

Authorized state signatures are confirmed by management for each liquidation request received via Avenu extranet or eFax, and each request is approved by the unit manager of custody or an appropriate designee for trade entry. Each liquidation request is reviewed by an Account Administrator to confirm posting in accordance with state instructions. Any identified discrepancies are researched and resolved.

#### 10. Voluntary Corporate Action Notifications

Control Objective 10: Controls provide reasonable assurance that voluntary corporate actions affecting the securities held by the states are properly and timely communicated to the state and that the results of the actions are properly recorded.

Voluntary corporate action notifications received via NEXEN® are entered on the Avenu extranet (if applicable) by the operations clerk to help ensure that states that hold property can view and submit responses. A reminder e-mail is sent by the Operations Clerk prior to or on the response due date to the state(s) that have not responded to voluntary corporate actions. Voluntary corporate action responses from the states are recorded within NEXEN® by the Operations Clerk. If the state does not provide a response by the due date, the default action is selected automatically by the NEXEN® system.

## 11. Treasury Insurance and Lottery Safeguards

Control Objective 11: Controls provide reasonable assurance that all transaction history related to securities held by the states for Treasury Insurance and Lottery programs are processed and uploaded for each business day to the AS400 System.

On each business day, the custodial account activity report is automatically generated from the NEXEN® system and is uploaded into the AS400 system. On each business day, management reviews status reports generated by the AS400 system to help ensure that the custodial account activity report is completely processed. Any identified issues are researched and resolved. On a monthly basis, state lottery holdings reports are generated from the AS400 system and are e-mailed to states by members of the custody department to help facilitate state reconciliation procedures.

## E. Additional Information about Management's Description

The Company has specified the control objectives and identified the controls which are designed to achieve the related control objectives. The specified control objectives and related controls are presented within Section IV of this report, Description of Avenu Insights & Analytics' Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results, and are an integral component of the Company's description of its system as described within this section.

## F. Changes to the System During the Specified Period

Management did not make any significant or relevant changes to the system during the period January 1, 2022 to September 30, 2022 (the "specified period").

## G. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve specific control objectives, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Control Objectives
Cyxtera Technologies, Inc. ("Cyxtera")	The Company uses Cyxtera for its third-party hosting and colocation of servers and equipment, including the restriction of physical access to the defined system as well as custody and safekeeping of the securities. The following control areas are critical to achieving the applicable control objectives:	Control Objective 1*
	<ul> <li>Controls around the physical security of the Data Centers hosting the in-scope applications, and</li> <li>Controls around the environmental protections at the Data Centers hosting the in-scope applications.</li> </ul>	

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Control Objectives		
	<ul> <li>In addition, the Company has identified the following controls to help monitor the subservice organization:</li> <li>On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.</li> </ul>			
The Bank of New York Mellon Corporation ("BNY Mellon")	<ul> <li>The Company uses BNY Mellon to provide custodian services, including holding securities and maintaining accounts. The following control areas are critical to achieving the applicable control objectives:</li> <li>Controls around the design and operation of holding securities in support of user entities, and</li> <li>Controls around the design and operation of account maintenance in support of user entities.</li> <li>In addition, the Company has identified the following controls to help monitor the subservice organization:</li> <li>On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SQC 2 reports, or the third party is subjected to continuous monitoring controls.</li> </ul>	Control Objective 6* Control Objective 7* Control Objective 11		

Subservice Organization	Service(s) Provided and Monitoring Controls					
Raymond James Financial, Inc. ("RJA")	The Company uses RJA to provide brokerage services for Company accounts that support the in-scope system. The following control areas are critical to achieving the applicable control objectives:	Control Objective 9*				
	<ul> <li>Controls around the design and operation of processing liquidations and accurately applying commission and SEC charges to processed transactions, and</li> <li>Controls around the design and operation of accurately performing the research and portfolio valuations in compliance with internal controls.</li> </ul>					
	In addition, the Company has identified the following controls to help monitor the subservice organization:					
	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.					

<sup>\*</sup> The achievement of design and operating effectiveness for this particular control objective assumes that complementary controls at this subservice organization are in place and are operating effectively to support and achieve this control objective.

## **H. User Entity Controls**

Avenu Insights & Analytics' controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company's system. It is not feasible for the control objectives to be solely achieved by the Company. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated control objective(s) are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

User Entity Controls	Related Control Objectives
Each user entity is responsible for approving access, removing access timely when necessary, and defining appropriate duties for personnel for NEXEN®.	Control Objective 5*
Each user entity is responsible for performing a periodic review of users' access to NEXEN®.	Control Objective 5*
Each user entity is responsible for monitoring user activity on NEXEN®.	Control Objective 5*
Each user entity is responsible for assigning user IDs to the proper personnel and for maintaining confidential passwords for NEXEN®.	Control Objective 5*
Each user entity is responsible for notifying Avenu of changes to access rights within NEXEN®.	Control Objective 5*
Each user entity is responsible for providing lists of authorized signatories to Avenu's Unclaimed Property Solutions and for periodically reviewing the authorized list for appropriateness.	Control Objective 5*
Each user entity is responsible for providing complete and accurate listings of securities to be delivered to state accounts.	Control Objectives 6*, 7*, and 8*
Each user entity is responsible for authorizing Night Withdrawal Transfers (NWTs), liquidation, and cash withdrawal requests.	Control Objectives 7* and 9*
Each user entity is responsible for responding to voluntary corporate actions by due dates if it wishes to take an action other than the default action.	Control Objective 10*

<sup>\*</sup> The achievement of design and operating effectiveness for this particular control objective assumes that this complementary user entity control is in place and is operating effectively to support and achieve this control objective.

# Section IV: Description of Avenu Insights & Analytics' Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results

## A. Information Provided by FORVIS, LLP

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at Avenu Insights & Analytics.

Our examination was limited to the control objectives and related controls specified by Avenu Insights & Analytics in Sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess the internal control environment. If the internal controls are not effective at a user entity, Avenu Insights & Analytics' controls may not compensate for such weaknesses.

Avenu Insights & Analytics' system of internal control represents the collective effect of various factors on establishing and enhancing the effectiveness of the controls specified by Avenu Insights & Analytics. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by Avenu Insights & Analytics, we considered aspects of Avenu Insights & Analytics' control environment, risk assessment process, monitoring activities, and information and communications.

## B. Types and Description of the Tests of Operating Effectiveness

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type Description	
Inquiry Inquired of appropriate personnel and corroborated with management	
Observation Observation of the application, performance, or existence of the control	
Inspection Inspection of documents, records, or other evidence indicating performance control	
Reperformance Reperformed the control, or processing of the application control, for actits operation	

In addition, as required by paragraph .36 of AT-C section 205, Assertion-Based Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

# C. Control Objectives, Control Activities, Tests Performed, and Results of Testing

Cambra	I Ohiostina	4
Contre	ol Objective	ш

Physical Security (Facilities): Controls provide reasonable assurance physical access to resources within Avenu Insights & Analytics facilities is restricted to appropriate personnel based on job function.

Cont	rol Activity Description	Tests Performed by Service Auditor	Results of Testing
1.01	All external access points to the Avenu Insights & Analytics facilities are controlled through electronic card key readers. Card key access is limited to appropriate individuals based on job function.	Observed all external access points to the Avenu Insights & Analytics facilities to determine that all external access points to the Avenu Insights & Analytics facilities were controlled through an electronic badge access system. Further, inquired of the Director, Unclaimed Property Solutions to determine that this process was in place throughout the specified period.	No exception noted.
		Inspected the listing of individuals with access to the Avenu Insights & Analytics facilities and the corresponding job titles for a sample of those users to determine that each selected user was appropriate to have this access based on job function. Further, inquired of the Director, Unclaimed Property Solutions to determine that each selected user was appropriate to have this access.	No exception noted.
1.02	Physical access the Avenu Insights & Analytics facilities must be approved by management prior to the granting of access.	Inspected the physical access requests related to a sample of new employees granted physical access to the Quincy Office Service Room to determine that each selected physical access request the Avenu Insights & Analytics facilities was approved by management prior to the granting of access.	No exceptions noted
1.03	Terminated employee access to the Avenu Insights & Analytics facilities is revoked within five business days of termination.	Inspected the access removal tickets and supporting documentation related to a sample of terminated employees to determine that each selected employee's access to the Avenu Insights & Analytics facilities was revoked within five business days of termination.	No exceptions noted.

Physical Security (Facilities): Controls provide reasonable assurance physical access to resources within Avenu Insights & Analytics facilities is restricted to appropriate personnel based on job function.

Cont	rol Activity Description	Tests Performed by Service Auditor	Results of Testing
1.04	Physical access to the Avenu Insights & Analytics facilities is reviewed on an annual basis by management to validate that employee access is commensurate with job responsibilities. Any issues identified are researched and resolved.	Inspected the physical access review documentation to determine that physical access to the Avenu Insights & Analytics facilities was reviewed by management during the specified period to validate that employee access was commensurate with job responsibilities. Further, inspected supporting documentation and inquired of the Senior Director, Client Partner to determine that no issues were identified as a result of the selected review; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
1.05	The ability to implement changes to physical access rights at the Avenu Insights & Analytics facilities is limited to appropriate personnel based on job function to prevent unauthorized changes.	Inspected the listing of users with the ability to implement changes to physical access rights the Avenu Insights & Analytics facilities and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function to help prevent unauthorized changes. Further, inquired of the Director Unclaimed Property to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
1.06	Visitors to the Avenu Insights & Analytics facilities are required to sign in at the front desk.	Observed the visitor process for the Avenu Insights & Analytics facilities to determine that visitors were required to sign in at the front desk. Further inquired of the Director, Unclaimed Property Solutions to determine that this process was in place throughout the specified period.	No exception noted.
		Inspected the Visitor Log to determine that visitor/temporary access to sensitive areas and locations was logged.	No exception noted.

Change Management – Network Infrastructure and Operating System: Controls provide reasonable assurance that network infrastructure and operating system changes are tested (if applicable) and approved prior to migration into the production environment.

Cont	rol Activity Description	Tests Performed by Service Auditor	Results of Testing
2.01	Each change to network infrastructure and the operating system is applied and tested (if applicable) within development and/or testing environments which are separate from the production environment prior to migration into the production environment.	testing environments related to the network infrastructure and the operating system to determine that each change to the network infrastructure and the operating system was applied and tested (if applicable) within a development and/or testing environment separate from the production environment. Further, inquired of the Project Management Manager II to determine that these environments were separate throughout the specified period.	No exceptions noted.
		Inspected the change requests and supporting documentation related to a sample of changes to the network infrastructure and the operating system to determine that each selected change was applied and tested (if applicable) within a development and/or testing environment separate from the production environment prior to migration into the production environment.	No exceptions noted.
2.02	Each change to network infrastructure and the operating system must be approved by a member of management prior to migration into the production environment.	Inspected the change tickets and supporting documentation related to a sample of changes to the network infrastructure and the operating system to determine that each selected change was approved by a member of management prior to migration into the production environment.	No exceptions noted.
2.03	Access to promote changes into the production environment related to network infrastructure and the operating system is limited to appropriate personnel based on job function.	Inspected the listings of users with Administrative access to the production environment related to network infrastructure and the operating system and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Senior Engineer Servers, Storage, Virtualization to determine that each user on the listings was appropriate to have this access.	No exceptions noted.

Change Management – Application and Database: Controls provide reasonable assurance that changes to the in-scope application (Escheatment System) and its related databases are tested (if applicable) and approved prior to migration into the production environment.

Cont	rol Activity Description	Tests Performed by Service Auditor	Results of Testing
3.01	Each change to the in-scope application and its related databases is applied and tested (if applicable) within development and/or testing environments which are separate from the production environment prior to migration into the production environment.	Observed the production, development, and testing environments to determine that each change to the in-scope application and related databases was applied and tested within a development and/or testing environment separate from the production environment. Further, inquired of the Software Engineer II to determine that these environments were separate throughout the specified period.	No exception noted.
		Inspected the change requests and supporting documentation related to a sample of changes to the in-scope application and related databases to determine that each selected change was applied and tested within a development and/or testing environment separate from the production environment prior to migration into the production environment.	No exception noted.
3.02	Each change to the in-scope application and its related databases must be approved by a member of management prior to migration into the production environment.	Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope application and related databases to determine that each selected change was approved by a member of management prior to promotion into the production environment.	No exceptions noted.
3.03	Access to promote changes into the production environment related to the inscope application and its related databases is limited to appropriate individuals based on job function.	Inspected the listing of users with access to promote changes into the production environment related to the in-scope application and its related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Project Management Manager II to determine that each user on the listing was appropriate to have this access.	No exceptions noted.

Change Management – Application and Database: Controls provide reasonable assurance that changes to the in-scope application (Escheatment System) and its related databases are tested (if applicable) and approved prior to migration into the production environment.

Contr	ol Activity Description	Tests Performed by Service Auditor  Observed the version control software and related code repositories to determine that version control software was in place to manage the current versions of source code related to the in-scope application and related databases. Further, inquired of the Software Engineer II to determine that the version control software was in place throughout the specified period.  Inspected the change management review documentation to determine that all changes to the production environment related to the in-scope applications and related databases were reviewed during the specified period to	Results of Testing	
3.04	Version control software is in place to manage current versions of source code related to the in-scope application and its related databases.		No exception noted.	
3.05	On an annual basis, all changes to the production environment related to the inscope applications and related databases are reviewed to verify that each change was authorized.	documentation to determine that all changes to the production environment related to the in-scope applications and related databases	No exceptions noted.	

Logical Security – Network Infrastructure and Operating System: Controls provide reasonable assurance that Administrative access to network infrastructure and operating system resources is restricted to appropriate personnel based on job function.

Conti	rol Activity Description	Tests Performed by Service Auditor	Results of Testing
4.01	Valid user IDs and passwords are required to access the Company's network infrastructure and operating system resources.	Observed the authentication configurations for the network infrastructure and operating system resources to determine that a valid user ID and password were required to access the Company's network infrastructure and operating system resources. Further, inquired of the Director, Unclaimed Property Solutions, to determine that these configurations were in place throughout the specified period.	No exceptions noted.
4.02	Administrative access to network infrastructure and operating system resources is restricted to appropriate personnel based on job function.	Inspected the listings of users with Administrative access to network infrastructure and operating system resources and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Senior Engineer of Server, Storage, and Virtualization to determine that each user on the listings was appropriate to have this access.	No exceptions noted.
4.03	Requests to add Administrative access to network infrastructure and operating system resources are approved by the Senior Engineer of Servers, Storage, and Virtualization prior to access being granted.	Inspected the request tickets and supporting documentation related to a sample of new users granted Administrative access to network infrastructure and/or operating system resources to determine that each selected new user's access was approved by the Senior Engineer of Servers, Storage, and Virtualization prior to access being granted.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no users granted Administrative access to the network infrastructure or operating system resources. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.

Logical Security – Network Infrastructure and Operating System: Controls provide reasonable assurance that Administrative access to network infrastructure and operating system resources is restricted to appropriate personnel based on job function.

Cont	rol Activity Description	Tests Performed by Service Auditor	Results of Testing  No exceptions noted.
		Inspected the query used to pull the system-generated listing of users granted Administrative access to the network infrastructure and operating system resources during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system- generated listing to determine that there were no users granted Administrative access to the network infrastructure or operating system resources during the specified period. Further, inquired of the Senior Engineer Servers, Storage, Virtualization to determine that there were no users granted Administrative access to the network infrastructure or operating system resources during the specified period.  Inspected the termination tickets and supporting documentation related to a sample of terminated employees to determine that each selected terminated employee's Administrative access to network infrastructure and/or operating system resources was removed or disabled within five business days of the employee's termination date.	
4.04	Administrative access to network infrastructure and operating system resources is removed or disabled within five business days of the employee's termination date.	supporting documentation related to a sample of terminated employees to determine that each selected terminated employee's Administrative access to network infrastructure and/or operating system resources was removed or disabled within five business days of the employee's	No exceptions noted.
4.05	Password parameters to network infrastructure and operating system resources are configured to require: • Expiration, • Minimum length, • History, • Complexity, and • Lockout after unsuccessful login attempts.		No exceptions noted.

Logical Security – Application and Database: Controls provide reasonable assurance that access, including Administrative and general user access, to the in-scope application (Escheatment System) and its related databases is restricted to appropriate personnel based on job function.

Conti	rol Activity Description	Tests Performed by Service Auditor	Results of Testing
5.01	Valid user IDs and passwords are required to access the in-scope application and its related databases.	Observed the authentication configurations for the in-scope application and its related databases to determine that a valid user ID and password were required to access the Company's the in-scope application and its related databases. Further, inquired of the Director, Unclaimed Property Solutions to determine that these configurations were in place throughout the specified period.	No exceptions noted.
5.02	Administrative access to the in-scope application and its related databases is restricted to appropriate personnel based on job function.	Inspected the listing of users with Administrative access to the in-scope application and its related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Director, Unclaimed Property Solutions, to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
5.03	Requests to add access to the in-scope application and its related databases are approved by management prior to access being granted.	Inspected the request tickets and supporting documentation related to a sample of new users granted access to the in-scope application and/or its related databases to determine that each selected new user's access was approved by management prior to access being granted.	No exceptions noted.
5.04	Access to the in-scope application and its related databases is removed or disabled within five business days of the employee's/contractor's termination date.	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the inscope application and/or its related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.

Logical Security – Application and Database: Controls provide reasonable assurance that access, including Administrative and general user access, to the in-scope application (Escheatment System) and its related databases is restricted to appropriate personnel based on job function.

Control Activity Description		Tests Performed by Service Auditor	Results of Testing
5.05	Password parameters to the in-scope application and related databases are configured to require:  • Expiration,  • Minimum length,  • History,  • Complexity, and  • Lockout after unsuccessful login attempts.	Observed the password configurations that governed user access to the in-scope application and related databases to determine that password parameters for the in-scope application and related databases were configured to require:  • Expiration,  • Minimum length,  • History,  • Complexity, and  • Lockout after unsuccessful login attempts. Further, inquired of the Engineer II, Software Engineering to determine that these configurations were in place throughout the specified period.	No exception noted.
5.06	The Company performs an annual review of access to the in-scope application and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.	Inspected the access review documentation to determine that the Company performed a review of access to the in-scope application and its related databases during the specified period to help ensure that user access was appropriate. Further, inspected supporting review documentation and inquired of the Director, Unclaimed Property Solutions, to determine that no issues were identified as a result of the selected review, however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

Logical Security – Application and Database: Controls provide reasonable assurance that access, including Administrative and general user access, to the in-scope application (Escheatment System) and its related databases is restricted to appropriate personnel based on job function.

Control Activity Description		Tests Performed by Service Auditor	Results of Testing
manage third part to confid that perfiservice reperation determine based or access, related do to operative ratine either pessecurity third part party's Sorganiza such as the third	ment evaluates the ties that have access lential data and/or form a managed related to the n of the System and les their risk-rating in their level of the sensitivity of the lata, and the impact tions. Based on this g, management erforms a vendor assessment of the ty, reviews the third ystem and lation Control reports SOC 2 reports, or party is subjected to us monitoring	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the Director of Operations to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted

Control Objective 6				
Receipt of Property: Controls provide reasonable assurance that physical property (cash/securities certificates) is received and properly credited to state accounts.				
Contr	rol Activity Description	Tests Performed by Service Auditor	Results of Testing	
6.01	Each business day, package logs are used to record physically received checks and certificates and to monitor the transfer of the property to the custody unit.	Inspected the package logs related to a sample of business days to determine that package logs were used to record physically received checks and certificates and to monitor the transfer of the property to the custody unit for each selected business day.	No exceptions noted	
6.02 Physical checks received are logged within the check log sheet by the Operations Clerk, and the logging is verified by an Account Administrator. The check	Inspected the check log sheet related to a sample of checks to determine that each selected physical check was logged within the check log sheet by the Operations Clerk, and the logging was verified by an Account Administrator.	No exceptions noted		
	amounts are posted to the state's account via NEXEN®, which is reviewed by an Account Administrator.	Inspected the NEXEN account administrator review and account history related to a sample of checks to determine that check amount for each selected check was posted to the state's account via NEXEN® and was reviewed by an Account Administrator.	No exceptions noted	
6.03 Certificate transmittal logs are used to record physically received property (cash/securities) that is sent to BNY Mellon, and a confirmation of receipt is	Inspected the certificate transmittal logs related to a sample of physically received property (cash/securities) to determine that a certificate transmittal log was used to record each selected physically received property (cash/securities) that was sent to BNY Mellon.	No exceptions noted		
	received from BNY Mellon to help ensure that property is properly credited to state accounts.	Inspected the confirmation of receipts related to a sample of physically received property (cash/securities) to determine that a confirmation of receipt was received from BNY Mellon to help ensure that each selected physically received property was properly credited to state accounts.	No exceptions noted	

# **Control Objective 6**

Receipt of Property: Controls provide reasonable assurance that physical property (cash/securities certificates) is received and properly credited to state accounts.

