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.

Header 1

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 1349742
Procurement Type: Central Master Agreement
Vendor ID: VC0000082535
Legal Name: AVENU SLS HOLDINGS LLC
Alias/DBA:
Total Bid: $56,362.00
Response Date: 01/30/2024
Response Time: 12:42
Responded By User ID: avenumike
First Name: Daniel
Last Name: Wurz
Email: daniel.wurz@avenuinsights.c
Phone: 9094968573

SO Doc Code: CRFQ
SO Dept: 1300
SO Doc ID: STO2400000003
Published Date: 1/22/24
Close Date: 1/30/24
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum No 1 - UP Securities Custodial
Total of Header Attachments: 1
Total of All Attachments: 1

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 Item	350.00000	EA	20.000000	7000.00

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 Research/Calcs	4.00000	EA	50.000000	200.00

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	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	Securities Custodial Services - Liquidate DTC Item	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	100.00000	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 Item	5.00000	EA	25.000000	125.00

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)

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

COVER LETTER

[illegible]

[illegible]
[illegible]
[illegible]
[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] Treasurer's [illegible] class unclaimed security management services to the State of West Virginia State Treasurer's Office ("STO") [illegible]

[illegible] Avenu team's [illegible] the STO's unclaimed securities program. Avenu's team offers a detailed and unmatched [illegible] the STO's [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]
[illegible]
[illegible]
[illegible]

[illegible]

[illegible] STO's Qualifications requirements in this section. For ease of reference, Avenu has [illegible] STO's requirements in [illegible]

[illegible]

[illegible] Treasurer's Office [illegible] administration of the state's [illegible] Treasurer's policy on restricting the flow of state dollars to [illegible]

[illegible] Neither of these companies is on the Treasurer's Restricted Financial [illegible]

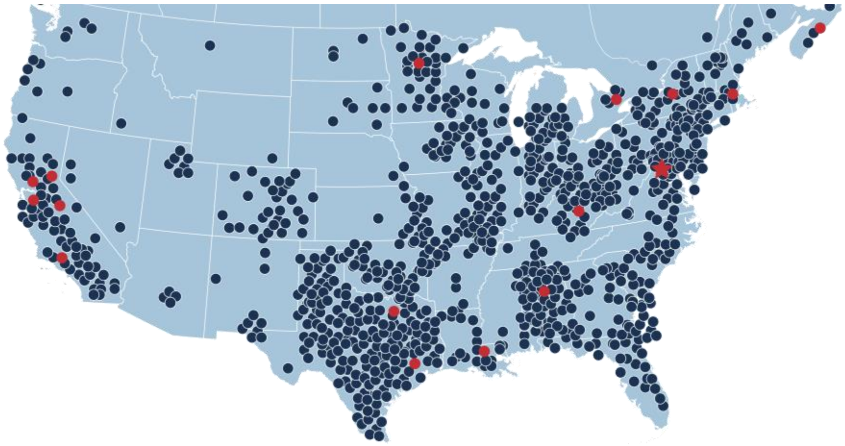
[illegible] 100 [illegible]

[illegible] Mellon ("[illegible]") [illegible] ("RJ") [illegible]

[illegible] 700 [illegible] 10 [illegible] Avenu's [illegible] 50 [illegible]

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

[illegible] 96 m[illegible] 8 [illegible] D[illegible] 0 [illegible]

D[illegible] 016 [illegible] commitment to the success of the STO's unclaimed securities custody operations [illegible]

[illegible] 9 [illegible] West Virginia State Treasurer's Office [illegible]

I[illegible]

For perspective, Avenu's custody solution has been developed and enhanced over a period of almost four decades, and [illegible]

[illegible] N[illegible] M[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

3.1 STAFF REQUIREMENTS:

[illegible]

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 [illegible]'s specific [illegible]