Contr	ol Activity Description	Tests Performed by Service Auditor	Results of Testing
6.04	An Account Administrator completes and signs off on each transmittal sheet indicating the control totals within the records received from the property holder(s) are balanced against the converted records within the system, including free receive transactions (certificates), to help ensure that property is properly credited to state accounts.	Inspected the transmittal sheets related to a sample of physical property (cash/securities) received to determine that an Account Administrator completed and signed off on the transmittal sheet indicating the control totals within the records received from the property holder(s) were balanced against the converted records within the system, including free receive transactions (certificates), to help ensure that property was properly credited to state accounts for each selected physical property (cash/securities) received.	No exceptions noted

Contr	Control Objective 7			
Delivering Transferring Securities: Controls provide reasonable assurance that Night Withdrawal Transfers (NWTs) are properly received and posted in accordance with state instructions.				
Contr	rol Activity Description	Tests Performed by Service Auditor	Results of Testing	
7.01	Authorized state signatures are confirmed by an Account Administrator for each NWT request received via Avenu extranet or mail, and the unit manager of custody or an appropriate designee approves each NWT for trade entry.	Inspected the NWT confirmation and approval documentation related to a sample of NWT requests to determine that authorized state signatures were confirmed by an Account Administrator for each selected NWT request received via Avenu extranet or mail, and that the unit manager of custody or an appropriate designee approved each selected NWT for trade entry.	No exceptions noted.	
7.02	Each NWT is reviewed by an Account Administrator to confirm posting in accordance with state instructions. Any identified discrepancies are researched and resolved.	Inspected the NWT request documentation related to a sample of NWTs to determine that each selected NWT was reviewed by an Account Administrator to confirm posting in accordance with state instructions. Further, inspected supporting documentation and inquired of the Director of Unclaimed Property to determine that no discrepancies were identified as a result of the selected reviews; however, that if any discrepancies had been identified, each discrepancy would have been researched and resolved and this process was in place throughout the specified period.	No exceptions noted.	

#### **Control Objective 8** Entitlement Calculations and Payments: Controls provide reasonable assurance that entitlement calculations and claim payments are prepared and processed in accordance with state instructions. **Control Activity Description Tests Performed by Service Auditor** Results of Testing 8.01 For participating states. Inspected the remittance summary No exceptions noted. remittance summary spreadsheets related to a sample of spreadsheets, including entitlement calculations and claim payments entitlement calculations and to determine that, for participating states, a claim payments, are remittance summary spreadsheet, including prepared by an Account entitlement calculations and/or claim Administrator and are payments, was prepared by an Account reviewed by the unit manager Administrator and was reviewed by the unit of custody or an appropriate manager of custody or an appropriate designee for accuracy. Any designee for accuracy for each selected identified discrepancies are entitlement calculation and/or claim payment. researched and resolved. Further, inspected supporting documentation and inquired of the Director of Unclaimed Property to determine that no discrepancies were identified as a result of the selected reviews; however, if discrepancies were identified, each discrepancy would have been researched and resolved and this process was in place throughout the specified period. 8.02 For participating states, if Inspected the state instructions, check No exceptions noted. cash is due to the owner and approval, and transmission documentation the state has elected Avenu related to a sample of check claim payments to pay the owner (claimant), a for participating states to determine that for check for the amount due is each selected check claim payment for approved by the unit participating states, if cash was due to the manager of custody or an owner and the state had elected Avenu to pay appropriate designee and is the owner (claimant), a check for the amount forwarded to the owner upon due was approved by the unit manager of settlement, in accordance custody or an appropriate designee and was with state instructions. forwarded to the owner upon settlement, in

accordance with state instructions.

#### **Control Objective 9** Liquidating Securities: Controls provide reasonable assurance that securities are liquidated with proper authorization by a state designee in accordance with state instructions. **Control Activity Description Tests Performed by Service Auditor Results of Testing** 9.01 Authorized state signatures Inspected the confirmation and approval No exceptions noted. are confirmed by documentation related to a sample of management for each liquidation requests received via Avenu liquidation request received extranet or eFax to determine that authorized via Avenu extranet or eFax, state signatures were confirmed by and each request is approved management for each selected liquidation by the unit manager of request and that each selected request was custody or an appropriate approved by the unit manager of custody or designee for trade entry. an appropriate designee for trade entry. 9.02 Each liquidation request is Inspected the liquidation request No exceptions noted. reviewed by an Account documentation related to a sample of Administrator to confirm liquidation requests to determine that each posting in accordance with selected liquidation request was reviewed by state instructions. Anv an Account Administrator to confirm posting in identified discrepancies are accordance with state instructions. Further, researched and resolved. inspected supporting documentation and inquired of the Director of Unclaimed Property to determine that no discrepancies were identified as a result of the selected reviews: however, that if any discrepancies had been identified, each discrepancy would have been researched and resolved and this process

was in place throughout the specified period.

# **Control Objective 10**

Voluntary Corporate Action Notifications: Controls provide reasonable assurance that voluntary corporate actions affecting the securities held by the states are properly and timely communicated to the state and that the results of the actions are properly recorded.

Control Activity Description Tests Performed by Service Auditor		Tests Performed by Service Auditor	Results of Testing
10.01	Voluntary corporate action notifications received via NEXEN® are entered on the Avenu extranet (if applicable) by the operations clerk to help ensure that states that hold property can view and submit responses. A reminder e-mail is sent by the Operations Clerk prior to or on the response due date to the state(s) that have not responded to voluntary corporate actions.	Inspected Avenu extranet history related to a sample of voluntary corporate actions received via NEXEN® to determine that each selected voluntary corporate action was entered on the Avenu extranet by the operations clerk to help ensure that states that hold property can view and submit responses. Further, inspected the reminder email, if applicable, related to the sample of voluntary corporate actions selected to determine that a reminder e-mail was sent by the Operations Clerk prior to or on the response due date to the state(s) that had not responded to each selected voluntary corporate action.	No exceptions noted.
10.02	Voluntary corporate action responses from the states are recorded within NEXEN® by the Operations Clerk. If the state does not provide a response by the due date, the default action is selected automatically by the NEXEN® system.	Inspected the NEXEN® system documentation related to a sample of voluntary corporate actions to determine that, for each selected voluntary corporate action, if the state responded, the voluntary corporate action response was recorded within NEXEN® by the Operations Clerk and if the state did not respond, the default action was automatically selected by the NEXEN® system.	No exceptions noted.

#### **Control Objective 11**

Treasury Insurance and Lottery Safeguards: Controls provide reasonable assurance that all transaction history related to securities held by the states for Treasury Insurance and Lottery programs are processed and uploaded for each business day to the AS400 System.

<b>Control Activity Description</b>		Tests Performed by Service Auditor	Results of Testing	
11.01	On each business day, the custodial account activity report is automatically generated from the NEXEN® system and is uploaded into the AS400 system.	Inspected the custodial account activity report and the upload status report related to a sample of business days to determine that the custodial account activity report was automatically generated from the NEXEN® system and was uploaded into the AS400 system for each selected business day.	No exceptions noted.	
11.02	On each business day, management reviews status reports generated by the AS400 system to help ensure that the custodial account activity report is completely processed. Any identified issues are researched and resolved.	Inspected the AS400 status reports related to a sample of business days to determine that management reviewed status reports generated by the AS400 system for each selected day to help ensure that the custodial account activity report was completely processed. Further, inspected supporting documentation and inquired of the Director of Unclaimed Property Solutions to determine that no issues were identified as a result of the selected reviews; however, that if any issues had been identified, each issue would have researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.	
11.03	On a monthly basis, state lottery holdings reports are generated from the AS400 system and are e-mailed to states by members of the custody department to help facilitate state reconciliation procedures.	Inspected the lottery holding reports and e-mails related to a sample of months to determine that state lottery holdings reports were generated from the AS400 system and were e-mailed to states by members of the custody department to help facilitate state reconciliation procedures for each selected month.	No exceptions noted.	



# Avenu Insights & Analytics

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

System and Organization Controls (SOC) for Service Organizations Report for the period of January 1, 2022 to September 30, 2022



An Independent Service Auditor Report issued by FORVIS, LLP

Avenu Insights & Analytics
SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

# **Table of Contents**

Section I: Report of Independent Service Auditors	. 1
Section II: Avenu Insights & Analytics' Assertion	. 4
Section III: Avenu Insights & Analytics' Description of its System and Controls	. 5
Section IV: Description of the Trust Services Category, Criteria, Avenu Insights & Analytics' Related Controls, and the Independent Service Auditor's Description of Tests and Results	19



# Section I: Report of Independent Service Auditors

To: Management of Avenu Insights & Analytics

#### Scope

We have examined Avenu Insights & Analytics' (the "Company") accompanying description of its General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com (the "System") titled *Avenu Insights & Analytics' Description of its System and Controls* throughout the period January 1, 2022 to September 30, 2022, (the "description") based on the criteria for a description of a service organization's System in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (the "description criteria") and the suitability of the design and operating effectiveness of the controls stated in the description throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security (the "applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The Company uses the subservice organizations listed in the *Subservice Organizations* table in Section III of this report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Company's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

#### Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Avenu Insights & Analytics' Assertion* (the "assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Company is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

# FORV/S

#### Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably
  designed to provide reasonable assurance that the service organization achieved its service commitments
  and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that
  the service organization achieved its service commitments and system requirements based on the applicable
  trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

#### **Inherent Limitations**

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the System that individual report users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

#### **Description of Tests of Controls**

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV of this report.

# FORV/S

#### **Opinion**

In our opinion, in all material respects,

- A. The description presents Avenu Insights & Analytics' General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com that was designed and implemented throughout the period January 1, 2022 to September 30, 2022, in accordance with the description criteria.
- B. The controls stated in the description were suitably designed throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that Avenu Insights & Analytics' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Avenu Insights & Analytics' controls throughout that period.
- C. The controls stated in the description operated effectively throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that Avenu Insights & Analytics' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Avenu Insights & Analytics' controls operated effectively throughout that period.

#### **Restricted Use**

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the period January 1, 2022 to September 30, 2022, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's System interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary user entity controls and complementary subservice organization controls and how those
  controls interact with the controls at the service organization to achieve the service organization's service
  commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

# FORVIS, LLP

Raleigh, NC

February 22, 2023



The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.



# Section II: Avenu Insights & Analytics' Assertion

We have prepared the accompanying description of Avenu Insights & Analytics' (the "Company") General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com (the "System") titled *Avenu Insights & Analytics' Description of its System and Controls* throughout the period January 1, 2022 to September 30, 2022 (the "description") based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (the "description criteria"). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with the Company's System, particularly information about system controls that the Company has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The Company uses the subservice organizations listed in the *Subservice Organizations* table in Section III of this report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with related controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Company's controls.

We confirm, to the best of our knowledge and belief, that:

- A. The description presents the System that was designed and implemented throughout the period January 1, 2022 to September 30, 2022, in accordance with the description criteria.
- B. The controls stated in the description were suitably designed throughout the period January 1, 2022 to September 30, 2022 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period.
- C. The controls stated in the description operated effectively throughout the period January 1, 2022 to September 30, 2022 to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

# Section III: Avenu Insights & Analytics' Description of its System and Controls

#### A. Overview of Services Provided

Headquartered in Centreville, Virginia, Avenu Insights & Analytics ("Avenu", or the "Company") has a long history of helping state unclaimed property administrators efficiently and accurately manage their statutory responsibilities. Each state has its own unique set of rules, policies, practices, and goals, and these guideposts change from time to time. Avenu provides, among other services, a flexible integrated unclaimed property solution suite that simplifies the administration of holder reports, securities custody management, database maintenance, claims, claims payments, imaging, and permanent records retention. States using Avenu's unclaimed property management solutions gain access to a powerful set of administrative tools that efficiently and accurately manage unclaimed properties at every point within the administrative process.

## Summary of Services Provided

Avenu's Unclaimed Property Solutions ("UPS") is a division of Avenu SLS Holdings, LLC. Avenu's UPS business line provides unclaimed property administration solutions to the District of Columbia, Puerto Rico, Alberta, Quebec, and nearly every state within the U.S. Avenu UPS is headquartered in Quincy, Massachusetts. Staffing consists of approximately 50 full-time employees and consultants. The Senior Management team is comprised of experienced unclaimed property professionals and technical staff members.

Avenu UPS has provided unclaimed property services to state governments for over 30 years. Avenu's unclaimed property solutions include, but are not limited to, the Clearview Connect unclaimed management system, securities custody management, eClaims website, call center services, holder reporting website, annual compliance services, and the MissingMoney multi-state unclaimed property search engine.

## **B. Principal Service Commitments and System Requirements**

Avenu Insights & Analytics designs its processes and procedures related to the Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com to meet its objectives for its services. Those objectives are based on the service commitments that Avenu makes to user entities; the laws and regulations that govern the provision of the services; and the financial, operational, and compliance requirements that Avenu has established for the services. Security commitments to user entities are documented and communicated within Service Level Agreements (SLAs) and other customer agreements, as well as within the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following items:

- Security principles within the fundamental designs of the Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com that are designed to permit system users to access the information they need based on their role within the system while restricting them from accessing information not needed for their role; and
- Use of encryption technologies to protect customer data both at rest and in transit.

Avenu establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated within Avenu 's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

# C. Components of the System Used to Provide the Services

#### 1. Infrastructure

The General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com runs on Microsoft Windows' servers.

Rackspace and Microsoft Azure provide computer operation services to Avenu's Unclaimed Property Solutions (UPS) business. Rackspace and Azure are responsible for computer hardware, operating system maintenance, and back-up storage. Information security, along with security system settings, is controlled by Microsoft or Rackspace and Avenu.

Employees access the infrastructure through their desktops on company-supplied encrypted computers. Data communications between offices are encrypted with Cisco Virtual Private Networking (VPN) technology using Advanced Encryption Standard 256-bit encryption to protect data and intra-company communications.

An Avenu company-wide system is used for processing invoices, maintenance of Accounts Receivable aging, and determination of revenue recognition values.

The Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com use Microsoft Windows Server. These database servers and file servers are housed within Rackspace and Microsoft Azure secured Network Operations Centers (NOCs).

#### 2. Software

The following solutions are in-scope for this report:

Solution	Description	Operating System
eClaim Web Service	Web-based SaaS	Microsoft Windows
ecialiii web Service		Server
UPS2000	Delphi-based software	Microsoft Windows
UP\$2000		Server
Holder Beneuting Website	Web-based SaaS	Microsoft Windows
Holder Reporting Website		Server
Minginghamou agus	Web-based SaaS	Microsoft Windows
MissingMoney.com		Server

#### 3. People

Avenu has a staff of approximately 600 employees organized into the following functional areas:

Corporate. Executives, senior operations staff members, and company administrative support staff
members, such as legal, compliance, internal audit, training, contracting, accounting, finance, human
resources, and transportation provider relations.

- Operations. Staff members who administer the administration of user entities and provide the direct day-to-day services.
- IT. Help desk, IT infrastructure, IT networking, IT system administration, software systems
  development and application support, information security, and IT operations personnel manage
  electronic interfaces and business implementation support and telecom.
  - The help desk group provides technical assistance to the Unclaimed Property Claims Website
    users.
  - The infrastructure, networking, and systems administration staff members support Avenu's IT infrastructure which is used by the software.
  - The software development staff members develop and maintain custom software for Avenu, including the Unclaimed Property Claims Website, supporting utilities, and the external websites that interact with the Unclaimed Property Claims Website. The staff members include software developers, database administration, software quality assurance, and technical writers.
  - The information security staff members support the Unclaimed Property Claims Website indirectly by monitoring internal and external security threats and maintaining current antivirus software.
  - The information security staff members maintain the inventory of IT assets.
  - IT operations group manages the user interfaces for the Unclaimed Property Claims Website.

#### 4. Data

Confidential data can include:

- Protected Identifiable Information (PII);
- Employee or customer social security numbers, or other personal information;
- Customer data, including customer lists and customer contact information; and
- Financial data which has not been released publicly.

If confidential data is shared with third parties, such as service providers or Business Associates, a written confidential information and/or non-disclosure agreement must govern the provider's use of confidential information.

Confidential data requires additional security controls in order to help ensure its integrity. Avenu requires that the following guidelines be followed:

- Strong Encryption: Confidential data must always be stored in an encrypted form, whether such storage occurs on a user system, server, laptop, or any other device that allows for data storage.
- Network Segmentation: The Company must use firewalls, access control lists, or other security
  controls to separate the confidential data from the rest of the corporate network, and more
  specifically, to isolate industry clearinghouse functions.
- Physical Security: Systems that contain confidential data, as well as confidential data in hardcopy form, must be stored within secured areas.

- Printing: When printing confidential data, the user must use best efforts to help ensure that the
  information is not viewed by others. Printers that are used for confidential data must be located
  within secured areas.
- Emailing: Confidential data must not be emailed inside or outside the Company without the use of strong encryption.

#### 5. Policies and Procedures

Management has developed and communicated procedures to restrict logical access to the General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com. Changes to these procedures are performed annually and are authorized by senior management. These procedures cover the key security life cycle areas.

A variety of policies and procedures have been developed to help ensure objectives are carried out and risks are mitigated. A formal program is in place to periodically review and update policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to associates.

# D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

#### 1. Control Environment

The control environment sets the tone of an organization and influences the control awareness of the organization. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to appropriate controls through management's actions supported by its policies, procedures, and organizational structure.

Commitment to Integrity and Ethical Values

Avenu has developed a formal ethics policy as part of the employee handbook which is available on its Intranet and contains rules about employee conduct. Employees are required to read and evidence their knowledge and receipt of Avenu's employee handbook upon hire and annually thereafter. Avenu offers its employees a number of channels through which potential breaches of ethical behavior may be reported.

Oversight Responsibility of the Executive Management

The Company operates under the direction of its Chief Executive Officer ("CEO"), along with other senior executives ("Executive Team") that also serve as heads of the business units described within. The Executive Team holds itself accountable to the Company's ethics and conflict of interest policies and provides oversight of operations and activities. All areas are led by capable, experienced, and well-qualified individuals with years of experience applicable to their respective job responsibilities. Executives provide oversight of business units and are directly involved in the Company's operations.

Assignment of Authority and Responsibility

Executive management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures, under the ultimate oversight of the Executive Team. Management recognizes its responsibility for establishing and maintaining sound internal control and promoting integrity and ethical values to all personnel on a day-to-day basis.

#### Commitment to Competence

Avenu's values and commitment to competence begin with a commitment to engaging, developing, and supporting its people. This commitment starts with a clearly documented people selection process. Detailed job descriptions are created and maintained for each key position. Avenu's commitment to quality and competence is further evidenced by its approach to monitoring, evaluating, and supporting its people. The talent management process, along with staff training and development, helps ensure Avenu is providing its people with opportunities for professional growth.

#### Human Resource Policies and Practices

People are the key to Avenu's success, and the Human Resource ("HR") function is the organization driving programs to help ensure the Company engages, develops, and supports its people. The goal of the HR function is to build an organization of outstanding employees in an environment that encourages maximum engagement, development, and professional growth. Avenu is committed to respecting and supporting one another, regardless of physical differences, beliefs, or personal values. This commitment is expressed in Avenu's personnel policies and practices and begins with the recruiting process, which is the joint responsibility of the Operations' hiring managers and the Talent Acquisition Organization.

Avenu is an equal opportunity employer and is committed to providing a discrimination-free workplace. Employment decisions are based on each individual's skills and qualifications without regard to race, color, creed, religion, ancestry, national origin, age, gender/sex, marital status, sexual orientation, physical or mental disability, use of a guide dog or service animal, military/veteran status, citizenship status, genetic information, or any other category protected by law. This approach extends to every phase of the employment process including recruiting, hiring, training, promotion, compensation, benefits, transfers, and company-sponsored educational, social and recreational programs.

#### 2. Risk Assessment Process

The service organization operates within an environment faced with a variety of risks from internal and external sources.

#### Risk Objectives

The risk assessment approach involves an iterative process for identifying and assessing risks to the achievement of objectives. This approach forms the basis for determining how risks will be addressed by management. Avenu recognizes that risk management is a critical component of internal controls affecting all levels of the organization. Management regularly assesses the risks of internal fraud and has taken measures to deter and prevent such actions from occurring. Management is also aware of the risks related to its Information Technology ("IT") infrastructure, such as security, network operations, and disaster recovery.

#### Identification and Analysis of Risks

Risk management is primarily the responsibility of individual business units which perform periodic risk assessments that identify and document significant risks facing Avenu, including any fraud risks. The results of these risk assessments determine how the business units develop and implement controls, operating procedures, and compliance processes for addressing and mitigating such risks. Avenu's policies require that any instances of suspected or actual fraud be brought to the immediate attention of senior management, the Chief Financial Officer, and Avenu's Legal department.

## 3. Monitoring Activities

Avenu employs a combination of ongoing and periodic monitoring activities to verify that controls are functioning effectively and that risks are appropriately mitigated.

#### Ongoing Monitoring

Avenu uses a variety of reports and monitoring mechanisms to help ensure controls are functioning as intended. Management regularly reviews and assesses business operations to verify that reporting and monitoring mechanisms used are effective in managing the operations of the business, controls, and related risks.

#### Monitoring of the Subservice Organizations

Avenu utilizes various subservice organizations to provide services for the Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com environments. Management receives and reviews applicable SOC reports of subservice organizations on an annual basis. In addition, through its daily operational activities, management monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

#### 4. Information and Communication

Policies, procedures, and other information necessary to help achieve Avenu's business objectives are communicated through several means, including the Intranet, emails, newsletters, memoranda, meetings, and training sessions. Policies and procedures enforce the importance of adherence to and compliance with rules and regulations that govern business and operations. Policies and procedures are documented and are made available to employees on the Company Intranet.

# E. Description of Controls

#### 1. Control Environment

A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities.

Each employee and contractor is subjected to a criminal background check prior to his/her start date. The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 45 business days of his/her start date, and annually thereafter. The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. The Company's new employees and contractors must acknowledge a statement signifying that they have read, understand, and will follow the information security policies and the Company's Employee Handbook within 30 days of hire.

On a quarterly basis, the Board of Directors, who is independent from Senior Management, meets to provide oversight of the business and discuss accomplishments, challenges, financial, and operational plans and results. Management has established an Organizational Chart, which is available to internal users via the Company's intranet, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities.

#### 2. Communication and Information

The Company has provided a description of the in-scope applications and related services, including applicable information related to the boundaries of the System and its security-related commitments, on its website. The Company has reporting mechanisms in place for reporting security incidents and compliance concerns. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident.

#### 3. Risk Assessment

The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.

# 4. Monitoring Activities

Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved.

On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution.

#### 5. Control Activities

The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. The Director of Cybersecurity is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users, related parties, and vendors.

#### 6. Logical and Physical Access Controls

Access to the backup tool is restricted to appropriate individuals based on job function. The backup tool is configured to automatically protect backups of the in-scope applications and related databases utilizing Advanced Encryption Standards (AESs).

Valid user IDs and passwords are required to access the Company's network, in-scope application, and related databases. Password parameters for the network, the in-scope applications, and the related databases are configured to require a maximum password age, inactivity timeout, minimum password length, and password complexity.

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

Administrative access to the in-scope application and related databases is restricted to appropriate individuals based on job function. Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, is restricted to appropriate individuals based on job function. The ability to modify data transmission protocols is limited to appropriate users based on job function. Remote access to the network and to the production environment related to the in-scope applications and related databases is restricted to appropriate users via VPN.

Access to the network, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. Requests to add and/or modify access to the network, to the in-scope applications, and/or to the related databases are approved by management prior to access being granted. The Company performs a quarterly review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.

Formal data retention and disposal standards have been developed to provide guidelines for the secure disposal of Avenu and customer data. Prior to removal from Company facilities, all digital media is completely degaussed and sanitized to remove any data and software.

Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment. All transmissions of electronic information are encrypted as the default setting over public networks via Transport Layer Security (TLS). Transmission or movement of digital output beyond the boundary of the system occurs using authorized software supporting the advanced encryption standard (AES).

Laptops are configured to enforce hard drive encryption. Mobile Device Management software is deployed to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets via remote wipe, passcodes, and encryption. Antivirus software is in place on all workstations, laptops, and Company-hosted servers related to the in-scope application, and is updated with current virus definitions to protect data from infection by malicious code or virus.

#### 7. System Operations

When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented.

A Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved. Incremental and full backups of the in-scope application and related databases are configured to be performed daily and weekly, respectively. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved.

#### 8. Change Management

The Company has documented a formal Change Management Policy which governs the design, implementation, modification, and management of the in-scope application and related databases. Version control software is in place to manage current versions of source code related to the in-scope application and related databases. Access to promote changes into the production environment related to the in-scope application and related databases is limited to appropriate individuals without development responsibilities.

Each change to the in-scope application and related databases is applied and tested within development and/or testing environments which are separate from the production environment prior to migration into the production environment. Each change to the in-scope application and related databases must be approved by a member of management prior to promotion into the production environment. Scans are performed on in-scope applications source code to detect potential vulnerabilities prior to the release of each change into the production environment. All critical items must be remediated prior to each change being moved into the production environment.

## 9. Risk Management

On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.

The Company has defined a standard agreement with key vendors and third parties which includes the required security commitments in accordance with the Company's security policies. These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. A member of the Legal Department is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security practices and commitments.

# F. Additional Information about Management's Description

The controls supporting the service organization's service commitments and system requirements based on the applicable trust services criteria are included within Section IV of this report, *Description of the Trust Services Category, Criteria, Avenu Insights & Analytics' Related Controls, and the Independent Service Auditor's Description of Tests and Results.* Although the applicable trust services criteria and related control activities are presented within Section IV, they are an integral part of the Company's description of its system.

# G. Changes to the System During the Specified Period

There were no changes that were likely to affect report users' understanding of how the system was used to provide the service during the period from January 1, 2022 to September 30, 2022 (the "specified period").

# H. System Incidents

Management did not identify any significant system incidents during the period January 1, 2022 to September 30, 2022.

# I. Non-Applicable Trust Services Criteria

Common Criteria			
Non-Ap	plicable Trust Services Criteria	Avenu Insights & Analytics' Ration	
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical access to the defined system is the responsibility of the respective subservice organization carved-out of this report.	

# J. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organization, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Criteria Addressed
Rackspace Technology, Inc. ("Rackspace")	The Company uses Rackspace to provide co-location Data Center and IT infrastructure management services, including the restriction of physical access to the defined system. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria:	CC 6.1*, CC 6.4* CC 6.8*, CC 8.1*
	<ul> <li>Controls around the physical security of the Data Centers hosting the in-scope applications,</li> <li>Controls around the environmental controls at the Data Centers hosting the in-scope applications to support the disaster recovery processes, and</li> <li>Controls around the antivirus, patching, and server management for the Data Centers hosting the in-scope applications.</li> </ul>	
	In addition, the Company has identified the following control to help monitor the subservice organization:	
	<ul> <li>On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.</li> </ul>	

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Criteria Addressed
Microsoft Corporation	The Company uses Microsoft Corporation's Azure environment to provide co-location Data Center and IT infrastructure management services, including the restriction of physical access to the defined system. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria:	CC 6.1*, CC 6.2* CC 6.4*, CC 7.5* CC 8.1*, CC 9.2*
	<ul> <li>Controls around the physical security of the Data Centers hosting the in-scope applications,</li> <li>Controls around logical access and change management of the infrastructure supporting the in-scope applications, and</li> <li>Controls around the environmental controls at the Data Centers hosting the in-scope applications to support the disaster recovery processes.</li> </ul>	
	In addition, the Company has identified the following control to help monitor the subservice organization:	
	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.	

<sup>\*</sup> The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.

# K. Complementary User Entity Controls

Avenu Insights & Analytics' controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

User Entity Controls	Related Criteria
Each user entity is responsible for implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Avenu.	CC 5.2*
Each user entity is responsible for helping to ensure data sent outside its organization is protected by appropriate methods that consider confidentiality, privacy, integrity, availability, and non-repudiation.	CC 6.7*
Each user entity is responsible for developing, and if necessary, implementing, a Business Continuity and Disaster Recovery Plan (BCDRP) that aids in the continuation of services provided by Avenu.	CC 7.5*, CC 9.1*
Each user entity is responsible for implementing industry-standard security practices such as device antivirus, network perimeter firewalls, and device vulnerability patching.	CC 6.6*, CC 6.8*, CC 7.1*, CC 7.2*
Each user entity is responsible for preventing unauthorized users from reading other users' screens through mechanisms such as screen savers and automatic logouts after a brief period of inactivity.	CC 6.1*
Each user entity is responsible for establishing proper controls over the use of user IDs and passwords that are used to access the System.	CC 5.2*, CC 6.1*
Each user entity is responsible for protecting the privacy of personal information that appears on screens or reports that are printed using the System.	CC 6.1*
Each user entity is responsible for helping to ensure that only authorized and properly trained personnel are allowed access to the System.	CC 6.2*, CC 6.3*
Each user entity is responsible for helping to ensure timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Avenu's System.	CC 6.1*, CC 6.2*, CC 6.3*, CC 6.6*, CC 6.7*

## Avenu Insights & Analytics SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

User Entity Controls	Related Criteria
Each user entity is responsible for contacting Avenu in the event of suspicious account activities or of a potential information security breach impacting the System.	CC 4.2*, CC 7.3*, CC 7.4*, CC 7.5*

<sup>\*</sup> The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.

# Section IV: Description of the Trust Services Category, Criteria, Avenu Insights & Analytics' Related Controls, and the Independent Service Auditor's Description of Tests and Results

# A. Information Provided by FORVIS, LLP

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to provide user entities of the Company's System, those prospective user entities, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System. The description is intended to provide users with information about the System. Our examination was limited to the applicable trust services criteria and related controls specified by the Company in sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations. It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. If internal control is not effective at user entities, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

# B. Types and Descriptions of the Tests of Operating Effectiveness

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type Description	
Inquiry Inquired of appropriate personnel and corroborated with management	
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control
Reperformance Reperformed the control, or processing of the application control, its operation	

In addition, as required by paragraph .36 of AT-C section 205, Assertion-Based Examination Engagements (AICPA, Professional Standards), when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Avenu Insights & Analytics SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

# C. Trust Services Category, Criteria, Control Activities, and Testing Provided by the Service Auditor

The trust services criteria relevant to security address that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the Company's ability to achieve its service commitments and system requirements.

Control activities, test procedures, and results presented without grey shading indicate an original instance of a particular control activity, test procedure, and result within Section IV of the report. Control activities, test procedures, and results presented with a grey shading indicate that the particular control activity, test procedure, and result has been previously presented within Section IV of the report. The duplication of these items results from the requirement that each criterion stands alone and the relevance of certain control activities for multiple criteria.

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 1.1 - CO	SO Principle 1: The entity demo	nstrates a commitment to integrity and	d ethical values.	
CC 1.1-01	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures.	Inspected the Employee Handbook and the Code of Ethics and Business Conduct to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the Director of Operations to determine that the Employee Handbook and the Code of Ethics and Business Conduct which were inspected were in place throughout the specified period.	No exceptions noted	
CC 1,1-02	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities.	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted	
CC 1.1-03	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet.	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category  CRITERIA GROUP 1: Common Criteria Related to Control Environment			
		Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 1.1-04	The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 45 business days of his/her start date,	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security to employees and contractors. Further, inquired of Director of Operations to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted.
	and annually thereafter.	Inspected the Security Awareness Acknowledgments related to a sample of new employees and contractors to determine that each selected new employee and contractor completed the security awareness program within 45 business days of his/her start date.	No exceptions noted.

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
		Inspected the Security Awareness Acknowledgments related to a sample of employees and contractors to determine that each selected employee and contractor completed the security awareness program during the specified period.	No exceptions noted.	
CC 1.1-05	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security.	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.	
CC 1.1-06	The Company's new employees and contractors must acknowledge a statement signifying that they have read, understand, and will follow the Company's Employee Handbook within 30 days of hire.	Inspected the Employee Handbook Acknowledgement Forms related to a sample of new employees and contractors to determine that each selected new employee and contractor signed a statement signifying that he/she had read, understood, and would follow the Company's Employee Handbook within 30 days of hire.	No exceptions noted.	

Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.				
CC 1.2-01	On a quarterly basis, the Board of Directors, who is independent from Senior Management, meets to provide oversight of the business and discuss accomplishments, challenges, financial, and operational plans and results.	Inspected the meeting minutes related to a selected quarter to determine that the Board of Directors, who is independent from Senior Management, met to provide oversight of the business and discuss accomplishments, challenges, financial, and operation plans and results for the selected quarter.	No exceptions noted	
CC 1.2-02	Management has established an Organizational Chart, which is available to internal users via the Company's intranet, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities.	Inspected the Organizational Chart to determine that management established and Organizational Chart and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the Director of Operations to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.	
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the Director of Operations to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.	

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.				
CC 1.3-01	The Director of Cybersecurity is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users, related parties, and vendors.	Observed the security policies on the Company's intranet and website to determine that the policies were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the Director of Operations to determine that these policies were available on the Company's intranet and website throughout the specified period.	No exceptions noted	
		Inspected the Director of Cybersecurity job description to determine that the Director of Cybersecurity was responsible for changes to security practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted	
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, email, and/or contract amendment.	The Service Auditor noted that this portion of the Contro Activity did not operate during the specified period, as there were no changes made to the security practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control	

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description	Tests Performed by Service Auditor	Results of Testing		
	Inspected the policy revision history used to pull the listing of changes made to the security practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no changes made to the security practices and commitments during the specified period. Further, inquired of the Director of Operations to determine that there were no changes made to the security practices and commitments during the specified period.	No exceptions noted		

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category  CRITERIA GROUP 1: Common Criteria Related to Control Environment				
CC 1.3-02	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the Director of Operations to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted	

CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 1.3-03	The Company has defined a standard agreement with key vendors and third parties which includes the required security commitments in accordance with the Company's security policies. These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. A member of the Legal Department is responsible for reviewing and approving of all new third-party contracts to help ensure that they	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security commitments in accordance with the Company's security policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the Director of Operations to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted		
	include the applicable security practices and commitments.	Inspected the third-party contracts related to a sample of new third parties to determine that a member of the Legal Department reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new third-party vendors during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.		

CRITERIA	GROUP 1: Common Criteria Rel	ated to Control Environment	
Control Ac	tivity Description	Tests Performed by Service Auditor	Results of Testing
		Inspected the query used to pull the system-generated listing of new third-party vendors during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no new third-party vendors during the specified period. Further, inquired of the Director of Operations to determine that there were no new third-party vendors during the specified period.	No exceptions noted
CC 1.3-04	Management has established an Organizational Chart, which is available to internal users via the Company's intranet, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management established and Organizational Chart and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the Director of Operations to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the Director of Operations to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.

COMMON C	COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA G	ROUP 1: Common Criteria Rela	ted to Control Environment			
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 1.3-05	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted		
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.		
CC 1.3-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.		

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.				
CC 1.4-01	Each employee and contractor is subjected to a criminal background check prior to his/her start date.	Inspected the background checks and supporting documentation related to a sample of new employees and contractors to determine that each selected new employee/contractor was subjected to a background check prior to his/her start date.	No exceptions noted	
CC 1.4-02	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook and the Code of Ethics and Business Conduct to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the Director of Operations to determine that the Employee Handbook and the Code of Ethics and Business Conduct which were inspected were in place throughout the specified period.	No exceptions noted	
CC 1.4-03	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-02)	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted	

	RITERIA CATEGORY: Criteria C	CRITERIA CROUR 4: Common Criteria Balata da Comta de Carta de Comta de Carta de Cart				
CRITERIA GROUP 1: Common Criteria Related to Control Environment						
Control Activ	vity Description	Tests Performed by Service Auditor	Results of Testing			
CC 1.4-04	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted			
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted			
CC 1.4-05	The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 45 business days of his/her start date, and annually thereafter. (CC 1.1-04)	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security to employees and contractors. Further, inquired of Director of Operations to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted			

CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Control Activ	vity Description	Tests Performed by Service Auditor	Results of Testing		
		Inspected the Security Awareness Acknowledgments related to a sample of new employees and contractors to determine that each selected new employee and contractor completed the security awareness program within 45 business days of his/her start date.	No exceptions noted		
		Inspected the Security Awareness Acknowledgments related to a sample of employees and contractors to determine that each selected employee and contractor completed the security awareness program during the specified period.	No exceptions noted		
CC 1.4-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development,	No exceptions noted		

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category  CRITERIA GROUP 1: Common Criteria Related to Control Environment				
	SO Principle 5: The entity holds ties in the pursuit of objectives.	individuals accountable for their inter	nal control	
CC 1.5-01	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook and the Code of Ethics and Business Conduct to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the Director of Operations to determine that the Employee Handbook and the Code of Ethics and Business Conduct which were inspected were in place throughout the specified period.	No exceptions noted	
CC 1.5-02	Management has established an Organizational Chart, which is available to internal users via the Company's intranet, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management established and Organizational Chart and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the Director of Operations to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted	
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the Director of Operations to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category  CRITERIA GROUP 1: Common Criteria Related to Control Environment				
CC 1.5-03	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-02)	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted	
CC 1.5-04	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted	
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these	No exceptions noted.	
	9:	policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.		

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category					
CRITERIA G	CRITERIA GROUP 1: Common Criteria Related to Control Environment				
Control Activity Description  Tests Performed by Service Auditor  Results of Testing			Results of Testing		
CC 1.5-05	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted		

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category  CRITERIA GROUP 2: Common Criteria Related to Communication and Information				
	O Principle 13: The entity obtai unctioning of internal control.	ns or generates and uses relevant, qu	ality information to	
CC 2.1-01	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met.	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	No exceptions noted	
CC 2.1-02	A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved.	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	

CRITERIA GROUP 2: Common Criteria Related to Communication and Information				
Control Act	ivity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted	
CC 2.1-03	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution.	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted	
CC 2.1-04	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted	

CRITERIA G	CRITERIA GROUP 2: Common Criteria Related to Communication and Information				
	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 2.1-05	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted		
	approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted		
CC 2.1-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted		

CRITERIA G	CRITERIA GROUP 2: Common Criteria Related to Communication and Information				
	vity Description	Tests Performed by Service Auditor	Results of Testing		
		nally communicates information, inclu ary to support the functioning of intern			
CC 2.2-01	The Company has provided a description of the in-scope applications and related services, including applicable information related to the boundaries of the System and its security-related commitments, on its website.	Observed the Company's website to determine that the Company provided a description of the in-scope applications and its services on its website and that the description included applicable information related to the boundaries of the System and its security-related commitments. Further, inquired of the Director of Operations to determine that a description of the in-scope applications and its services was on the Company's website throughout the specified period.	No exceptions noted		
CC 2.2-02	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the	Observed the Company's website to determine that the Company has reporting mechanisms in place for reporting security incidents and compliance concerns, and that these mechanisms were communicated to all stakeholders via the Company's external website. Further, inquired of the Director of Operations to determine that this process was in place throughout the specified period.	No exceptions noted		
	nature of the suspected ethics/policy violation claim or suspected security incident.	Inspected the incident reports and corresponding job titles related to a sample of security incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident and each management individual's job function.	No exceptions noted		

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 2: Common Criteria Related to Communication and Information				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 2.2-03	The Director of Cybersecurity is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users, related parties, and vendors. (CC 1.3-01)	Observed the security policies on the Company's intranet and website to determine that the policies were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the Director of Operations to determine that these policies were available on the Company's intranet and website throughout the specified period.	No exceptions noted	
		Inspected the Director of Cybersecurity job description to determine that the Director of Cybersecurity was responsible for changes to security practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted	
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, email, and/or contract amendment.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no changes made to the security practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.	

CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Control Act	ivity Description	Tests Performed by Service Auditor	Results of Testing		
		Inspected the policy revision history used to pull the listing of changes made to the security practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no changes made to the security practices and commitments during the specified period. Further, inquired of the Director of Operations to determine that there were no changes made to the security practices and commitments during the specified period.	No exceptions noted		
CC 2.2-04	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted		

CDITEDIA	DOUD O. C Outtool - Dillo	4.44.0	
CRITERIA GROUP 2: Common Criteria Rela Control Activity Description		Tests Performed by Service Auditor	Results of Testing
		Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted
CC 2.2-05	The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 45 business days of his/her start date,	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security to employees and contractors. Further, inquired of Director of Operations to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted
	and annually thereafter. (CC 1.1-04)	Inspected the Security Awareness Acknowledgments related to a sample of new employees and contractors to determine that each selected new employee and contractor completed the security awareness program within 45 business days of his/her start date.	

CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing		
		Inspected the Security Awareness Acknowledgments related to a sample of employees and contractors to determine that each selected employee and contractor completed the security awareness program during the specified period.	No exceptions noted		
CC 2.2-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.		
CC 2.2-07	The Company's new employees and contractors must acknowledge a statement signifying that they have read, understand, and will follow the Company's Employee Handbook within 30 days of hire. (CC 1.1-06)	Inspected the Employee Handbook Acknowledgement Forms related to a sample of new employees and contractors to determine that each selected new employee and contractor signed a statement signifying that he/she had read, understood, and would follow the Company's Employee Handbook within 30 days of hire.	No exceptions noted.		

CRITERIA G	ROUP 2: Common Criteria Rela	ted to Communication and Information	1
Control Activity Description		Tests Performed by Service Auditor	Results of Testing
	SO Principle 15: The entity comming of internal control.	municates with external parties regard	ling matters affecting
CC 2.3-01	The Director of Cybersecurity is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users, related parties, and vendors. (CC 1.3-01)	Observed the security policies on the Company's intranet and website to determine that the policies were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the Director of Operations to determine that these policies were available on the Company's intranet and website throughout the specified period.	No exceptions noted
		Inspected the Director of Cybersecurity job description to determine that the Director of Cybersecurity was responsible for changes to security practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, email, and/or contract amendment.	The Service Auditor noted that this portion of the Contro Activity did not operate during the specified period, as there were no changes made to the security practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Contro

COMMON C	COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information						
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing			
		Inspected the policy revision history used to pull the listing of changes made to the security practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no changes made to the security practices and commitments during the specified period. Further, inquired of the Director of Operations to determine that there were no changes made to the security practices and commitments during the specified period.	No exceptions noted			
CC 2.3-02	The Company has provided a description of the in-scope applications and related services, including applicable information related to the boundaries of the System and its security-related commitments, on its website. (CC 2.2-01)	Observed the Company's website to determine that the Company provided a description of the in-scope applications and its services on its website and that the description included applicable information related to the boundaries of the System and its security-related commitments. Further, inquired of the Director of Operations to determine that a description of the in-scope applications and its services was on the Company's website throughout the specified period.	No exceptions noted			

CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 2.3-03	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim	Observed the Company's website to determine that the Company has reporting mechanisms in place for reporting security incidents and compliance concerns, and that these mechanisms were communicated to all stakeholders via the Company's external website. Further, inquired of the Director of Operations to determine that this process was in place throughout the specified period.	No exceptions noted		
	or suspected security incident. (CC 2.2-02)	Inspected the incident reports and corresponding job titles related to a sample of security incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident and each management individual's job function.	No exceptions noted		

CRITERIA G	CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing			
	SO Principle 6: The entity specif n and assessment of risks relati	ies objectives with sufficient clarity to ing to objectives.	enable the			
CC 3.1-01	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted			
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted			

CRITERIA GROUP 3: Common Criteria Related to Risk Assessment				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 3.1-02	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted	
CC 3.1-03	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted	

CRITERIA G	CRITERIA GROUP 3: Common Criteria Related to Risk Assessment						
	vity Description	Tests Performed by Service Auditor	Results of Testing				
		ifies risks to the achievement of its objection					
CC 3.2-01	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted				

CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 3.2-02	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the Director of Operations to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions note		

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Control Activity Description		Tests Performed by Service Auditor	Results of Testing		
CC 3.2-03	The Company has defined a standard agreement with key vendors and third parties which includes the required security commitments in accordance with the Company's security policies. These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. A member of the Legal Department is responsible for reviewing and approving of all new third-party contracts to help ensure that they	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security commitments in accordance with the Company's security policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the Director of Operations to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions note		
	include the applicable security practices and commitments. (CC 1.3-03)	Inspected the third-party contracts related to a sample of new third parties to determine that a member of the Legal Department reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new third-party vendors during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.		

CRITERIA G	ROUP 3: Common Criteria Rela	ted to Risk Assessment	
Control Activity Description		Tests Performed by Service Auditor	Results of Testing
		Inspected the query used to pull the system-generated listing of new third-party vendors during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no new third-party vendors during the specified period. Further, inquired of the Director of Operations to determine that there were no new third-party vendors during the specified period.	No exceptions noted
	SO Principle 8: The entity consider to a society of objectives.	ders the potential for fraud in assessin	g risks to the
CC 3.3-01	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 3: Common Criteria Related to Risk Assessment				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
	SO Principle 9: The entity identifof internal control.	ies and assesses changes that could	significantly impact	
CC 3.4-01	Management has established an Organizational Chart, which is available to internal users via the Company's intranet, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management established and Organizational Chart and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the Director of Operations to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted	
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the Director of Operations to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted	
CC 3.4-02	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted	

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 3: Common Criteria Related to Risk Assessment				
Control Activ	vity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted	
CC 3.4-03	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted	

CRITERIA G	ROUP 3: Common Criteria Rela	ted to Risk Assessment	
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing
CC 3.4-04	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the Director of Operations to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions note:

CRITERIA	A GROUP 4: Common Criteria Re	elated to Monitoring Activities			
Control A	activity Description	Tests Performed by Service Auditor	Results of Testing		
CC 4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.					
CC 4.1- 01	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	No exceptions noted.		
CC 4.1- 02	A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved.	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted.		
	(CC 2.1-02)	Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted.		

CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Control A	ctivity Description	Tests Performed by Service Auditor	Results of Testing		
CC 4.1- 03	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted		
timely ma		aluates and communicates internal con le for taking corrective action, including			
CC 4.2- 01	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented.	Inspected the Incident Response Plan to determine that when an incident related to system security was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the Director of Operations to determine that the Incident Response Plan which was inspected was in place throughout the specified period.	No exceptions noted		
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	No exceptions noted		

CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities				
Control A	ctivity Description	Tests Performed by Service Auditor	Results of Testing	
CC 4.2- 02	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
	\$ t	Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	No exceptions noted.	
CC 4.2- 03	A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted.	
	(00 2.1-02)	Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted.	

CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities				
Control A	ctivity Description	Tests Performed by Service Auditor	Results of Testing	
CC 4.2- 04	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted	
CC 4.2- 05	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of noncompliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook and the Code of Ethics and Business Conduct to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the Director of Operations to determine that the Employee Handbook and the Code of Ethics and Business Conduct which were inspected were in place throughout the specified period.	No exceptions noted	

COMMON C	COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category					
CRITERIA G	ROUP 5: Common Criteria Rela	ted to Control Activities				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing			
CC 5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.						
CC 5.1-01	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.  Inspected the escalation procedures and the support tickets related to a sample of alert notifications to	No exceptions noted.  No exceptions noted.			
		determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	J			
CC 5.1-02	A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted.			

CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted.	
CC 5.1-03	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted.	
CC 5.1-04	Management has established an Organizational Chart, which is available to internal users via the Company's intranet, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management established and Organizational Chart and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the Director of Operations to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.	
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the Director of Operations to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.	

COMMON C	RITERIA CATEGORY: Criteria C	ommon to the Security Trust Services	Category		
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Control Activity Description		Tests Performed by Service Auditor	Results of Testing		
CC 5.1-05	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted		
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted		

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Act	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 5.1-06	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted	
	SO Principle 11: The entity also to support the achievement of o	selects and develops general control a bjectives.	activities over	
CC 5.2-01	Each change to the in-scope applications and related databases is applied and tested within development and/or testing environments which are separate from the production environment prior to migration into the production environment.	Observed the production, development, and testing environments to determine that each change to the in-scope applications and related databases was applied and tested within a development and/or testing environment separate from the production environment. Further, inquired of the Senior Engineer of Servers, Storage, and Virtualization to determine that these environments were separate throughout the specified period.	No exceptions noted	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Acti	ivity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the change requests and supporting documentation related to a sample of changes to the in-scope applications and related databases to determine that each selected change was applied and tested within a development and/or testing environment separate from the production environment prior to migration into the production environment.	No exceptions noted	
CC 5.2-02	Access to promote changes into the production environment related to the inscope applications and related databases is restricted to appropriate individuals based on job function.	Inspected the listing of users with access to promote changes into the production environment related to the in-scope applications and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listing was appropriate to have this access.	No exceptions noted	
CC 5.2-03	Each change to the in-scope applications and related databases must be approved by a member of management prior to promotion into the production environment.	Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope applications and related databases to determine that each selected change was approved by a member of management prior to promotion into the production environment.	No exceptions noted	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Acti	vity Description	Auditor	Results of Testing  No exceptions noted.	
CC 5.2-04	The Company has documented a formal Change Management Policy which governs the design, implementation, modification, and management of the inscope applications and related databases.			
CC 5.2-05	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.	Inspected the listings of users with Administrative access to the in-scope applications and related databases and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted.	
CC 5.2-06	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, is restricted to appropriate individuals based on job function.	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted.	

CRITERIA G	ROUP 5: Common Criteria Rela	ted to Control Activities	
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing
CC 5.2-07	Valid user IDs and passwords are required to access the Company's network, in-scope applications, and related databases.	Observed the authentication configurations for the network, the inscope applications, and the related databases to determine that a valid user ID and password were required to access the Company's network, inscope applications, and related databases. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted
	SO Principle 12: The entity deplo d in procedures that put policies	bys control activities through policies into action.	that establish what is
CC 5.3-01	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	No exceptions noted

COMMON C	COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 5: Common Criteria Related to Control Activities  Control Activity Description  Tests Performed by Service Auditor  Results of Testing					
					CC 5.3-02
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted.		
CC 5.3-03	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted.		

CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 5.3-04	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Response Plan to determine that when an incident related to system security was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the Director of Operations to determine that the Incident Response Plan which was inspected was in place throughout the specified period.	No exceptions noted	
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	No exceptions noted.	
CC 5.3-05	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-02)	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted.	
CC 5.3-06	The Director of Cybersecurity is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users, related parties, and vendors. (CC 1.3-01)	Observed the security policies on the Company's intranet and website to determine that the policies were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the Director of Operations to determine that these policies were available on the Company's intranet and website throughout the specified period.	No exceptions noted.	

CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Activity Description	Tests Performed by Service Auditor	Results of Testing		
	Inspected the Director of Cybersecurity job description to determine that the Director of Cybersecurity was responsible for changes to security practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted		
	Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, email, and/or contract amendment.	The Service Auditor noted that this portion of the Contro Activity did not operate during the specified period, as there were no changes made to the security practices and commitments during the specified period. Therefore, the Service Auditor could not test the		
		operating effectiveness of this portion of the Contro Activity.		

CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Act	vity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the policy revision history used to pull the listing of changes made to the security practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no changes made to the security practices and commitments during the specified period. Further, inquired of the Director of Operations to determine that there were no changes made to the security practices and commitments during the specified period.	No exceptions noted	
CC 5.3-07	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 5: Common Criteria Related to Control Activities				
Control Activ	vity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted	
CC 5.3-08	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted	

		common to the Security Trust Services		
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.				
CC 6.1-01	Access to the backup tool is restricted to appropriate individuals based on job function.	Inspected the listings of users with access to the backup tool and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	
CC 6.1-02	The backup tool is configured to automatically protect backups of the in-scope application and related databases utilizing Advanced Encryption Standards (AESs).	Observed the backup tool configurations to determine that the backup tool was configured to automatically protect backups of the in-scope application and related databases with Advanced Encryption Standards (AESs). Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
CC 6.1-03	Laptops are configured to enforce hard drive encryption.	Observed the group policy encryption configurations to determine that the group policy was configured to enforce hard drive encryption on all Company laptops. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	

COMMON C	COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing  No exceptions noted.		
CC 6.1-04	Access to the network, to the in-scope application, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date.	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the inscope application, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.			
CC 6.1-05	Password parameters for the network, the in-scope application, and the related databases are configured to require a maximum password age, inactivity timeout, minimum password length, and password complexity.	Observed the password configurations that governed user access to the network, the in-scope application, and the related databases to determine that password parameters for the network, the in-scope application, and the related databases were configured to meet or exceed the requirements defined within the control activity. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		
CC 6.1-06	The ability to modify data transmission protocols is limited to appropriate users based on job function.	Inspected the listing of users with the ability to modify data transmission protocols and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listing was appropriate to have this access.	No exceptions noted.		

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 6.1-07	Remote access to the network and to the production environment related to the in-scope application and related databases is restricted to appropriate users via VPN.	Observed the remote access authentication configurations to determine that remote access to the network and to the production environment related to the in-scope application and related databases was restricted via VPN. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
		Inspected the listing of users with remote access to the network and to the production environment related to the in-scope application and related databases and the corresponding job titles for a sample of those users to determine that each selected user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each selected user on the listing was appropriate to have this access.	No exceptions noted	
CC 6.1-08	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listings of users with Administrative access to the in-scope applications and related databases and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Act	ivity Description	Tests Performed by Service Auditor	Results of Testing	
CC 6.1-09	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	
CC 6.1-10	Valid user IDs and passwords are required to access the Company's network, in-scope applications, and related databases. (CC 5.2-07)	Observed the authentication configurations for the network, the inscope applications, and the related databases to determine that a valid user ID and password were required to access the Company's network, inscope applications, and related databases. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
authorizes r	ew internal and external users ss is administered by the entity	and granting system access, the entity whose access is administered by the entity, user system credentials are removed	ntity. For those users	
CC 6.2-01	Requests to add and/or modify access to the network, to the in-scope application, and/or to the related databases are approved by management prior to access being granted.	Inspected the request tickets and supporting documentation related to a sample of users granted access to the network and access modifications to the in-scope applications and/or to the related databases to determine that each selected addition or modification was approved by management prior to access being granted.	No exceptions noted.	

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 6.2-02	Access to the network, to the in-scope application, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-04)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the inscope application, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted	
protected in	formation assets based on roles	removes access to data, software, fund s, responsibilities, or the system desig t privilege and segregation of duties, t	n and changes,	
CC 6.3-01	Access to the network, to the in-scope application, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-04)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the inscope application, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted	
CC 6.3-02	Requests to add and/or modify access to the network, to the in-scope application, and/or to the related databases are approved by management prior to access being granted. (CC 6.2-01)	Inspected the request tickets and supporting documentation related to a sample of users granted access to the network and access modifications to the in-scope applications and/or to the related databases to determine that each selected addition or modification was approved by management prior to access being granted.	No exceptions noted	

CRITERIA G	ROUP 6: Common Criteria Rela	ted to Logical and Physical Access Co	ontrols		
Control Activity Description		Tests Performed by Service Auditor	Results of Testing		
CC 6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.					
CC 6.5-01	Formal data retention and disposal standards have been developed to provide guidelines for the secure disposal of Avenu and customer data.	Inspected the Security Policy to determine that formal data retention and disposal standards had been developed to provide guidelines for the secure disposal of Avenu and customer data. Further, inquired of Director of Operations to determine that the Security Policy was in place throughout the specified period.	No exceptions noted		
CC 6.5-02	Prior to removal from Company facilities, all digital media is completely degaussed and sanitized to remove any data and software.	Inspected the data scrubbing certifications related to a sample of physical media devices (e.g., hard drives, thumb drives, etc.) which were disposed/destroyed to determine that each selected physical media device was scrubbed prior to disposal to avoid compromising confidential information.	No exceptions noted		
	entity implements logical accesside its system boundaries.	ss security measures to protect agains	st threats from		
CC 6.6-01	Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment.	Observed the network device (e.g., routers, switches, firewalls) configurations to determine that the devices were deployed and were maintained to detect and prevent threats to the Company's environment. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Control Activity Description		Tests Performed by Service Auditor	Results of Testing		
		Inspected the network diagram to determine that network devices (e.g., routers, switches, and firewalls) were deployed at all external access points to detect and prevent threats to the Company's environment. Further, inquired of the Director of Operations to determine that the network diagram which was inspected was in place throughout the specified period.	No exceptions noted		
CC 6.6-02	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	No exceptions noted		

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 6.6-03	A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted		
CC 6.6-04	Access to the backup tool is restricted to appropriate individuals based on job function. (CC 6.1-01)	Inspected the listings of users with access to the backup tool and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted		

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 6.6-05	Administrative access to the network and in-scope utilities; including access to firewalls and intrusion prevention devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	
CC 6.6-06	Access to the network, to the in-scope application, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-04)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the inscope application, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted	
CC 6.6-07	The ability to modify data transmission protocols is limited to appropriate users based on job function. (CC 6.1-06)	Inspected the listing of users with the ability to modify data transmission protocols and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listing was appropriate to have this access.	No exceptions noted	

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA G	CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Act	vity Description	Tests Performed by Service Auditor	Results of Testing		
CC 6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.					
CC 6.7-01	Mobile Device Management software is deployed to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets via remote wipe, passcodes, and encryption.	Observed the Mobile Device Management software configurations to determine that software was deployed to protect mobile devices (such as laptops, smart phones, and tablets) that served as information assets vi remote wipe, passcodes, and encryption. Further, inquired of the Senior Engineer of Servers, Storage, Virtualization to determine that these configurations were in place throughout the specified period.	No exceptions noted		
CC 6.7-02	All transmissions of electronic information are encrypted as the default setting over public networks via Transport Layer Security (TLS).	Observed the transmission configurations to determine that all transmissions of electronic information were encrypted as the default setting over public networks via TLS. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		
CC 6.7-03	Transmission or movement of digital output beyond the boundary of the system occurs using authorized software supporting the advanced encryption standard (AES).	Observed the transmission configurations related to the transmission or movement of digital output beyond the boundary of the system to determine that transmission or movement of digital output beyond the boundary of the system was configured to occur using authorized software supporting the advanced encryption standard (AES). Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 6.7-04	Access to the backup tool is restricted to appropriate individuals based on job function. (CC 6.1-01)	Inspected the listings of users with access to the backup tool and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	
CC 6.7-05	The backup tool is configured to automatically protect backups of the in-scope application and related databases utilizing Advanced Encryption Standards (AESs). (CC 6.1-02)	Observed the backup tool configurations to determine that the backup tool was configured to automatically protect backups of the in-scope application and related databases with Advanced Encryption Standards (AESs). Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted.	
CC 6.7-06	Laptops are configured to enforce hard drive encryption. (CC 6.1-03)	Observed the group policy encryption configurations to determine that the group policy was configured to enforce hard drive encryption on all Company laptops. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted.	
CC 6.7-07	Prior to removal from Company facilities, all digital media is completely degaussed and sanitized to remove any data and software. (CC 6.5-02)	Inspected the data scrubbing certifications related to a sample of physical media devices (e.g., hard drives, thumb drives, etc.) which were disposed/destroyed to determine that each selected physical media device was scrubbed prior to disposal to avoid compromising confidential information.	No exceptions noted.	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category  CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
CC 6.7-08	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)			
CC 6.7-09	Access to the network, to the in-scope application, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-04)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the inscope application, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted	
CC 6.7-10	Remote access to the network and to the production environment related to the in-scope application and related databases is restricted to appropriate users via VPN. (CC 6.1-07)	Observed the remote access authentication configurations to determine that remote access to the network and to the production environment related to the in-scope application and related databases was restricted via VPN. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Control Act	ivity Description	Tests Performed by Service Auditor	Results of Testing		
		Inspected the listing of users with remote access to the network and to the production environment related to the in-scope application and related databases and the corresponding job titles for a sample of those users to determine that each selected user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each selected user on the listing was appropriate to have this access.	No exceptions noted		
	entity implements controls to p d or malicious software to meet	prevent or detect and act upon the intro the entity's objectives.	oduction of		
CC 6.8-01	Access to the network, to the in-scope application, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-04)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the inscope application, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted		
CC 6.8-02	Antivirus software is in place on all workstations, laptops, and Company-hosted servers related to the inscope application, and is updated with current virus definitions to protect data from infection by malicious code or virus.	Observed the antivirus software global configurations to determine that antivirus software was in place on all workstations, laptops, and Company-hosted servers related to the in-scope application, and that antivirus software was updated with current virus definitions automatically to protect data from infection by malicious code or virus. Further, inquired of Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted		

CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 6.8-03	On an annual basis, all changes to the production environment related to the inscope applications and related databases are reviewed to verify that each change was authorized.	Inspected the change management review documentation to determine that all changes to the production environment related to the in-scope applications and related databases were reviewed during the specified period to verify that each change was authorized. Further, inspected supporting documentation and inquired of the Director, Unclaimed Property Solutions to determine that no issues were identified as a result of the selected monthly reviews; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted	
CC 6.8-04	Access to promote changes into the production environment related to the inscope applications and related databases is restricted to appropriate individuals based on job function. (CC 5.2-02)	Inspected the listing of users with access to promote changes into the production environment related to the in-scope applications and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of	No exceptions noted	
	9	Operations to determine that each user on the listing was appropriate to have this access.	i	
CC 6.8-05	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listings of users with Administrative access to the in-scope applications and related databases and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	

COMMON C	RITERIA CATEGORY: Criteria C	common to the Security Trust Services	Category	
CRITERIA G	ROUP 6: Common Criteria Rela	ted to Logical and Physical Access Co	ontrols	
Control Activity Description  Tests Performed by Service Auditor  Results of Testing				
CC 6.8-06	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion prevention devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listings was appropriate to have this access.	No exceptions noted	

CRITERIA G	ROUP 7: Common Criteria Rela	ted to Systems Operations	
Control Activity Description		Tests Performed by Service Auditor	Results of Testing
changes to	meet its objectives, the entity us configurations that result in the covered vulnerabilities.	ses detection and monitoring procedu introduction of new vulnerabilities, ar	res to identify (1) nd (2) susceptibilities
CC 7.1-01	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted
that are indi- its objective	cative of malicious acts, natural s; anomalies are analyzed to de	nents and the operation of those comp disasters, and errors affecting the en- termine whether they represent secur	tity's ability to meet
CC 7.2-01	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.				
CC 7.3-01	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
		and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged, tracked, reported, and resolved.	The exceptions noted	
CC 7.3-02	A monitoring solution has been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted	
CC 7.3-03	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted	
CC 7.3-04	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Response Plan to determine that when an incident related to system security was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the Director of Operations to determine that the Incident Response Plan which was inspected was in place throughout the specified period.	No exceptions noted	
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	No exceptions noted	

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 7.3-05	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted	
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted	
CC 7.3-06	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's website to determine that the Company has reporting mechanisms in place for reporting security incidents and compliance concerns, and that these mechanisms were communicated to all stakeholders via the Company's external website. Further, inquired of the Director of Operations to determine that this process was in place throughout the specified period.	No exceptions noted	

CRITERIA G	ROUP 7: Common Criteria Rela	ted to Systems Operations	
Control Activity Description		Tests Performed by Service Auditor	Results of Testing
		Inspected the incident reports and corresponding job titles related to a sample of security incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident and each management individual's job function.	No exceptions noted
CC 7.3-07	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted

CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.				
CC 7.4-01	Intrusion Prevention Systems (IPSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IPS configurations to determine that the IPS was configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, trends, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.  Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was generated, logged,	No exceptions noted	
CC 7.4-02	A monitoring solution has been implemented to detect	tracked, reported, and resolved.  Observed the monitoring system configurations to determine that a	No exceptions noted	
	potential security threats and vulnerabilities, including unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	monitoring solution had been implemented to detect potential security threats and vulnerabilities, including unauthorized access to the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.		

CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated and resolved.	No exceptions noted	
CC 7.4-03	On an annual basis, security assessments are performed by a third party and results and recommendations for improvement are reported to management for resolution. (CC 2.1-03)	Inspected the most recent security assessments and supporting documentation to determine that security assessments were performed by a third party during the specified period and results and recommendations for improvement were reported to management for resolution.	No exceptions noted	
CC 7.4-04	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Response Plan to determine that when an incident related to system security was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the Director of Operations to determine that the Incident Response Plan which was inspected was in place throughout the specified period.	No exceptions noted	
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	No exceptions noted	

CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 7.4-05	The Company has implemented a formal written Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct which collectively address the security of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on	Observed the Company's intranet to determine that the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct were posted on the Company's intranet. Further, inquired of the Director of Operations to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted	
	an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Inspected the Information Security Policy, Change Management Policy, Incident Response Policy, and Code of Conduct to determine that these policies collectively addressed the security of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the Director of Operations to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted	
CC 7.4-06	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's website to determine that the Company has reporting mechanisms in place for reporting security incidents and compliance concerns, and that these mechanisms were communicated to all stakeholders via the Company's external website. Further, inquired of the Director of Operations to determine that this process was in place throughout the specified period.	No exceptions noted	

CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
	vity Description	Inspected the incident reports and corresponding job titles related to a sample of security incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident and each management individual's job function.	Results of Testing  No exceptions noted.	
CC 7.4-07	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted	

CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.				
CC 7.5-01	A Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved.	Inspected the Disaster Recovery Plan and related testing results to determine that a Disaster Recovery Plan was documented and was tested during the specified period. Further, inspected the test results and inquired of the Director of Operations to determine that no issues were identified during the testing of the Plan; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted	
CC 7.5-02	Incremental and full backups of the in-scope applications and related databases are configured to be performed daily. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved.	Observed the backup configurations for the in-scope applications and related databases to determine that incremental and full backups of the in-scope applications and related databases were configured to be performed daily, and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted	
		Inspected the backups related to a sample of days to determine that incremental and full backups of the in-scope applications and related databases were completed for each selected day, or if the backups failed repeatedly on the selected day, an alert was sent to IT personnel and the backup failure was investigated and resolved.	No exceptions noted	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 7: Common Criteria Related to Systems Operations				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 7.5-03	When an incident related to system security is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Response Plan to determine that when an incident related to system security was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the Director of Operations to determine that the Incident Response Plan which was inspected was in place throughout the specified period.	No exceptions noted	
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	No exceptions noted	
CC 7.5-04	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's website to determine that the Company has reporting mechanisms in place for reporting security incidents and compliance concerns, and that these mechanisms were communicated to all stakeholders via the Company's external website. Further, inquired of the Director of Operations to determine that this process was in place throughout the specified period.	No exceptions noted	

CRITERIA GROUP 7: Common Criter	ia Related to Systems Operations	
Control Activity Description	Tests Performed by Service Auditor	Results of Testing
	Inspected the incident reports and corresponding job titles related to a sample of security incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident and each management individual's job function.	No exceptions noted

SOC 2® Type 2 Report – SOC for Service Organizations: Trust Services Criteria
General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim
Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA G	CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		Tests Performed by Service Auditor	Results of Testing	
CC 8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.				
CC 8.1-01	Version control software is in place to manage current versions of source code related to the in-scope applications and related databases.	Observed the version control software and related code repositories to determine that version control software was in place to manage the current versions of source code related to the in-scope applications and related databases. Further, inquired of the Director of Operations to determine that the version control software was in place throughout the specified period.	No exceptions noted	
CC 8.1-02	Each change to the in-scope applications and related databases is applied and tested within development and/or testing environments which are separate from the production environment prior to migration into the production environment. (CC 5.2-01)	Observed the production, development, and testing environments to determine that each change to the in-scope applications and related databases was applied and tested within a development and/or testing environment separate from the production environment. Further, inquired of the Senior Engineer of Servers, Storage, and Virtualization to determine that these environments were separate throughout the specified period.	No exceptions noted	
		Inspected the change requests and supporting documentation related to a sample of changes to the in-scope applications and related databases to determine that each selected change was applied and tested within a development and/or testing environment separate from the production environment prior to migration into the production environment.	No exceptions noted	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category				
CRITERIA GROUP 8: Common Criteria Related to Change Management				
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing	
CC 8.1-03	Access to promote changes into the production environment related to the inscope applications and related databases is restricted to appropriate individuals based on job function. (CC 5.2-02)	Inspected the listing of users with access to promote changes into the production environment related to the in-scope applications and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the Director of Operations to determine that each user on the listing was appropriate to have this access.	No exceptions noted	
CC 8.1-04	Each change to the in-scope applications and related databases must be approved by a member of management prior to promotion into the production environment. (CC 5.2-03)	Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope applications and related databases to determine that each selected change was approved by a member of management prior to promotion into the production environment.	No exceptions noted	
CC 8.1-05	The Company has documented a formal Change Management Policy which governs the design, implementation, modification, and management of the inscope applications and related databases. (CC 5.2-04)	Inspected the Change Management Policy to determine that the Company had documented a formal Change Management Policy which governed the design, implementation, modification, and management of the in-scope applications and the related databases. Further, inquired of the Director of Operations to determine that the Change Management Policy which was inspected was in place throughout the specified period.	No exceptions noted	

General Computer Control Environment that Supports its Unclaimed Property Claims Website with eClaim Web Service, UPS2000, Holder Reporting Website, and MissingMoney.com

CRITERIA G	CRITERIA GROUP 9: Common Criteria Related to Risk Management		
Control Activity Description		Tests Performed by Service Auditor	Results of Testing
	CC 9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC 9.1-01	A Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved. (CC 7.5-01)	Inspected the Disaster Recovery Plan and related testing results to determine that a Disaster Recovery Plan was documented and was tested during the specified period. Further, inspected the test results and inquired of the Director of Operations to determine that no issues were identified during the testing of the Plan; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted
CC 9.1-02	Incremental and full backups of the in-scope applications and related databases are configured to be performed daily. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved. (CC 7.5-02)	Observed the backup configurations for the in-scope applications and related databases to determine that incremental and full backups of the in-scope applications and related databases were configured to be performed daily, and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the Director of Operations to determine that these configurations were in place throughout the specified period.	No exceptions noted
		Inspected the backups related to a sample of days to determine that incremental and full backups of the in-scope applications and related databases were completed for each selected day, or if the backups failed repeatedly on the selected day, an alert was sent to IT personnel and the backup failure was investigated and resolved.	No exceptions noted

CRITERIA GROUP 9: Common Criteria Related to Risk Management			
		Tests Performed by Service	Danika S.T. dia
Control Acti	vity Description	Auditor	Results of Testing
CC 9.1-03	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted

CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing
CC 9.2 - The	entity assesses and manages	risks associated with vendors and bus	iness partners.
CC 9.2-01	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services) of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-04)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services) of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted

CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Acti	vity Description	Tests Performed by Service Auditor	Results of Testing
CC 9.2-02	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the Director of Operations to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted

CRITERIA GROUP 9: Common Criteria Related to Risk Management  Control Activity Description  Tests Performed by Service Auditor  Results of Testing			
			Results of Testing
CC 9.2-03	The Company has defined a standard agreement with key vendors and third parties which includes the required security commitments in accordance with the Company's security policies. These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. A member of the Legal Department is responsible for reviewing and approving of all new third-party contracts to help ensure that they	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security commitments in accordance with the Company's security policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the Director of Operations to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted
	include the applicable security practices and commitments. (CC 1.3-03)	Inspected the third-party contracts related to a sample of new third parties to determine that a member of the Legal Department reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security practices and commitments.	The Service Auditor noted that this portion of the Contro Activity did not operate during the specified period, as there were no new third-party vendors during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

CRITERIA GROUP 9: Common Criter	CRITERIA GROUP 9: Common Criteria Related to Risk Management		
Control Activity Description	Tests Performed by Service Auditor	Results of Testing	
	Inspected the query used to pull the system-generated listing of new third-party vendors during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no new third-party vendors during the specified period. Further, inquired of the Director of Operations to determine that there were no new third-party vendors during the specified period.	No exceptions noted	

### **Business Continuity Plan**

CONFIDENTIAL AND PROPRIETARY

NOT FOR PUBLIC DISCLOSURE



# Avenu Insights & Analytics, LLC Unclaimed Property Solutions

**Business Continuity Plan** 

Confirmed: 2023

# STOP!

If an <u>EVENT WHICH COULD POTENIALLY BECOME A</u>

<u>DISASTER</u> or notification of a <u>DISASTER HAS BEEN</u>

<u>DECLARED</u>, please proceed to Section 5: Event Notification Process.

# Security and Privacy Directive

In the event of a disruption of operations requiring a relocation or redirection of work and staff, all Avenu security and privacy procedures must be strictly followed.

## **Table of Contents**

#### **Contents**

1.	O	verview	8
1	.1	Definitions	9
2 S	сор	e of Plan	10
2	2.1	Business Continuity Flow	11
2	2.2	Emergency Incident Procedures	11
2	2.3	Site Strategy Summary	13
3 U	PS I	Incident Management Team	14
3	3.1	UPS Incident Management Team Role and Participants	14
4 B	usir	ness Continuity Coordinator Procedures	16
4	1.1	Business Continuity Coordinator Role and Responsibilities	16
5 E	ven	t Notification Process	17
6 C	risis	Command Center	19
6	5.1	Crisis Command Center Locations	20
7 U	PS I	ncident Management Team Procedures	20
7	7.1	Facilities / Security Team Assignment	21
7	7.2	Incident Detection & Prelim Assessment (Facilities/Security Team)	21
7	7.3	Activate Incident Management Team	22
(	Site	Management Team)	22
7	7.4	Evaluate Disaster Impact	22
(	Site	Management Team)	22
7	7.5	Activate Business Continuity Plan	23
(	Site	Management Team)	23
7	7.6	Implement Support Procedures	23
(	Inci	dent Management Team)	23
	7.	6.1 Audit	23

	7.6.2 Corp	porate Communications	24
	7.6.3 Envi	ronmental & Safety	24
	7.6.4 Facil	lities	24
	7.6.5 Retr	rieval of PHI / PII	24
	7.6.6 Food	d Services	25
	7.6.7 Infor	rmation Technology (IT)	25
	7.6.8 Offic	ces Services (Mailroom, Shipping / Receiving)	25
	7.6.9 Purc	chasing	25
	7.6.10	Vital Records Management	25
	7.6.11	Physical Security	26
	7.6.12	Transportation	26
	7.6.13	Financial Considerations	26
7	.7 Track	Incident Status and Recovery Progress	26
(1	MT Leader	·)	26
8 U	PS Operation	on Recovery Procedures	26
8	.1 Server I	Recovery	26
8	.2 Telecor	mmunications Recovery	27
8	.3 DSS Red	covery	27
8	.4 EDI Clea	earinghouse Recovery	27
8	.5 Deskto	p Personal Computer Recovery Procedures	27
8	.6 Mail Ce	enter Recovery	27
8	.7 Print Re	ecovery	28
8	.8 Financia	ial Services Recovery	28
9 Re	eturning to	Primary Site	28
9	.1 Facility	Restoration	28
9	.2 Travel F	Preparations	29
9	.3 Prepari	ing for System Cutover	29
9	.4 Prepari	ing for Recovery Site Shutdown	29
9	.5 Emerge	ency Material Replenishment	30
9	.6 Recove	ery Analysis and Final Documentation	30
10 E	Backup Prod	cedures	30
1	0.1 Networ	rk Backup Procedures	30
1	0.2 Offsite	Storage Facilities	31
11 F	lan Mainte	enance Procedures	31
1	1.1 Plan Re	evisions	31

11.2 Plan <i>A</i>	Auditing Requirement	32
11.3 Plan S	Security	32
11.4 Plan [	Distribution and Access	32
12 Testing Pr	ocedures	33
12.1 Plan T	esting	33
12.2 Testir	ng Objectives	34
13 Contact D	irectories	34
13.1 Avenu	u Contact Directory	34
13.2 Vend	or Contact Directory	35
14 Appendix	es	35
14.1 Disast	ter Declaration Procedure	35
14.2 Corpo	orate Media Policy	35
14.2.1	Applicability	35
14.2.2	Policy	36
14.2.3	Avenu Insights & Analytics, LLC' Corporate Press Contact	36
14.2.4	Procedure	36
14.2.5	Process	36
14.2.6	Accountability	36
14.3 Incide	ent and Crisis Response Center	36
14.3.1	Incident and Crisis Response	37
14.4 Temp	orary Staffing	37
14.5 AVEN	U UPS Office	37
14.5.1 D	virections to AVENU UPS Office from Logan Int'l Airport	38
14.5.2 B	est Western Adams Inn Crisis Command Center	38
14.5.3	Directions to Best Western Adams Inn from UPS Office	38
14.5.4	Venetian Garden Command Center	38
14.5.5	Directions to Venetian Garden from UPS Office	38
14.6 Disast	ter Assessment Checklist	39
14.7 Disru	ption of Service Checklist	43
14.9 Busin	ess Resumption Safety Checklist	44

#### 1. Overview

This plan was developed to address the Business Continuity strategy specific to the Avenu Insights & Analytics, LLC Unclaimed Property Solutions (UPS) business unit with personnel and key resources located at 100 Hancock Street 10th Floor Quincy, MA. It is intended to define the scope, along with describing the policies, recovery requirements and the recovery strategies necessary to ensure the UPS facility and staff can continue to fulfill its responsibilities to Avenu UPS clients.

The 100 Hancock Street Quincy, MA site is the home office of Avenu UPS, one of the largest providers unclaimed property services in the country. The Unclaimed Property Solutions Business unit consists of about 45 employees with the majority located in the Quincy office and others in remote/home offices across the United States.

UPS is a provider of fully diversified, end-to-end, business process outsourcing (BPO) and information technology (IT) solutions to commercial and government clients in the United States and Canada. Avenu has proven success delivering strategic value, business results, and operational gains to its clients. Avenu's people and culture make the difference.

Avenu UPS has provided unclaimed property reporting services for over 30 years. The Avenu UPS Senior Management team is comprised of experienced unclaimed property professionals and technical staff to support its operations with significant tenure and who have received training in their respective areas of expertise. Avenu UPS products and services are based on propriety processes and systems.

Avenu UPS performs core unclaimed property administration services that consist of the following:

- Unclaimed Property Management Systems
- Claims Processing
- Holder Reports Processing
- Securities Custody
- Database Management
- Annual Compliance Services

This Plan covers the operations for the Avenu UPS business unit.

#### 1.1 Definitions

Table 0-1 **D**efinitions

Te <b>r</b> m/Ac <b>r</b> onym	Explanation/Expansion
ВСР	Business Continuity Plan
UPS	Unclaimed Property Solutions
DRP	Disaster Recovery Plan
ICRC	Incident and Crisis Response Center
IMT	Incident Management Team
PHI	Personal Health Information
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective

#### 2 Scope of Plan

#### This plan is intended to:

- Provide an effective method of communication during a crisis situation.
- Ensure the safety and welfare of employees, contractors and partners of Avenu UPS in the event of an emergency.
- Eliminate, or at least minimize the risk of service disruptions to critical business functions caused by natural, technological or human error problems.
- Maintain the ability to quickly resume critical operations in the event of an emergency through the
  use of predetermined procedures and checklists that assure rapid and accurate recovery.
- Provide the training materials and basis for rapid recovery of processes in the event of service disruptions whether caused by nature, intentional acts, or unintentional human error.
- Identify vital information and educate the staff in the recovery of processes needed for long-term Business Continuity.

#### The basic assumptions for this plan are:

- That sufficient number of staff will be available to carry out the required recovery steps;
- That short term/limited outages will be addressed and resolved using documented local operating procedures;
- That a "worst case" event or circumstance that renders the facility totally unusable for an undetermined amount of time will be addressed and resolved using these documented procedures,
- For incidents less than the "worst case" scenario, Avenu UPS will activate only those parts of the plan
  applicable to the current situation.

In the event of an incident that incapacitates Avenu UPS personnel's ability to maintain critical business processes, this plan clearly identifies the necessary steps to restore full production for the UPS facility as quickly as possible. Through proper training and testing, Site Management and Avenu UPS staff will understand what needs to be done to restore full production capabilities within the contractual service level agreements.

#### 2.1 Business Continuity Flow

The process of Business Continuity is to predefine a set of procedures that may be followed during a highly disruptive event. The objective is to provide the information needed to make the decision-making processes as efficient as possible during an incident and to give guidance to the incident team leads in executing comprehensive, documented procedures so that recovery of the production environment is within the predefined recovery time objective.

#### 2.2 Emergency Incident Procedures

Emergency incident procedures refer to the predetermined actions, which are performed immediately following an emergency incident. These procedures include coordination of the specific response and recovery actions. Emergency incidents include, but not limited to: fire, medical emergency and/or illness, bomb threat, tornado, power outage, suspicious mail, violence in the workplace, and cyber-attacks. The goals of emergency incident procedures are to reduce injuries, prevent loss of life, and avoid or minimize damage to the organization's reputation or the ability to operate.

The Emergency Action Plan (EAP) contains quick reference information and checklist procedures on:

- How to report an emergency
- Who will assist you in an emergency
- What to do in case of an emergency

Avenu Insights & Analytics, LLC maintains these procedures and policies to ensure the safety and security of its employees, contractors, and business partners. The *Employee Handbook* outlines many of the policies and procedures that affect employees are located on Avenu Insights & Analytics, LLC intranet site, CentralAve and others are maintained by Avenue's Director of Security.

The following diagram summarizes a typical emergency incident procedure notification flow and initial actions.