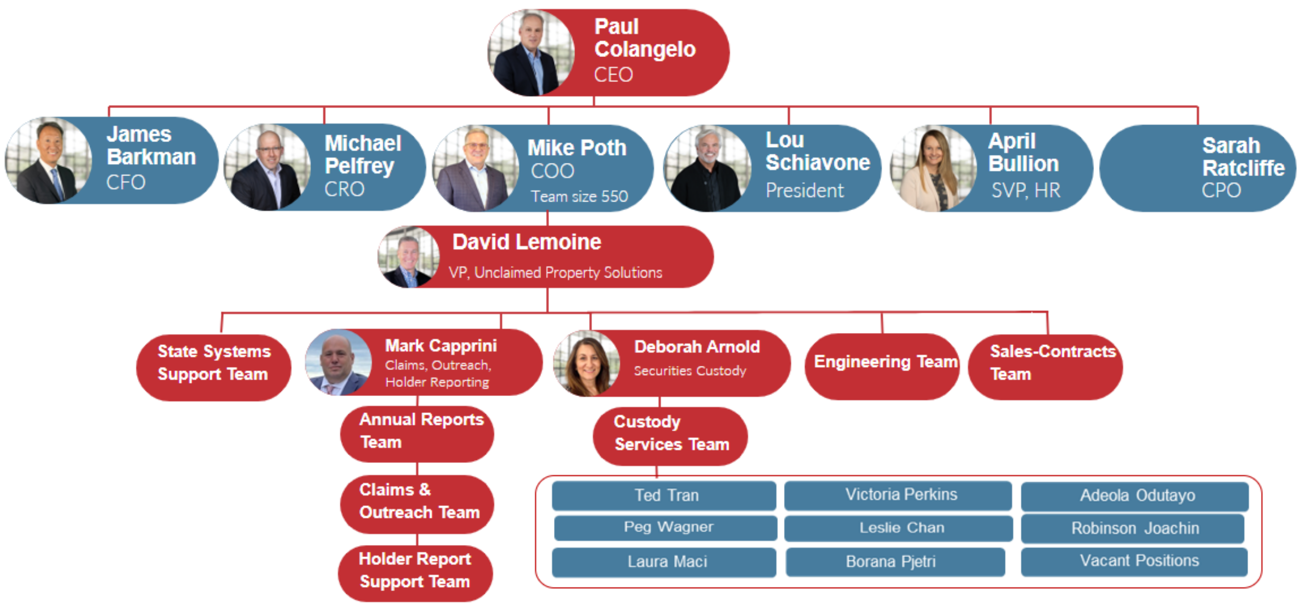
[illegible]

[illegible]

[illegible]

[illegible]

Avenu Leadership



3.1.1 AVENU – STO ASSIGNED STAFF RESUMES

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

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, [illegible]

[illegible]

[illegible] Maine's important credit status. He also gained enormous insight into o[illegible]

[illegible]

[illegible]
[illegible]

[illegible]

[illegible] ars' exper[illegible]

[illegible]

[illegible]

[illegible]
[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

She strengthens Avenu's team with her experience in unclaimed property audits, clear client communications, complex report [illegible]

[illegible] bachelor's degree in business management [illegible]

3.1.2 RAYMOND JAMES RESUMES

[illegible]

[illegible]

58[illegible]0 [illegible] 00
[illegible] 6
80[illegible] 5[illegible] 11[illegible] 8
[illegible]

[illegible] In those positions, he had direct responsibility for Virginia's unclaimed property program [illegible]

[illegible]

[illegible] Ron's career highlights and credentials are listed as follows:

- [illegible] 001[illegible] 0[illegible]

- Manage Firm's Unclaimed Property Security Liquidation Practice for 30 States, the District of C[illegible]m[illegible]d [illegible] C[illegible]mm[illegible]
  - M[illegible] M[illegible]d [illegible] I[illegible]m[illegible] [illegible]r[illegible]
- Secretary of Finance, Virginia Governor's Cabinet. 1996–2001
- Tr[illegible]r [illegible]r[illegible] [illegible]d D[illegible] Tr[illegible]r [illegible]r[illegible] 1987–1996
- [illegible]r [illegible]d[illegible]r[illegible] [illegible]m[illegible] C[illegible]mm[illegible] [illegible]d [illegible]d[illegible] [illegible]d [illegible] C[illegible]mm[illegible] 1978–1987