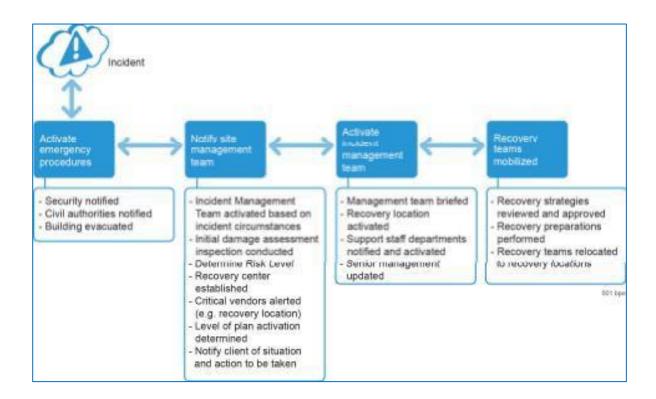


Figure 2-2 Typical Emergency Incident Procedure Notification Flow and Initial Actions

#### 2.3 Site Strategy Summary

This plan will provide established procedures for management in the event of a disaster, emergency or technical interruption to daily production operations. In the event of a disruption to production operations, this plan will assist in re-establishing technical, telephonic, and other critical operations for continued business, while meeting contractual obligations.

The Recovery Time Objective (RTO) is defined as the maximum number of hours that it will take to restore use of critical business functions. In the case of a disaster, the disaster recovery plan will be implemented to recover the production site to achieve the specified Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) within the contracted recovery times.

- Install Licensed Internal Code (Avenu IT)
- Install Operating Systems (Avenu IT)
- End Systems to Restricted State (Avenu UT)
- Restore User Profiles (Avenu IT)
- Restore Configuration Objectives (Avenu IT)
- Restore Libraries \*NONSYS (Avenu IT)
- Restore Documents and Folders (Avenu IT)
- Restore Directories (Avenu IT)
- Verify All Production Data Restored (Avenu UPS)
- Restore Any Production Objects not Restored (Avenu IT)
- Restore Private Authorities (Avenu IT)
- Re-Configure Communications Resource (Avenu IT and UPS)
- Perform an Unattended IPL (Avenu IT)
- Verify System Integrity (Avenu IT and UPS)
- Turnover to Client for Application Testing (Avenu UPS)
- Add Temporary Application License Keys (Avenu IT)
- Application Verification (Avenu UPS)
- User Application Testing Quincy (Avenu UPS)
- User Application Testing Client (Avenu UPS)
- Tentative Testing Completion Wrap up (Avenu UPS)
- System Turnover (Avenu IT)

Should the staff be unable to perform their normal daily operational duties because of an emergency situation or disaster, Site Management will make the determination to hire clerical and programming personnel from a temporary staffing and/or technical services agency or shift work to other Avenu Insights & Analytics, LLC locations.

In the event that production operations relocates to another facility, employees and/or temporary personnel will be responsible for transporting themselves to the alternate site or working remotely.

#### 3 UPS Incident Management Team

When normal business operations are disrupted by any event, there are three things that have to be accomplished immediately:

- Ensure the safety and welfare of employees, contractors and partners of Avenu Insights & Analytics, LLC UPS in the event of an emergency.
- Execute the notification process to alert Site Management and to notify Avenu management.
- Making use of the resources at the local facility that has been affected, assess the damage quickly and determine if the site may be restored to full production status within the established recovery time objective.

Avenu Insights & Analytics, LLC UPS has established an Incident Management Team (IMT) for the UPS location at 100 Hancock Street, Quincy, MA. This team is responsible for investigating and assessing the incident, conferring with other support areas to perform an initial evaluation and damage assessment, planning, coordinating, and executing the recovery activities. Based upon the Incident Management Team assessment, plan activation procedures are either initiated or terminated. While the composition of the team varies according to the site's needs, it generally includes Site Management, Senior Technical and Operational Managers from the departments that have been directly affected by the incident, and members of the Avenu Insights & Analytics, LLC UPS Service Continuity Delivery Team. Each member of the Incident Management Team is provided with a copy of the Avenu UPS Business Continuity plan.

#### 3.1 UPS Incident Management Team Role and Participants

The UPS Incident Management Team is responsible for managing internal and external communications, directing response and recovery activities, monitoring the recovery progress, and providing or reallocating recovery resources. The IMT will interface with appropriate civil authorities as dictated by the incident.

The UPS IMT leader's responsibilities include contacting all members of the UPS IMT after being notified of the situation, determine with the team's input if a disaster should be declared, and communicating the situation with the Avenu Insights & Analytics, LLC Service Continuity Delivery Team and Avenu UPS Executive Management. Avenu UPS Executive Managers must be consulted prior to any decision of disaster declaration. Avenu Insights & Analytics. LLC Corporate Management has the ultimate authority to declare a disaster.

Other UPS IMT members are given the responsibility to communicate to the essential incident team leads that a disaster has been declared and the directives from the IMT, document the recovery progress, work with HR on resolving personnel issues and/or concerns, address financial and compensation issues, document recovery costs, coordinate internal communications among the incident recovery teams, and coordinate media and external communications with clients and the Avenu Insights & Analytics, LLC Communications & Public Relations Manager.

Table 3-1 Service Continuity Delivery Team

Position	Name
Avenu, CTO	Greg Graham
Avenu, Vice President, Technology	Johan Milbrink
Avenu, Director, Network Operations/IT Infrastructure	Mark Terrill
Avenu, Director of Security	Allarick Greer
Avenu, Vice President, Software Engineering	Joseph Atwell
Avenu, Software Engineer II	Jeremy Rosine

Table 3-2 Site **M**anagement Team

Avenu Insights & Analytics, LLC	Name
Managing Director	David Lemoine
Director	Mark Capprini
Director	Deborah Arnold

Each member of the IMT should have a designated backup/alternate that can carry on in the event of illness (during or before the emergency) or unavailability. This gives members of the team a chance to rest if recovery activities are continuous over an extended period of time. All appropriate contact numbers must be documented for each alternate.

It should be noted that all Avenu Insights & Analytics, LLC UPS employees and contractors, including members of the Incident Management Team, must be subjected to pre-employment background checks. This is a standard part of the Avenu Insights & Analytics, LLC hiring process and should not present a problem in a recovery situation.

In determining how to proceed in a recovery situation, the Incident Management Team must consider the Recovery Time Objective for business functionality from the time that normal operations were interrupted. The team must also make every effort to adhere to contracted Service Level Agreements (SLAs) and should take whatever action is necessary and possible to ensure that partners and contractors do the same.

The IMT Leader will consult with Avenu Executive Management and the client(s) on whether a disaster should be declared and describe the recovery effort to resume production operations.

- If the site can be restored, execute the predefined steps necessary to resume production operations.
- If the assessment determines that relocation is necessary, notify Avenu Insights & Analytics, LLC Service Continuity Delivery Team and Avenu Executive Management that production operations must relocate to the recovery facility or if staff will work fully remote. While production operations are being restored at the recovery facility, assessment and restoration of the damaged facility continues. When the primary facility is restored, production operations will relocate back to the primary facility to continue operations.
- If the incident is not on the physical location in Quincy but at one of the Data Centers or a cyber security incident the Avenu Insights & Analytics, LLC Service Continuity Delivery Team and Avenu Executive Management will identify actions items and recovery plan. The incident management team will communication with UPS staff and clients.

If the incident is not deemed a disaster Avenu will follow the Incident Response Policy

Throughout this process, it is essential that internal Avenu Insights & Analytics, LLC UPS communications occur freely between the recovering damaged site, the recovery backup site, the Incident Management Team, and the Avenu Insights & Analytics, LLC Service Continuity Delivery Team. During the restoration process, it is imperative that internal status updates be provided at predefined intervals. See Section 13.1: Avenu Contact **Directory** for office phone numbers and e-mail addresses.

#### **4 Business Continuity Coordinator Procedures**

#### 4.1 Business Continuity Coordinator Role and Responsibilities

The roles and responsibilities of the Business Continuity Coordinator are as follows:

- Assists in defining business continuity requirements for critical business functions.
- Develops and maintains Emergency Notification list.
- Maintains Business Continuity plans according to maintenance schedule.
- Coordinates Business Continuity plan testing.
- Coordinates all phases of the recovery in the event of a disruption.
- Provides input to Disaster Declaration decisions with Local Management and Avenu Insights & Analytics, LLC Service Continuity Delivery Team.

- Assists in the identification and provision of needed resources during the recovery process.
- Serves as the focal point for communications between the recovery teams and the Incident Management Team (IMT).
- Makes recommendations and assists the IMT in all aspects of the recovery process.
- Contacts all Incident Team Leads and instructs them to activate their team's recovery plan at the direction of the IMT.
- Updates Business Continuity plan(s) to reflect lessons learned during the recovery process.

The Avenu Insights & Analytics, LLC Service Continuity Delivery Team is available to assist the Business Continuity Coordinator in any testing, recovery or coordination activity. While it is preferred that a local coordinator be assigned these tasks, the Avenu Insights & Analytics, LLC Service Continuity Delivery Team can assume the role of Business Continuity Coordinator if necessary.

NOTE: Refer to Section 13.1: Avenu Contact Directory for office phone numbers and e-mail addresses.

Table 4-1 Business Continuity Coordinators

Avenu Insights & Analytics, LLC Position	Name	Primary/Alternate
VP, Unclaimed Property Solutions	David Lemoine	Primary
Director, Claims, Calls, Holders Reports	Mark Capprini	Alternate

#### **5 Event Notification Process**

One of the most critical elements of any Business Continuity Plan is the notification process for notifying all involved parties of any incident. Implementation of predefined contact lists (i.e. call-down tree or notification software product) has proven to be the most effective way of providing information to all parties that need to be involved in the recovery process. This predefined notification process will allow Management to deal with immediate issues and to notify other affected Avenu Insights & Analytics, LLC UPS organization and clients.

Depending upon the nature and time of day of the incident, notification of a potentially disruptive incident may come from several different sources. Initial response notification is dictated by company emergency response procedures and standard operating practices.

The safety and well-being of personnel is top priority. If necessary, evacuate personnel according to local evacuation procedures and make sure that all personnel are accounted for and safe. If injuries have occurred, call 911 immediately for assistance and follow the facility's standard procedure for on-the-job injuries. Depending on the type of disruption, local authorities may have initial responsibility for the situation. Local Fire and Police Authorities will determine when local management can resume responsibility of the situation.

When a situation requires activation of any part of this plan, the Site Management Team (see Table 3-2) will immediately notify the Avenu Insights & Analytics, LLC Service Continuity Delivery Team (See Table 3-1) of the circumstances that may require execution of the Business Continuity plan, or the circumstances that may cause disruption of services. When a situation initiates this plan, the IMT Leader or IMT Alternate Leader will establish the location of a Crisis Command Center. See Section 6: Crisis Command Center for information on determining the location of the Crisis Command Center and Section 6.1: Crisis Command Center Locations.

Upon declaration of a disaster at any operational location, the Account Manager will be delegated to notify the client of the disaster declaration. The Account Manager will be the client's primary link with Avenu Insights & Analytics, LLC throughout the recovery process. During the emergency or situation that would initiate the execution of a disaster recovery plan, it is imperative that detailed status updates be provided at predefined intervals with the client. See Section 13.1: Avenu Contact **Directory** for office phone numbers and e-mail addresses.

After the declaration of a disaster at a project operational location, the Account Manager (or their alternate) will delegate notifying Avenu Insights & Analytics, LLC's business partners about the disaster declaration and the recovery efforts to resume productions operations to the appropriate Avenu UPS Managers or Team Leads. It is the client's responsibility to notify its business partners (those other than Avenu Insights & Analytics, LLC business partners) about the disaster declaration and the recovery efforts.

In the event of a situation where an employee is unable to contact their immediate supervisor or manager with their immediate status and location, the employee should contact the Avenu Insights & Analytics, LLC Human Resource Department.

While the Avenu Insights & Analytics, LLC Service Continuity Delivery Team will provide assistance as needed throughout any emergency, Site Management must make the initial decisions regarding notification and declarations due to the potential fees, fines and/or penalties associated with the contractual requirements for our clients.

In the case of an event that may come to the attention of the general public, such as the relocation of staff to a backup site or personnel casualties, it is imperative to contact the Avenu Insights & Analytics, LLC Communications and Public Relations Manager. Any individual representing a press/media organization is to be immediately referred to the Avenu Insights & Analytics, LLC Communications and Public Relations Manager. No other employee of Avenu Insights & Analytics, LLC or its partners should make any comment to the media regarding the incident. All press releases or information provided to the media must be generated by this organization. Due to the interdependency of operations at all Avenu Business Services, LLC locations, news of a disruption in operations at an Avenu Insights & Analytics, LLC facility will be communicated to other locations by this organization. The Avenu Insights & Analytics, LLC Communications and Public Relations manager will coordinate with the appropriate client Public Relations interfaces prior to releasing any media information. See the below table for contact information for Avenu Insights & Analytics, LLC Public Relations and/or Media Management organizations. See Section 14.2: Corporate Media Policy for the procedures for communicating to the press/media.

Table 5-1 Avenu Insights & Analytics, LLC Communications & Public Relations

Avenu Insights & Analytics, LLC Position	Name
Avenu Insights & Analytics, LLC Corporate Marketing VP, Corporate Communications	Brennan Middleton

During any event requiring notification procedures, Avenu Insights & Analytics, LLC Human Resources must be made aware of the circumstances. Human Resources personnel play a vital role during recovery operations. Please see table below for contact information for Avenu Insights & Analytics, LLC Corporate Human Resources Management.

Table 5-2 Avenu Insights & Analytics, LLC Human Resources

Avenu Insights & Analytics, LLC Position	Name
AVENU Vice President, Human Resources	April Bullion

#### **6 Crisis Command Center**

In the event of a situation where the IMT needs to assess and discuss the incident with other support teams, the IMT will establish a Crisis Command Center. The Crisis Command Center will provide a facility for the IMT to monitor and control all recovery activities, regardless of whether they occur at the primary facility or the designated backup location.

Examples of Crisis Command Center locations are available onsite conference rooms, local hotel conference rooms, another Avenu Insights & Analytics, LLC facility, or the backup recovery site. Section 6.1: Crisis Command Center Locations identifies the Crisis Command Center locations for Avenu UPS.

Depending on the facility damage assessment, an additional Crisis Command Center may need to be established near the primary facility as well as at the backup recovery site. This will allow IMT members to oversee production recovery operations as well as primary facility restoration.

Consideration of the location of a Crisis Command Center should be given to the availability of telephones, fax machines, public security access, white boards or flip charts and duration. IMT members with company laptops should bring them to the Crisis Command Center so that e-mail communications with other support teams and Avenu Insights & Analytics, LLC Executive Management can be maintained. The necessary office supplies can be purchased at a local office supply store.

#### **6.1 Crisis Command Center Locations**

The UPS Management Team (see Table 3-2) will be notified after the discovery of a major problem. The UPS Management Team will assemble in the following locations respectively one hour after being notified. Depending on the damage assessment of the UPS facility, the UPS Management Team will designate one of the following locations as the "Crisis Command Center".

- If there is an incident at the UPS facility, then the UPS Management team will direct the Facilities team
  to assess the damage. The UPS Management team will contact all IMT members to report to an
  available conference room for a damage assessment report. Based on the damage assessment
  report, initiation of the plan will be determined.
- If the damage assessment indicates that the UPS facility should be declared off-limits, then the UPS Management team will contact all IMT members to report to Best Western Adams Inn.

The UPS IMT will designate this location as the "Command Center" until the damage assessment has been reviewed. Based on the damage assessment report, initiation of the plan will be determined. Refer to Section 14.5: Best Western Adams Inn Crisis Command Center.

• If the damage assessment indicates the necessity to relocate all production operations to another facility, then the UPS Management team will contact the Service Continuity Delivery Team to inform them that production operations is relocating. The UPS Management team will contact all IMT members to report to the above Command Center location for instructions on relocating production operations to another facility. The IMT leader will instruct the other IMT members to communicate to their staff information about the relocation. The UPS IMT will assemble in the alternate UPS facility and will designate a conference room as the "Command Center".

#### 7 UPS Incident Management Team Procedures

This section provides a comprehensive checklist for the coordination of Business Continuity activities to be followed in the event of a disruption in operations or in the event of an emergency situation. This checklist is intended to provide a beginning process for notification and for evaluating the effects of the emergency and the steps that need to be followed to initiate recovery. This checklist assumes that an incident has occurred and the steps to be followed are identified to help assist in the discovery, notifications, and remediation processes. These steps are intended to provide a common approach to detect what has happened, and to begin the disaster recovery processes.

#### 7.1 Facilities / Security Team Assignment

If a situation has developed that may require the declaration of an emergency situation the Business Continuity Coordinator or Account Manager will be immediately contacted to carry out initial site assessment. If the preliminary reaction is that an emergency situation has occurred or needs further investigation, the Business Continuity Coordinator and/or the Account Manager will name a Facilities/Security Team. If the Business Continuity Coordinator or Account Manager is unavailable, contact the Avenu Insights & Analytics, LLC Service Continuity Delivery Team (see Table 3-1) to assist in designating a Facilities/Security Team. This team will normally be comprised of a small group of 3-5 key individuals that may include the Business Continuity Coordinator, facility, technical or key staff members.

#### 7.2 Incident Detection & Prelim Assessment (Facilities/Security Team)

#### Facilities related event:

Follow Company Emergency Response Procedures (See Section 2.2: Emergency Incident Procedures).

Find out if the entire building has been evacuated or if the problem seems to be limited to a small area.

Ask about the atmosphere: has panic broken out, are people calmly addressing the problem, or are people unaware of the problem?

Conduct a preliminary physical damage assessment, if it can be done safely. No recovery activities should be undertaken if personnel are placed in danger. After notification that a problem has occurred, a decision is needed as to whether the situation might actually be a disaster or not. Not all emergency conditions result in a disaster. In this initial assessment phase, minimal information will be presented. Most likely, the only information available will be the information given by the individual who discovered the problem and notified management.

If access to the facility is allowed, conduct a physical site assessment. If local authorities (police, fire, rescue, city officials) have deemed the building unsafe or prohibit site access, gather as much information as possible from what resources are available. This could be witnesses, local authorities, or property management. Gather all details about of the situation noting the source and credibility. Use the Disaster Assessment Checklist as a tool to document details. (See Section 14.6: **D**isaster Assessment Checklist).

While conducting a physical inspection, be aware of water, exposed electric (hanging wires), smoke, residual fire or other potential hazardous conditions.

Write as much detail as possible. If camera is available, take as many photos that will assist in assessing the damage. Videotaping or voice recording may also be useful.

Reassemble the Facility/Security team after the site assessment to perform a preliminary assessment.

#### Datacenter or Cyber related event:

The Service Continuity Delivery Team members as required will evaluate the incident to extend of the issue or exposure. If the event impacts the data center or hosting environments the Service Continuity Delivery Team will review with Avenu UPS, Vendors and executive management to determine if a disaster is to be declared and implement the Disaster Recovery Plan and execution of moving to backup locations. If the even is a cyber incident the Service Continuity Delivery Team will review with Avenu UPS, Vendors and executive management to determine scope and impact of the incident to determine appropriate plan of actions and communcication to staff,

vendors and client(s) impacted. If necessary, proceed to next step, Section 7.3: Activate Incident Management Team, and begin to notify members of the Site Management Team.

#### 7.3 Activate Incident Management Team

#### (Site Management Team):

The Site Management Team will determine if the Incident Management Team should be activated and if necessary:

Notify Incident Management Team Members.

- Information may include conference bridge information, meeting / Crisis Center location, situation description, brief damage assessment and initial recovery recommendations.
   Request those unable to meet at the Crisis Command Center participate via a conference call with scheduled time.
- If possible, send an email with necessary information to IMT members.

Activate the Crisis Command Center (See Section 6.1: Crisis Command Center Locations).

#### 7.4 Evaluate Disaster Impact

#### (Site Management Team):

Incident Management Team Members will meet to review and assess available information to determine the course of action.

Have the Facility Assessment team or IMT Leader review the situation and the preliminary physical assessment of the facility with the IMT members. If digital photos are available, distribute the photos to the team for further clarification of the situation.

Determine if the severity of the impact requires implementation of the business continuity plan

Determine recovery objectives including:

- Priorities. Recognition of functions that may be able to be continued at the facility immediately or within a 1 day effort will be noted.
- Recovery strategies considering the contractual Service Level Agreements (SLA) and Recovery Time Objective (RTO) obligations.
- Action plans. Review possible situations that may best utilize available resources.
- Decision as to alerting of additional members of Site Management and Incident Team Leads.

#### 7.5 Activate Business Continuity Plan

#### (Site Management Team):

Notify Incident Team Leads and members using either a direct call to each member. This will be assigned by Business Continuity Coordinator and can be conducted by IMT.