M[illegible]r [illegible]rd[illegible] [illegible]d [illegible]r [illegible]m[illegible]

- C[illegible]mm[illegible] [illegible]r[illegible] D[illegible]C[illegible] [illegible]d[illegible]r C[illegible]mm[illegible] [illegible]r [illegible]m[illegible] 010–0[illegible]
- C[illegible]r N[illegible]r [illegible]r [illegible]rd [illegible]r [illegible]r [illegible]m[illegible] 0[illegible]0[illegible]6
  - Tr[illegible] C[illegible]r [illegible]r C[illegible]d[illegible]r C[illegible]r N[illegible]r [illegible]r[illegible]
  - C[illegible]rm[illegible] I[illegible]m[illegible] C[illegible]mm[illegible] CN[illegible] [illegible]d[illegible]
- [illegible]rd [illegible] Tr[illegible] N[illegible] I[illegible]r [illegible] N[illegible] Tr[illegible]r[illegible] [illegible]d [illegible]rd[illegible] [illegible]r 015–0[illegible]
- C[illegible]rm[illegible] [illegible]rd [illegible]r C[illegible]r[illegible] 005–0[illegible]
- C[illegible]r[illegible] [illegible]d[illegible]r [illegible]rd N[illegible] Tr[illegible]r[illegible] 0[illegible]0[illegible]5

SE[illegible] [illegible]d [illegible]d[illegible]r [illegible]r A[illegible]r[illegible] N[illegible]A[illegible]

[illegible]r[illegible] 7 – [illegible]r[illegible]r[illegible] [illegible]r[illegible]
[illegible]r[illegible] 50 – M[illegible]d[illegible]r [illegible]r[illegible]
[illegible]r[illegible] 5[illegible] – M[illegible]r[illegible] [illegible]r[illegible]
[illegible]r[illegible] 5[illegible] – M[illegible]r[illegible] [illegible]r[illegible]
[illegible]r[illegible] 5[illegible] – M[illegible]d[illegible]r [illegible]r[illegible]
[illegible]r[illegible] 6[illegible] – [illegible]rm [illegible]r[illegible] [illegible]m[illegible]
[illegible]r[illegible] 79 – I[illegible]m[illegible] [illegible]r[illegible]
[illegible]r[illegible] 99 – [illegible]r[illegible] [illegible]r[illegible] [illegible]r[illegible]

[illegible]d[illegible]r [illegible]r[illegible] D[illegible]r[illegible]m[illegible] [illegible]r [illegible]r[illegible]r [illegible]r[illegible] [illegible]r[illegible]r[illegible]d [illegible]d [illegible]d[illegible]l [illegible]dd[illegible] [illegible]r [illegible]r[illegible] r[illegible]r [illegible]d [illegible]d[illegible] r[illegible] D[illegible]r[illegible]m[illegible] [illegible]r[illegible]

[illegible]AM A[illegible]EN
[illegible]I[illegible]T [illegible]IC[illegible] [illegible]ID[illegible]NT [illegible]I[illegible]T[illegible]NT

[illegible]m [illegible]d [illegible] 1981 [illegible]d [illegible]r[illegible]d[illegible] M[illegible]r[illegible] C[illegible]rd[illegible]r [illegible] I[illegible] Tr[illegible]d[illegible] D[illegible]r[illegible]m[illegible] M[illegible] [illegible]r [illegible]r[illegible]r M[illegible]r[illegible] I[illegible] [illegible]r[illegible]r [illegible]rm'[illegible] C[illegible]rm[illegible]
[illegible] 1991 M[illegible] [illegible]r[illegible] I[illegible]m[illegible] D[illegible] [illegible]dd[illegible] I[illegible] D[illegible]r[illegible]m[illegible] M[illegible]r[illegible] [illegible]rd[illegible] m[illegible]r[illegible] [illegible]r [illegible]r I[illegible] [illegible]r[illegible] [illegible]d[illegible]r [illegible]r[illegible] [illegible]d [illegible]r M[illegible]r[illegible] [illegible]d [illegible]r[illegible] [illegible]r[illegible] [illegible]d r[illegible]d[illegible] [illegible]r[illegible]