Brief Incident Team Leads and alternates regarding:

- Priorities and initial action plan as decided in Section 7.4, Evaluate Disaster Impact.
- Delegate Assignments to members of IMT. These may include initial contact to staff, recording of emergency phone messages, evaluation of recoverable assets, implementation of procedures regarding workflow, etc.
- Reporting; designate which team members are to report on recovery, staff availability, coordination of site availability, etc.
- Communications procedures; make decisions on how to handle communications between team members. Designate central contact phone numbers (i.e. IMT cell phones, site phone number, etc) or alternate forms of communications (i.e. internet, phone relay, local courier, and fax).

#### 7.6 Implement Support Procedures

#### (Incident Management Team):

As directed by the Incident Management Team Leader, Incident Management Team support personnel will provide recovery support to all affected business units. The IMT may take initial direction from management that are on site as to recovery efforts, alternate site planning, equipment availability, staffing.

#### 7.6.1 Audit

Consult/provide advice on changes to standard operating procedures to be implemented during the recovery effort

Ensure that the following policies and standards are maintained during the recovery effort:

- Financial security and control policies
- Anti-fraud policies
- Information security standards

Provide reports and recommendations to the IMT as required

Provide additional resources to other business units during the recovery effort as needed

#### 7.6.2 Corporate Communications

Instruct employees to direct all media inquiries to Corporate Communications (See Section 14.2: Corporate Media Policy).

#### 7.6.3 Environmental & Safety

As directed by the Incident Management Team Leader, Incident Management Team support personnel will provide recovery support to all affected business units. If any units (i.e. Production Support, Review & Determination) are remaining in the site, as many precautions as possible will be followed to protect staff from injury, dangers or health issues.

- Ensure the health and safety of employees
- Ensure that response activities to address fire, spills and/or medical emergencies are performed in accordance with regulatory guidelines
- Notify regulatory agencies of the incident as required
- Enlist the assistance of vendors and agencies to assist in support activities as appropriate.

#### 7.6.4 Facilities

Contact Avenu UPS Corporate Facilities. This should be done after the preliminary assessment and usability of site. Refer to Section 13.1: Avenu Contact **D**irectory for office phone numbers and e-mail addresses

- Conduct detailed damage assessment. Refer to Section 14.6: Disaster Assessment Checklist
- Conduct salvage and restoration activities. Before any salvage operations begin, consult with Corporate
- Facilities regarding insurance requirements and information.
- Acquire replacement office space if necessary
- Notify tenants of the incident and provide periodic updates regarding the condition of their affected office space

#### 7.6.5 Retrieval of PHI / PII

Secure all documents containing Personally Identifiable Information (PII). Determine the scope of the records involved and retrieve as much information as possible. This would include retrieval of laptops or desktops that contain PHI/PII documentation. Only Avenu Insights & Analytics, LLC authorized personnel would be allowed to retrieve the PII documentation. The primary step would be to retrieve all or as much as possible, of the documentation and move to a secure location. The Site's Privacy Coordinator is required to submit a Privacy Incident Report documenting the situation.

The Corporate Security Privacy Officer should be alerted if there is a mass exposure of PII or a situation where consultation is required. The Site's Privacy Coordinator is required to submit a Privacy Incident Report documenting the situation.

Because of the potential of PII document exposure, only authorized personnel (i.e. Avenu Insights & Analytics, LLC staff or those with pre-established authorization) should be able to handle documents with PII in the site. Obviously emergency workers (police, fire, and rescue) have precedence in order to re- establish a safe environment for staff; however any assistance by these individuals in recovery or securing of documents or PII related items should be discouraged.

#### 7.6.6 Food Services

During salvage and recovery operations, meal(s) or food service may be provided to personnel at the damaged and/or alternate operation locations. This decision will be at the discretion of the IMT Leader (i.e. Account Manager) and Avenu UPS Executive Management. Any expenditure would be charges using a credit card with as much detail as possible regarding staff or personnel involved.

#### 7.6.7 Information Technology (IT)

- Conduct and review computer system, servers, applications, databases and telecommunications damage assessment
- Activate alternate operating locations (for system recovery)
- Recover computer systems and network environment(s)
- Acquire and install replacement computer equipment
- Re-establish data network connections to external resources (remote locations, vendors)
- Implement all telephone response plans (re-routing critical telephone numbers)
- Ensure all system security devices and procedures are in place

#### 7.6.8 Offices Services (Mailroom, Shipping / Receiving)

- Re-establish mail and shipping services
- · Re-direct all mail and parcel receipts to alternate operating locations

#### 7.6.9 Purchasing

- Manage all incident related purchasing.
- Acquire office supplies, forms and equipment for affected business units.
- Implement any necessary short-term financial tracking controls, using designated cost centers.
- Implement any necessary short-term financial tracking controls, using designated cost centers.
- Coordinate all financial transactions with the IMT Leaders, Business Continuity Coordinator, Avenu UPS management and Avenu Insights & Analytics, LLC CFO.

#### 7.6.10 Vital Records Management

- Coordinate with business units in retrieving all offsite documentation and media.
- Because of the potential of PII document exposure, only authorized personnel (i.e. Avenu UPS staff or those with pre-established authorization) should be allowed into the site. Obviously emergency workers (police, fire, and rescue) have precedence in order to re- establish a safe environment for staff; however any assistance by these individuals in recovery or securing of documents or PHI/PII related items should be discouraged.
- Coordinate documentation retrieval and document restoration.

#### 7.6.11 Physical Security

- Coordinate onsite security for affected facilities and all alternate operating locations
- Control access to affected facilities
- Monitor equipment and records being removed from facilities

#### 7.6.12 Transportation

- Provide local transportation during response and recovery activities as required.
- Provide travel arrangements and accommodations for employees traveling to remote recovery locations.

#### 7.6.13 Financial Considerations

The Account Manager, Avenu UPS Management and Avenu Insights & Analytics, LLC CFO will review any expenses that may start occurring during the emergency recovery and establishment (or reestablishment) of the site. It is advisable to utilize vendors who have established Avenu Insights & Analytics, LLC accounts in order to minimize out of pocket or credit card transactions.

If travel arrangements and accommodations are required for employees traveling to remote recovery locations, follow company travel policy to secure reservations. The Account Manager, Financial Analyst, and/or the Senior Regional VP would be responsible for the financial arrangements of such transactions.

## 7.7 Track Incident Status and Recovery Progress (IMT Leader):

- Conduct periodic debriefing sessions with recovery teams to monitor progress and determine problem areas
- Reallocate and/or provide resources
- The UPS IMT Leader prepares a status report for Avenu UPS Executive Management. Avenu UPS
   Executive Management should have a detailed status report within 3-4 hours from when the UPS IMT
   Leader was first contacted.

#### **8 UPS Operations Recovery Procedures**

#### 8.1 Server Recovery

In the event of a server outage, an evaluation and determination of the usability of all data processing hardware/VMs will be performed. This evaluation should involve the vendor representative. Upon completion of the evaluation and the estimated timeframe for repair and/or replacement hardware/VMs, recommendations will be presented to the IMT as to what steps should be performed to resume production operations.

If relocation to another facility is required and/or new server hardware, VMs or other equipment is required, the Avenu UPS team will work with Avenu Insights & Analytics, LLC management and vendors move to the backup data center location and environment in the event of any Disaster Recovery plan being executed.

#### 8.2 Telecommunications Recovery

Telecommunications between Avenu Insights & Analytics, LLC UPS locations is established using Mitel MiCloud Connect Service. Office desk phones can be directed to mobile phones if required and all voice messages are sent to staff by email to ensure calls are captured at all times. Softphones can be used if needed.

#### 8.3 DSS Recovery

The UPS facility does not access or utilize any Data Warehouse or Decision Support System (DSS) servers.

#### 8.4 EDI Clearinghouse Recovery

The UPS facility does not access the Electronic Data Interchange servers.

#### 8.5 Desktop Personal Computer Recovery Procedures

In the event of a temporary or long-term outage requiring relocation of production operations to facility, Infrastructure Services Group will purchase the necessary replacement desktops and/or laptops for recovery. Replacement equipment will be charged back to the appropriate Cost Center.

#### 8.6 Mail Center Recovery

In the event of a situation that requires the relocation of the Mail Center operations, the Mail Operations Lead will notify the local U.S. Postal office to reroute all incoming mail to the alternate recovery location. Avenu Insights & Analytics, LLC employees will continue to pick up the mail at the Post Office until the Post Office is able to forward the mail to the recovery location. The United States Postal Service (USPS) has confirmed that they are able to reroute mail within 72 to 96 hours of notification.

Contact Avenu Insights & Analytics, LLC' mail-in house vendor for production relocations and mailing of all internal correspondence.

In the case of a disaster resulting in the scattering of documents containing Personal Health Information (PHI) or Personally Identifiable Information (PII), the UPS staff should take all reasonable steps to determine the scope of the records involved and retrieve that information when possible. Remember that the safety of staff members is always the first priority.

#### 8.7 Print Recovery

In the event of relocating production operations to another facility, smaller priority reports will be rerouted to another printer at the recovery location.

The AS400 hosted in Dallas-Fort Worth, Texas has a printer associated with the Quincy LPAR that is located in the Quincy office. In the event that operations are relocated, a separate printer will need to be procured and the output re-routed so that it prints at the alternate printer. For security purposes, the alternate printer will be located within a secured room.

#### 8.8 Financial Services Recovery

The site facility does not perform any financial services for their client.

#### 9 Returning to Primary Site

The following steps should be considered when returning production to the primary site. Perform only the tasks or activities that are required and appropriate.

#### 9.1 Facility Restoration

- Work with Corporate Facilities in determining if a new facility is required or if the facility will be repaired.
- Check with local code officials to identify building code requirements for repairs, new construction or demolition.
- · Verify the health, safety and security of the facility.
- Verify the operational state of key suppliers and subcontractors and develop procedures for quickly procuring critical hardware, software, and supplies.
- Determine what equipment & software needs to be ordered.

- Advise employees of any health, security, and security concerns within the facility. Screen
  employees for risk factors as heart conditions, asthma, comprised immune systems and allergies to
  mold and dust.
- Provide appropriate protective equipment to personnel (gloves, disinfectant wipes, & masks).
- Prior to resuming production in the facility, conduct a thorough facility assessment. Refer to the American Society of Safety Engineer News (ASSE) business resumption safety checklist in Section 14. 9.

## 9.2 Travel Preparations

- Provide the Local Business Continuity Coordinator with a list of personnel that relocated.
- Request the Site Office Administrator make the appropriate travel arrangements.
  - o Ensure meals and lodging are considered, if appropriate.
  - If driving to the recovery site is appropriate, team members will be responsible for providing their own transportation.
  - Monitor team travel to ensure team's safe arrival.

## 9.3 Preparing for System Cutover

- Prioritize the order of resuming operations and identifying any obstacles or risks.
- Determine whether system relocation will be a phased or cut-over approach.
- If a phased approach, determine which phase every recovery team member will be assigned.
- Ensure successful cut-over of re-routed telephone systems.
- Ensure successful cut-over of all network communication systems.
- Ensure successful system / database / file synchronization and cut-over of computer systems.
- Ensure successful user testing and cut-over of all critical business function support applications.

## 9.4 Preparing for Recovery Site Shutdown

- Once production business functions are confirmed operational at the primary site, ensure that all data is erased on the recovery site's system.
- Request travel arrangements for remaining Recovery Team members.
- Ensure proper storage or return of Recovery Site equipment.
- Inventory and replenish expended site-stocked material (if applicable).
- Ensure utility shutdown (if applicable and as appropriate).
- Ensure all keys (if any) are accounted for and returned to the appropriate individual or location.
- Ensure site security upon departure.
- Monitor team travel to ensure team's safe arrival.

## 9.5 Emergency Material Replenishment

- Inventory, purchase and restock all supplies and documentation used during relocation.
- Ensure the return of the replenished team box(es) to offsite storage by the Business Continuity Coordinator.

## 9.6 Recovery Analysis and Final Documentation

- IMT will have a final meeting after full recovery and restoration of full service at principal site.
- Ensure that all documentation about the incident, all procedure checklists and forms are collected and assembled into a document that may be required for review.

## 10 Backup Procedures

Systems Administrators or IT Departments must establish and implement appropriate backup procedures and a backup/recovery plan for each local Avenu Services leased or owned data center. Systems Administrators or IT Departments must afford backup files the same degree of security and protection as the original data and ensure archive storage media is appropriate for expected longevity and format.

Systems Administrators or IT Departments will establish, implement, and test restore procedures in accordance with contractual obligations and document the results of all testing

Avenu UPS meets all backup requirements outline by each client contract based on each product and service supported.

## **10.1 Network Backup Procedures**

Avenu performs daily full backups to an Azure Storage account with Georedundant Storage, where a copy is maintained in three (3) different Azure regions across the United States.

Backups are kept for thirty (30) days by default but are adjusted based on client contract requirements.

## **10.2 Offsite Storage Facilities**

Avenu utilizes Azure storage

## 11 Plan Maintenance Procedures

Avenu Insights & Analytics, LLC UPS owns and maintains the Business Continuity Plan.

#### 11.1 Plan Revisions

Avenu Insights & Analytics, LLC. UPS Business Continuity plans and supporting documents are to be reviewed regularly by each Incident Team leader to ensure that the documents reflect current practices, procedures, etc. Any changes to the Business Continuity plan should be submitted to the Local Business Continuity Coordinator. The Local Business Continuity Coordinator will submit the changes to the Avenu Insights & Analytics, LLC Service Continuity Delivery Team. The Avenu Insights & Analytics, LLC Service Continuity Delivery Team will update the relevant section(s) of the Business Continuity plan and redistribute it using the plan distribution guidelines.

Plan revisions resulting from changes to hardware configurations, networks, production processing etc. should be submitted as soon as possible for incorporation into the Business Continuity plan. This includes:

- Change in system or application architectures.
- Hardware, VM or environmental changes.
- Major changes in operating system(s) or utility software programs
- Major changes in the design of a production database.
- Major changes in communication, systems network design, modems, adapters, etc. (e.g., addition of a communications circuit to a new location, an upgrade in network bandwidth).
- Changes in off-site storage facilities and methods of cycling backups to the off-site and/or backup facility.
- New application systems development or system maintenance.
- Discontinuance of an application system from production.
- Significant modification of business processes or data flow requirements.
- Changes in the Notification Lists or the Business Continuity team.

## 11.2 Plan Auditing Requirement

Annual plan audits will be conducted to determine:

- The readiness of the Incident Management Team to respond to an emergency.
- Whether backed up data and documentation stored off-site are adequate to support the resumption of business operations
- Whether the inventories, tasks and procedures are adequate to support the resumption of business operations.
- Whether the Business Continuity Plan has been properly maintained and updated to reflect the actual resumption, recovery and restoration needs.

The plan audits will take place as part of the evaluation process through annual structured walk-through Avenu UPS or actual disaster recovery tests. Once the walk-throughs and tests are completed, the Avenu Insights & Analytics, LLC Service Continuity Delivery Team in consultation with the Local Business Continuity Coordinator will produce a plan audit report based on the bulleted items above. The plan audit report will document how well the plan meets the above requirements, identify any deficiencies in the plan, and make recommendations for improvement. The Avenu Insights & Analytics, LLC Service Continuity Delivery Team will update the plan to address the deficiencies identified in the plan audit report. The plan audit report and any necessary updates to the Business Continuity Plan will be submitted to the site's Incident Management Team and the Avenu Insights & Analytics, LLC Service Continuity Delivery Team for review.

## 11.3 Plan Security

The Business Continuity Plan is classified confidential and contains proprietary information to Avenu Insights & Analytics, LLC. These plans are not to be shared with anyone outside of Avenu Insights & Analytics, LLC without the approval of the Avenu Insights & Analytics, LLC Service Continuity Delivery Team. Plans must be scrubbed of all confidential and proprietary information when distributed outside of Avenu Insights & Analytics, LLC.

#### 11.4 Plan Distribution and Access

The following describes the processes and guidelines for distributing copies of the Business Continuity Plan, to ensure that key personnel have access to recovery procedures in the event of a disaster, and to ensure that copies of the plans are stored at a secure offsite location.

The Business Continuity Plan will be created and maintained in the following formats:

• Electronic: An electronic copy of the plan will be stored on the Avenu UPS network

The Local Business Continuity Coordinator will distribute new copies of the plan to team members, and ensure that all previous versions are destroyed. This will ensure that, in the event of a disaster, everyone is working from the same version of the plan. The Local Business Continuity Coordinator will also ensure that all appropriate team members are educated and trained on the plan changes.

## 12 Testing Procedures

This section contains an overview of the Business Continuity Testing process. Business Continuity Testing will address elements of the production system(s), which may require recovery (i.e. hardware, software, telecommunications, production data files and system documentation). The Avenu Insights & Analytics, LLC Service Continuity Delivery Team will develop a Business Continuity Testing Document which will include full details of the planned test, a detailed task timeline of the test schedule and any problems or recommendations documented during the test.

Business Continuity testing addresses:

- Notification of key individuals in the event of an emergency.
- Directing the work force to the recovery site.
- Obtaining and/or moving any required physical inventory to the recovery site.
- Establishing network connectivity.
- Redirecting vendor services to the recovery site.

The Avenu Insights & Analytics, LLC Service Continuity Delivery Team will work with the Local Business Continuity Coordinator in scheduling recovery tests, coordinating test activities and evaluating the recovery test results. The Local Business Continuity Coordinator will determine team members for planning the test as well as those who will participate in a test. The Avenu Insights & Analytics, LLC Service Continuity Delivery Team will track and document the recovery test, which will include any problems that occur or recommendations. When a recovery test has been completed, the Avenu Insights & Analytics, LLC Service Continuity Delivery Team will facilitate a post-review meeting with the recovery test participants. The Avenu Insights & Analytics, LLC Service Continuity Delivery Team will provide a summary report showing tasks performed, task timeframes, results, and action items. The summary report will be distributed to all test participants including Site and Client Management.

## 12.1 Plan Testing

Business Continuity Plan Testing for the business processing locations will be scheduled and performed on an annual basis. Structured walk-throughs and/or live testing exercises will determine the accuracy and completeness of the procedures and will help evaluate the timely recovery at the recovery site. Each test will be designed to simulate production operations at the recovery location in the event a disaster outage is declared.

Various types of potential interruptions to operational groups will be tested. Prior to a scheduled recovery test, a comprehensive walk-through of the Business Continuity plan will be performed to ensure the accuracy and completeness of the plan. This meeting will review previously documented disaster recovery plans and discuss the detailed steps to be followed by the sites in the event of a disaster.

The objectives of the walk-through will be to ensure that:

- Names of the people responsible for the plans are correct
- Detailed recovery steps are practical and will work
- Recovery locations are correct
- New applications or business functions are incorporated into the plans
- All team members fully understand the plans

## **12.2 Testing Objectives**

The scope, objectives, and timeline will be determined prior to each Business Continuity test and documented in the Business Continuity Testing Document. Problem resolution will be measured during each test. Upon the completion of the test, results will be compared to the test objectives to determine if all of the test objectives were met. If a test objective was not met, the results will be documented and will be included as a test objective in a future test. Issues and recommendations from the test will be documented for follow-up. A summary of the results of each test will be provided to all test participants including Site and Client Management.

## 13 Contact Directories

## 13.1 Avenu Contact Directory

Table 13-1 Avenu Contact **Directory** 

Name	Avenu	Phone	Email
David Lemoine	Vice President, UPS	O: 617-722-9673	David.lemoine@avenuinsights.com
Mark Capprini	Director, Claims, Calls and Holder Reports	O: 617-722-9643	Mark.capprini@avenuinsights.com
Deborah Arnold	Director, Securities Custody	O: 617-722-9657	deborah.arnold @avenuingishts.com

## 13.2 Vendor Contact Directory

Avenu Procurement maintains the vendor list

## 14 Appendixes

#### 14.1 Disaster Declaration Procedure

Service Continuity requires that authorized Account Management contact them when declaring a disaster. If a disaster declaration is required, proceed with the following procedure:

Enter a ServiceNow ticket to notify Avenu IT of the Disaster situation and provide them with the following information:

- 1) Your Name
- 2) Incident location
- 3) Physical Address (address of the facility where the disaster event is taking place)
- 4) Telephone number where the person reporting the incident can be reached
- 5) Nature of Disaster/Incident

The Avenu Helpdesk will take appropriate next actions to escalate with Avenu UPS, Executive management, Security Officer and others as needed. Situation Management will verbally contact the Service Continuity Management Team to review and escalate the incident as deemed necessary. A conference bridge will also be opened by Situation Management for Service Continuity Management to meet with the Site Management declaring the disaster event.