M[illegible]d[illegible] N[illegible]D [illegible]r[illegible] 7 – [illegible]r[illegible]r[illegible] [illegible]r[illegible] [illegible]r[illegible] [illegible]d [illegible]m[illegible]d N[illegible] [illegible]r[illegible] 6[illegible] – [illegible]rm [illegible]r[illegible] [illegible]m[illegible] M[illegible] [illegible]d [illegible]r[illegible]d[illegible] [illegible]r[illegible] [illegible]r [illegible]9 [illegible]r M[illegible] [illegible]d d[illegible]r[illegible] [illegible]r [illegible]d[illegible] [illegible]m[illegible]d [illegible]r[illegible] [illegible]r 11 [illegible]r [illegible]r[illegible] T[illegible]d [illegible]

[illegible]d[illegible]r [illegible]r[illegible] D[illegible]r[illegible]m[illegible]m [illegible]r [illegible]d[illegible]d[illegible] [illegible]r [illegible]r[illegible]d[illegible] [illegible]r[illegible]

[illegible] A[illegible]
[illegible]r[illegible]d[illegible] [illegible]r [illegible]d[illegible] [illegible]m[illegible]d [illegible]r[illegible]
1[illegible]80 [illegible]r[illegible]
C[illegible] NC [illegible]7517

[illegible]

3.1.3 BANK OF NEW YORK MELLON RESUMES

[illegible]

Jessica joined Asset Servicing's Investment Management segment, as a Relationship Manager, in February 2022. In this [illegible] Asset Servicing's efforts in managing key strategic relationships, in our growing Asset Manager space. [illegible]

Prior to joining BNY Mellon in 2009, Jessica was a Client Manager for Bank of America's Government Banking division. [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Treasurer's Office, Division of Unclaimed Property

Avenu is proud to be the incumbent custodian with a current team in place for the West Virginia State Treasurer's Office,

Avenu is proud to be the incumbent custodian with a current team in place for the West Virginia State Treasurer's Office,

Indiana Attorney General's Office

[illegible]

N[illegible] Organization	[illegible] Services	[illegible] Services Performed	[illegible] Address [illegible] Number
[illegible] Auditor's **General's Office** [illegible] Department	[illegible] Custodial [illegible] 1990 [illegible]	[illegible] Custodial [illegible] M[illegible] M[illegible] Treasury [illegible] M[illegible] Corporate [illegible]	[illegible] Director [illegible] Department [illegible] 50[illegible] IN [illegible]616[illegible] [illegible]17[illegible]88[illegible]5[illegible]1 [illegible]
T[illegible] S[illegible] Tr[illegible] [illegible] Department	[illegible] Custodial [illegible] 1990 [illegible]	[illegible] Custodial [illegible] M[illegible] M[illegible] Treasury [illegible] M[illegible] Corporate [illegible]	[illegible] Director [illegible] 10[illegible] N[illegible] TN [illegible]7[illegible]0[illegible] 615[illegible]5[illegible]0[illegible]
M[illegible] S[illegible] Tr[illegible]r's Office M[illegible] Department	[illegible] Custodial [illegible]019 [illegible]	[illegible] Custodial [illegible] M[illegible] M[illegible] Treasury [illegible] M[illegible] Corporate [illegible]	[illegible] Director [illegible] 10 [illegible] C[illegible] M[illegible] 6510[illegible] 57[illegible]751[illegible]08[illegible]

3.2 WEB PORTAL REQUIREMENTS

[illegible]

[illegible] N[illegible] M[illegible]'s extraordinarily [illegible] N[illegible]X[illegible]N[illegible] [illegible] Custodial [illegible] N[illegible]X[illegible]N[illegible] [illegible] T[illegible]1[illegible] N[illegible]X[illegible]N[illegible] [illegible] 15 [illegible] system's [illegible] N[illegible]M [illegible] N[illegible]X[illegible]N[illegible] [illegible] the bank's [illegible] N[illegible]X[illegible]N[illegible] [illegible] built on BNY Mellon's BXP Platform as a Service (PaaS). I[illegible] X

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

- **Microsoft Edge (Chromium Engine)**
- **Google Chrome**
- **Apple Safari**
- **Mozilla Firefox**

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] 6 ***CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE*** [illegible]

[illegible] our client's key data resides [illegible]

[illegible] g authorized signer lists. Avenu's annual third [illegible]

[illegible]

[illegible]

[illegible]

E[illegible]

[illegible]

T[illegible]

S[illegible] in the position to perpetrate and conceal errors or irregularities in the normal course of an employee's duties. For each [illegible]

A[illegible] **d** [illegible] **rd** [illegible] **A**[illegible] **S**[illegible] **rd**[illegible]

[illegible]

Avenu maintains each of our client's monthly statements onsite, which includes both a statement of transactions as well [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] as it provides access to many securities exchange markets around the world. BNY Mellon's data center for its [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] **M**[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

T[illegible]**M**[illegible]

- [illegible]

T[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

3.3 DISASTER RECOVERY AVAILABILITY

[illegible] **STO** [illegible]

[illegible] (“Disaster Recovery”) for inspection by STO [illegible] 8 *CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE*[illegible]

[illegible]

[illegible] Avenu’s custody solution and [illegible]

[illegible] BNY Mellon [illegible] overview of BNY Mellon's disaster recovery is included under Exhibit 8 *CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE*[illegible]

[illegible]

Avenu's BCP [illegible]

Avenu's sub[illegible] client's key data is held on the BNY Mellon [illegible] BNY Mellon's Business Continuity Program (BCP) is based on industry [illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]

[illegible] BNY Mellon [illegible] management. These data centers are configured to operate indefinitely at 100% of the production data center's capacity [illegible]

[illegible] failover from the primary data center be required. BNY Mellon's Business Continuity [illegible] 7 *CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE*[illegible]

[illegible] the event a disaster disrupts the firm's ability to do business.

[illegible]

[illegible]

[illegible] laptops that support Avenu's custody solution and have been tested. Key STO data is held on the BNYM NEXEN [illegible]

[illegible]

[illegible]

3.4 PERSONALLY IDENTIFIABLE INFORMATION

[illegible]

- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

[illegible]

Avenu's Solution provides:

- [illegible]
- Industry leading Enterprise Email Security solution which consistently ranks in the top right (Leader's) Gartner [illegible]
- 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.
- [illegible]
- [illegible]
- [illegible]

- [illegible]
- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible] West Virginia's assets reside within BNY Mellon's NEXEN platform and as the leader in the custody [illegible]

[illegible] NIST [illegible] committees, including the Board of Directors. BNY Mellon's appr[illegible]

- [illegible] use "defense in depth" where multiple layers of security controls are placed throughout creating deliberate [illegible]

- [illegible]'s information protection policies and standards.
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] compliance with the SEC's Customer Protection Rule and Net Capital [illegible]

For perspective, Avenu's custody solution has been developed and enhanced over a period of almost four decades, and

198

Avenu's website can be found at:

STATE OF WEST VIRGINIA STATE TREASURER'S OFFICE

[illegible] M[illegible]ND[illegible]T[illegible] [illegible]I[illegible]M[illegible]NT[illegible]

4.1 MANDATORY CONTRACT SERVICES REQUIREMENTS AND DELIVERABLES

[illegible]