## 14.2 Corporate Media Policy

## 14.2.1 Applicability:

This Corporate Media Policy applies to all Avenu Insights & Analytics, LLC UPS employees and subcontractor staff.

#### 14.2.2 Policy

All press/media contacts are to be referred to Avenu Insights & Analytics, LLC Corporate Headquarters for assistance or approval.

### 14.2.3 Avenu Insights & Analytics, LLC' Corporate Press Contact

Press/media contacts include newspapers, television stations, radio stations, magazines, newsletters, journals, and trade publications for the health care industry, on-line services, and other organizations gathering and distributing information for the public. All responses to press/media requests are to be provided at Avenu Insights & Analytics, LLC Corporate Headquarters, unless otherwise approved.

#### 14.2.4 Procedure

Any individual representing a press/media organization is to be immediately referred to the local Manager on site. The Manager will refer the press/media representative to the appropriate corporate contact for assistance.

#### 14.2.5 Process

The employee receiving the press/media call or contact will refer the individual to the Avenu UPS Managing Director who will explain to the press/media contact that all press/media requests are addressed at Avenu Insights & Analytics, LLC' Corporate Headquarters and refer the individual to the appropriate corporate contact. The Managing Director will then proceed to inform the corporate contact that a press/media referral has been made.

Avenu Insights & Analytics, LLC corporate contact will seek approval to conduct the press/media interview. If approval is not given, the press/media contact will be notified by Avenu Insights & Analytics, LLC corporate contact.

With the approval of the State client and Avenu Insights & Analytics, LLC Vice President, key messages and answers to the press/media questions will be completed, a spokesperson designated, and an interview meeting scheduled. The press/media interview will be conducted. Avenu Insights & Analytics, LLC corporate contact will complete any follow-up activities.

#### 14.2.6 Accountability

The Avenu Insights & Analytics, LLC employee receiving the press/media contact is accountable for ensuring that the individual is immediately transferred to the Manager on-site. The Manager is then accountable for ensuring that the press/media is immediately referred to the appropriate corporate contact.

## 14.3 Incident and Crisis Response Center

In the event of an emergency situation at UPS facility, ensure all employees are aware of the following procedure.

#### 14.3.1 Incident and Crisis Response

In the event of a situation where an employee is unable to contact their supervisor or manager with their immediate status and location, the employee should contact the Avenu Insights & Analytics, LLC Human Resources team. The Avenu Insights & Analytics, LLC Human Resources team will be used as a backup for employees to report their status and location.

The employee should tell the representative the following information:

- That they have not been able to contact their immediate supervisor/manager (give the representative the name of their immediate supervisor/manager)
- That they (and their family) are safe
- If there are any personal or family injuries
- If they have experienced any personal property damage (residence or car)
- Their ability to get to work
- Their location and contact information (especially if they evacuated their home area).

## **14.4 Temporary Staffing**

In the event the Avenu UPS staff is unable to perform their normal daily operational duties because of an emergency situation or disaster, Avenu Senior Management will make the determination to hire clerical and programming personnel from a temporary staffing and/or technical services agency.

Table 15-1 Contract Labor Program Contact

Avenu Insights & Analytics, LLC Position	Name
CFO	James Barkman

## **14.5 AVENU Unclaimed Property Solutions Office**

AVENU UPS 100 Hancock Street 10<sup>th</sup> Floor Quincy, MA 02171 617-722-9600

#### 14.5.1 Directions to AVENU UPS Office from Logan Int'l Airport

(Driving time approx. 17 minutes / 9.54 miles)

Leave airport terminal and merge onto I-90 West/Mass Pike via Ted Williams Tunnel. Take the I-93 exit, exit 25-24, toward South Boston.

Take exit 24 on the left toward I-93.

Merge onto I-93 S/US-1 S/RT-3 S via the exit on the LEFT. Take exit 12 toward RT-3A S/Neponset/Quincy.

Turn slight right onto Gallivan Blvd/Rt-203 E. Turn slight right onto Gallivan Blvd. Turn slight right onto RT-3A S/Neponset Ave.

RT-3A S/Neponset Ave. becomes Neponset Bridge. Neponset Bridge becomes Hancock St. 100 Hancock St. is on the left.

#### 14.5.2 Best Western Adams Inn Crisis Command Center

Best Western Adams Inn 29 Hancock Street Quincy, MA 02171 (800) 276-7415

#### 14.5.3 Directions to Best Western Adams Inn from UPS Office

Start out going northwest on Hancock St./Rt.-3A N toward Newport Ave. Ext. Continue to follow Hancock St. The Best Western Adams Inn is on the Right.

#### 14.5.4 Holiday Inn Command Center

Holiday Inn Express & Suites Dorchester

1269 Massachusetts Ave. Dorchester, MA 02125 (617) 288-9262

#### 14.5.5 Directions to Holiday Inn from UPS Office

Start out going northwest on Hancock St./Rt.T-3A N toward Newport Ave Ext. Continue to follow Hancock St. Turn slight left onto Neponset Bridge. Neponset Bridge becomes Rt.-3A N/Morrissey Blvd./William T Morrissey Blvd. Merge onto I-93 N/US-1 N/RT-3 N/Southeast Expwy toward Boston. Take the Columbia Rd. exit, Exit 15, toward Edward Everett Sq. Turn right onto Columbia Rd. Pass through 1 roundabout. Turn slight right onto Massachusetts Ave.

1269 Massachusetts Ave is on the left.

## **14.6 Disaster Assessment Checklist**

Table 14-6 Disaster Assessment Checklist

Assessment conducted by:		Date/Time:
	Yes/No	Notes
Employee Safety		
Any worker injuries?		
How serious?		
Anyone hospitalized?		
Building Condition		
Are streets accessible?		
Is building accessible?		
All entrances accessible?		
Any safety concerns?		
Is building habitable?		
Utilities		
Is power on in the building?		
Is power on in the site?		
If not, is there partial power? Where?		
Any exposed electrical lines?		
Are there electric lights on?		
Is there water in the building?		
Is HVAC system on in building?		
HVAC on in site?		
HVAC on in Server Room?		
Is there sewer service?		
Are restrooms available?		

Physical Site	
Is site accessible?	
Both entrances?	
Do elevators work?	

Detail exactly what areas are affected physically. Take photos and/or voice recordings during a walk thru. Note such items as water/smoke/fire damage. Items such as hanging wires, ceiling tiles, wall problems, broken glass from terrace windows, dripping water, exposed structure, unsafe doorways, upended or turned over furniture, initial indication of equipment status. Be very diligent to gather as much information on problems/potential Yes/No Notes Basement storage room Is it accessible? Is freight elevator working? Any inventory damage? If yes, is inventory salvageable? Server Room Are servers up and running? If not all, which ones are on? Any UPS power units running? Are the routers working? Do the lights indicate any activity? Is Server Room usable? **Telecommunications** Are ACD lines up and running? Is network useable? Both inbound/outbound lines on? Are emergency phones working? Site Facility Floor Are cubicles/desks usable?

Any water/smoke/fire damage? If so, where?	
Are file cabinets damaged?	
Are any paper files damaged or destroyed?	
Mailroom	
Is mailroom intact? Usable?	
Any/all/some equipment usable?	
Has any mail/case files/manual records been damaged/ destroyed?	
File Room	
Note if any damage to records	
Managers Offices	
List which are usable	
Break & Conference Room	
Is kitchen usable?	
Annex Conference Room usable?	

## 14.7 Disruption of Service Checklist

Table 15-3 Disruption of Service Checklist

Notification of incident Business Continuity Coordinator performs the following:

- o Notify site management
- o Notify Avenu Insights & Analytics, LLC Service Continuity Delivery Team
- o Notify Avenu Insights & Analytics, LLC Shared Services Help Desk

Can disruption be corrected within the Recovery Time Objective?

	o Determine risk level	
)	If NO:	o If YES:
	Is building evacuation necessary?	Follow local site

Is building evacuation necessary?  o Are ALL employees accounted for o Are there any medical injuries?	Follow local site recovery procedures; no disaster declaration required
IMT activated based on incident circumstances	IMT activated based
o Notify Communications & Public Relations and Human Resources for assistance	, .

Initial damage assessment conducted	IMT meets at designated
	command center

Determine level of plan activation	Determine level of
Account Manager notifies client of situation and action to be taken	Account Manager
	notifies client of
	situation and action to
Notify critical vendor of situation	Primary Site returns

	to normal production
Notify staff of situation and decision to relocate	
Meet with recovery facility staff to review situation and recovery tasks	

Notify offsite storage facility to deliver offsite backups and materials to recovery site.

Arrange for travel arrangements for recovery teams.

Provide UPS Executive Management and client with situation update
Third party vendor prepares recovery facility for Avenu Insights & Analytics, LLC
Recovery teams and necessary staff relocate to recovery facility

Establish command center at recovery facility

Meet with recovery teams on approved strategies and recovery time expectations

Recovery preparations performed at recovery facility

- o Recover/restore/implement voice communications
- o Recover/restore/implement data connectivity

Monitor recovery; Provide UPS Executive Management and client updates at least every 3-4 hours.

on incident

## 14.9 Business Resumption Safety Checklist

The American Society of Safety Engineers' (www.asse.org) disaster safety checklist assists in providing items that need to be considered before, during and after a disaster.

- STRUCTURAL SECURITY: Have the structural integrity of the building or facility validated by qualified professionals before anyone enters the facility.
- SAFE ENTRY: Contact the proper government agencies to get approval to resume occupancy of the building. Do not enter a facility or building unless the proper clearances have been attained.
- CLEAN-UP SAFETY: Implement clean-up and business resumption processes in a safe and healthful
  manner. Nothing will be accomplished if employees are injured or killed during the post- disaster
  phase-in period. Provide training in proper selection and use of Personal Protective Equipment (PPE)
  for employees such as eyewear, gloves, and dust masks/respirators for cleaning, and where
  appropriate in other operations.
- AIR QUALITY ASSESSMENT: Make sure the atmosphere in the workplace environment is tested
  for asbestos and other chemical/toxic agents. Air quality is an issue businesses may wish to pay careful
  attention to when restarting business operations.
- VENTILATION: Have vents checked to assure that water heaters and gas furnaces are clear and operable. Dust and debris can stop or impede airflow decreasing its quality and healthfulness. Safely start-up heating, ventilation and air conditioning (HVAC) systems, which includes prior inspection of lines before energizing and pressurizing of the systems. Test ventilation systems now after inspection or have a qualified specialist do so. Blow cold air through HVAC systems first, as opposed to warm air, as it will help prevent the growth of mold in duct systems.
- INTERIOR, EXTERIOR EXPOSURES: For interior spaces, ensure no wall or ceiling materials are
  in danger of falling. If such exposures do exist, the work environment is not ready for occupancy.
  Check for cracked windows and outside building materials, as these could fall onto pedestrians at any
  time -- now and in the future.
- PROTECTION EQUIPMENT: For fire and smoke alarms it is important to assure that these have been
  cleaned and tested before allowing occupancy of the building. If such systems are wired into other
  systems ensure that they are still compatible and work in an efficient and effective manner. Thorough
  inspection of fire-fighting systems such as sprinkler and chemical equipment functions is a must do
  item.
- ELECTRICAL SAFETY: Have checks made of electrical systems, computer cables
  and telecommunications' equipment to ensure that they are still safe and there is no danger of
  exposure to electricity. Wiring inspections should be conducted from the outside in to ensure
  all wiring and connections are not in danger of shorting out due to water damage from rain or firefighting efforts.

- USE EXISTING FEDERAL GUIDELINES: Utilize existing start-up guidance materials provided by government agencies such as the Federal Emergency Management Agency (FEMA), http://www.fema.gov and the National Institute for Occupational Safety and Health (NIOSH), http://www.cdc.gov/niosh.
- HEALTH/SANITATION ISSUES: The general facility sanitation systems with the facility should be inspected and tested to guard against potential employee exposure to toxic agents. Food sanitation should also be an issue. Any unused foodstuffs should be discarded. If the workspace has a kitchen, inspect oven hoods and other ventilation devices to ensure they are not clogged and are working efficiently.
- OFFICE FURNITURE: Inspect the furniture to ensure it can withstand expected loads and
  usages. Ensure that binder bins (storage devices screwed or bolted to railing systems on walls and
  panels) have not become unstable due to water damage or shaking due to explosions. Inspect
  office equipment to ensure it is level, stable, and cannot tip over.
- LIGHTING: Make sure there are adequate illumination levels for employees. Emergency lighting should be checked to ensure it operates and functions in the correct manner.
- EMERGENCY PLANNING: Ensure that there is a clear path of egress for the emergency
  evacuation of employees that the fire extinguishers are still operable and that checks for damage and
  serviceability are made to see if any fire extinguishers' facilities were used during the disaster. If
  damage is found, they should be replaced immediately.
- SOLID/HAZARDOUS WASTE REMOVAL: Broken glass, debris, or other materials with cutting edges should be safely gathered and disposed of immediately. Ensure that such materials can be disposed of before collection to avoid creating even bigger hazards for both employees and the public. Solid waste disposal will be an issue, especially if hazardous waste is involved. Evaluate waste disposal issues prior to beginning clean-up operations to ensure it can be properly disposed of. ASSE's free 'Hazardous Materials Safety Information Guide' has key information and is available by contacting customerservice@asse.org.
- POWER CHECKS: If there is no access to electricity on the site, do not use fueled generators or heaters indoors. Ensure that there are no gas and sewer leaks in the facility. Check with local utilities for information regarding power, gas, water, and sewer usage.
- CHECK MAINFRAMES: If the facility has mainframe computer applications see that lines and cabling for chiller systems are checked to avoid chemical leak out.
- EMERGENCY PROCEDURES: Create a new emergency plan and distribute it to employees as soon as they return to work. In case of emergency, designate a place for employees to gather once out of the building or a phone number they should call following the emergency so that all can be accounted for. Frequently update the emergency contact list of names and phone numbers.
- MACHINE INSPECTIONS: Inspect the condition of drain, fill, plumbing, and hydraulic lines on processes and machines. It would be prudent to have plumbing lines evaluated and tested in order to detect any hazardous gases.
- SURFACES: Make sure flooring surfaces are acceptable and free from possible slips, trips and falls
   the second leading cause of on-the-job deaths in the U.S. ANSI standard A1264 protection of floor and wall openings is a good starting point.

## Disaster Recovery Plan

CONFIDENTIAL AND PROPRIETARY

NOT FOR PUBLIC DISCLOSURE

# **DISASTER RECOVERY OVERVIEW**



#### Overview

BNY Mellon has a robust testing program that covers a wide array of scenarios. Disaster Recovery (DR) exercises are conducted on a regular basis to ensure that, in the event of a natural disaster or similar disruption, we are prepared to maintain the highest level of availability and processing for our clients.

## Data Center Strategy

BNY Mellon takes a global approach to Technology Recovery with data centers in the U.S. and regional data centers in APAC, EMEA, and LatAm, each of which are strategically separated from our business operations. The sites are ISO 27001 certified, and Tier-3 grade facilities.

These data centers leverage redundant hardware, diversified and redundant telecommunications and utility power feeds, and redundant Universal Power Supply systems and backup generators. In addition, they provide disaster recovery services as well as computer operations command centers and crisis situation event rooms.

BNY Mellon contingency data centers are dedicated facilities controlled and supported by BNY Mellon staff and management. These data centers are configured to operate indefinitely at 100% of the production data center's capacity.

Our primary production data center recovers to one of two dedicated contingency data centers with replication of data occurring continuously. Local data backups are automated and conducted daily, or more frequently as defined by the application's architecture.

## **Testing Strategy**

Our Disaster Recovery program includes a variety of exercises throughout the year, including both targeted and large-scale internal tests, as well as participation in global forums and sector exercises—all designed to continuously enhance our resiliency posture. These exercises are a key component of our enterprise resiliency framework and validate our technology recovery capabilities and preparedness. These include, at a minimum, annual exercises for our primary and regional data centers.

A Disaster Recovery Test Exercise Memo, including timing and approach, can be shared upon request. As a matter of policy and for security purposes, we do not share the details of the DR exercise results.

The resiliency of our technology recovery program was demonstrated in July 2021 in response to flooding at our Luxembourg City site which damaged the power supply to the data center at that location. The failover to our alternate data center was successfully completed in response to this event and ensured continuity of service was maintained.

## Data Center Facilities Resiliency

#### **Environmental Protection**

Facilities infrastructure (e.g., air conditioning, water towers, generators, etc.) are isolated and protected by concrete walls. Each data center uses either self-contained glycol cooling or water storage tanks. The storage tanks can support both cooling and domestic water requirements and are configured to maintain cooling operations indefinitely.

Information Classification: Confidential

Specialized fire protection is implemented within the data processing areas and monitoring systems are in place and in compliance with all applicable local codes. Fire protection is provided by double interlocked pre-action firecycle sprinkler systems and central fire alarm controllers with addressable photoelectric smoke detectors and heat sensors located above and below the floor.

#### **Power Supply**

Our data centers are supported by automated power fail over systems which include multiple connections to outside electrical sources through different routes, battery back-up sufficient to carry the full load of the center while we convert to generator and triple redundant generator power to provide ongoing operations in the event of an electrical failure.

Our online double-conversion UPS systems provide the highest level of protection by isolating the computing equipment from raw utility power, while managing power anomalies such as sags or surges. The system also provides zero transfer time and protects against electrical line noise, frequency variation and harmonic distortion.

Diversity and redundancy are built into our designs and infrastructure configurations.

Network infrastructure is fully redundant (i.e., routers, switches, firewall, load balancers).

Primary and backup components comprise the infrastructure.

#### **Physical Security**

Our data centers are surrounded by secured fencing and monitored 24x7 by security guards. Internal physical access control includes retinal scanning for the most critical areas. Exterior and interior security cameras span all areas that record activity. Facilities infrastructure (e.g., air conditioning, water towers, generators) are isolated and protected by concrete walls.

#### **Data Center Rotations**

BNY Mellon's Enterprise Resiliency strategy addresses the risk related to the ability to provide

uninterrupted services. As such, a key element of the Enterprise Resiliency strategy is to plan appropriately so that in the event of a disruption, applications supporting Critical Business Services ("CBS") can rotate to a designated alternate data center and resume sustainable operations for an extended period. This ability, and BNY Mellon's Enterprise Resiliency strategy as a whole, is supported by the applications, infrastructure, and operational capabilities that underpin these services.

The establishment of Data Center Rotation (DCR) exercises represents advancement in BNY Mellon's resiliency and builds on existing DR practices focused on the restoration of technology and information assets. DCR goes beyond DR's restoration goal with the aim of achieving sustained business-as-usual ("BAU") production in an alternate location.

DCR requires active participation of applicable technology, business services, and/or functions, including external clients, vendors, and other third parties, to support and build response capabilities to increase BNY Mellon's preparedness to operate through planned and unplanned operational and technology disruptions.

#### Governance

Under our Disaster Recovery Policy, BNY Mellon has developed and maintains a DR Program, which establishes our DR strategy, framework and standards of execution for all areas involved in our DR planning and testing.

BNY Mellon's business continuity framework is developed, overseen, and governed by our Enterprise Resiliency Office (ERO), which aligns, centralizes and integrates disciplines and capabilities to deliver timely and effective incident identification, impact assessment, escalation, communication and resolution; provide clients with superior service; and deliver resilient world-class products and services.

Our Enterprise Resiliency Council is responsible for providing oversight, governance, and

guidance to ensure that business continuity risks are defined, understood, and effectively managed and reports to BNY Mellon's Technology Oversight Committee.

BNY Mellon's ERO has senior level oversight, focus and support, including the Board of Directors, the Senior Risk and Controls Committee, the Technology Oversight Committee, and the Enterprise Resiliency Council.

BNY Mellon is the corporate brand of The Bank of New York Mellon Corporation and may be used to reference the corporation as a whole and/or its various subsidiaries generally. This material does not constitute a recommendation by BNY Mellon of any kind. The information herein is not intended to provide tax, legal, investment, accounting, financial or other professional advice on any matter, and should not be used or relied upon as such. The views expressed within this material are those of the contributors and not necessarily those of BNY Mellon. BNY Mellon has not independently verified the information contained in this material and makes no representation as to the accuracy, completeness, timeliness, merchantability or fitness for a specific purpose of the information provided in this material. BNY Mellon assumes no direct or consequential liability for any errors in or reliance upon this material.

This material may not be reproduced or disseminated in any form without the express prior written permission of BNY Mellon. BNY Mellon will not be responsible for updating any information contained within this material and opinions and information contained herein are subject to change without notice. Trademarks, service marks, logos and other intellectual property marks belong to their respective owners.

© 2023 The Bank of New York Mellon Corporation. All rights reserved. Member FDIC.