[illegible] C[illegible] D[illegible]

4.2 DELIVERABLES

[illegible]

[illegible] ST[illegible] S[illegible] Tr[illegible] ST[illegible] ST[illegible]

[illegible] we have an account established in the STO's name for use solely by the STO and Avenu on its behalf [illegible] DTC[illegible]D[illegible] C[illegible]D[illegible] T[illegible]

[illegible] T[illegible] D[illegible]

[illegible] ST[illegible] ST[illegible] ST[illegible] ST[illegible]

[illegible] TO's [illegible] T[illegible]

[illegible] T[illegible]'s [illegible]

[illegible] DTC[illegible]D[illegible] C[illegible]D[illegible] T[illegible] assigned nominee name, in the street name and owner's name) when certificates are delivered, however, we work to

[illegible] DTC [illegible]

[illegible]

[illegible]

[illegible] Tr[illegible]

[illegible] DTC [illegible] accuracy of holder reporting. This in turn reduces the amount of time required by the State's staff to have to follow up on [illegible]

[illegible] sure that all property reported and presented for delivery into the State's account is received. Avenu credits the positions [illegible]

[illegible] S[illegible]

[illegible] DTC[illegible]

[illegible] State's account. This happens within 48 hours of the transfer agent's approval.

[illegible]

- [illegible]
- [illegible]
- [illegible] shares are deposited into the State's account.

[illegible] allows the position to be settled at DTC within 48 hours of transfer agent's approval and reflected in your [illegible] the books of the transfer agent to the customer's account with [illegible]

- [illegible]
- [illegible]

- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

N[illegible]S[illegible] (NS[illegible])

[illegible]

A[illegible] A[illegible] Tr[illegible] S[illegible] (A[illegible]ATS)

[illegible]

[illegible]S[illegible]

[illegible]

[illegible] ST[illegible]'s account manager will advise the ST[illegible] [illegible] ST[illegible]'s account, maintained in the vault, and coded as such. [illegible]

[illegible] registration to Hare & Co (BNY's nominee name) to ensure certificate is valid. When the new certificate is received from [illegible]

M[illegible]d[illegible]d [illegible]

Avenu's automated maintenance for Mutual Funds and Dividend Reinvestment Plans (DRPs) eliminates the processing of [illegible] positions are properly maintained in the STO's account. Daily

r[illegible] m[illegible] [illegible]

Mutual Funds – [illegible] m[illegible] T[illegible] NXN[illegible] [illegible] 5[illegible] – M[illegible]

DRPs – [illegible] regularly and posted to the STO's account.

[illegible] mutual fund holdings in the STO's accounts.

S[illegible]

Avenu provides custody services for almost every foreign market through BNY Mellon's sub[illegible]

[illegible] M[illegible]

[illegible] T[illegible]'s current provider, Avenu currently ensures the posting of all dividends, interest and other distributions to the [illegible] NXN[illegible] is the security's CUSIP number.

[illegible] end of each day to ensure the STO's account has been properly credited. All information related to all security types is [illegible] NXN[illegible] NXN[illegible]

[illegible] 5[illegible]

[illegible] A[illegible]

[illegible]

[illegible] A[illegible] Tr[illegible] [illegible]

[illegible] DTC [illegible] DTC [illegible]

[illegible] M[illegible] S[illegible]

Avenu believes a true partner should focus on looking for ways to make our clients' lives easier and more efficient. We [illegible]

[illegible]'s desire and process all [illegible]

[illegible]

[illegible] A[illegible]

[illegible] N[illegible]X[illegible]N[illegible]

T[illegible] may operate on a standing instruction to take the 'default' [illegible]

[illegible] N[illegible]X[illegible]N[illegible] C[illegible]d[illegible] Tr[illegible] [illegible]

[illegible] 5 [illegible] Tr[illegible] [illegible]

M[illegible]d[illegible]r[illegible] A[illegible]

Avenu tracks and processes all mandatory corporate actions made by issuers of securities which are held in Avenu's [illegible]'s account. As [illegible]

[illegible] DTC [illegible]'s account and held in our vault.

[illegible]'s account

[illegible]
etc. Avenu processes and posts all corporate actions made by issuers of securities which are held under Avenu's custody [illegible]

[illegible]

[illegible]'s account. All income balances are reconciled daily to ensure that the [illegible]'s account has been properly credited with [illegible] 5 [illegible]

[illegible] M[illegible] ST[illegible] ST[illegible]

[illegible]'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 [illegible]'s [illegible]

[illegible] 1951 [illegible]
New York City, is one of the nation's leading mutual fund companies. A co[illegible] Dr[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] client's accounts. We additionally will contact entities, at the request of the STO, or if we identify that they are holding [illegible] account.

[illegible]

[illegible] account which includes the [illegible]

[illegible]

such cases, BNY Mellon's Global Pricing team would use a secondary vendor, if available. If one is not available, they will

Global Pricing Unit Vendor Chart

The Bank of New York Mellon subscribes to a number of pricing sources. The following outlines the service provided by these pricing vendors and their designation as primary or secondary price source.

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,

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

[illegible] We currently have our clients’ [illegible] packages which include a List of Assets and Transaction Statement in .pdf as well as Excel for the STO’s records[illegible]

[illegible]

[illegible] ’s authorized signers for verification.

[illegible] are submitted by an authorized user from the STO. Additional information on Avenu’s [illegible]

After the verification process is complete, transactions are processed and immediately will show in the STO’s custodial [illegible]

[illegible]

[illegible] perform a “quick” lookup by security name on the NEXEN® home page to obtain any CUSIP numbers. Avenu is happy to [illegible]

[illegible]

[illegible] ’s unclaimed property management system.

[illegible]N® is BNY Mellon’s Internet[illegible]

[illegible] ’s staff is fully [illegible]

[illegible] ’s accounts and can select from [illegible]

[illegible]

[illegible]

[illegible]

Avenu currently receives and deposits into the STO's unique account all securities, including Mutual Funds delivered by [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

- 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 [illegible]
- [illegible]
- [illegible]
- [illegible]

1 [illegible]

[illegible]

- [illegible] STO's approval to liquidate as such.

- [illegible] "write off" non[illegible] DTC [illegible]

[illegible] STO's approval. [illegible]

[illegible] DTC [illegible] STO's portfolio with explanations. DTC refers to this process as PREM or Position REMoval. [illegible] DTC [illegible] STO's regular reports.

[illegible]

[illegible] STO's account until specific [illegible]

[illegible]

[illegible] STO's administrator, will execute the sale of any listed [illegible] STO's instructions and report each liquidation with a detailed transaction [illegible] STO's investment Account immediately upon settlement of the sale.

A[illegible] S[illegible]r S[illegible]

[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]

[illegible]

[illegible]’s account upon settlement and wired upon [illegible]

[illegible]

[illegible]

[illegible]’s account.

[illegible]’s Investment Account. All [illegible]

[illegible]’s account and simultaneously, sale proceeds deposited to the account then automatically swept to the State’s chosen investment account. Al[illegible]

[illegible]’s authorized [illegible]

[illegible] of all marketable securities, which creates a transaction on BNY Mellon’s Global Securities Processing System and in turn [illegible]’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 [illegible]

[illegible] STO's account manager with Avenu must actively verify each sale transaction, [illegible] STO's account and sale proceeds are received at that time. These shares are [illegible]

Avenu's account administrator will provide the [illegible]

[illegible]

- [illegible] STO's authorized individual inputs a trade request through our web [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible] DTC ID [illegible]
- [illegible]
- [illegible] DTC [illegible]
- [illegible]

[illegible]

[illegible] then be uploaded to the STO's Unclaimed Property System.

[illegible]

[illegible] of DTC. The STO's account manager at Avenu receives the STO's instructions to liquidate, and instead of forwarding the [illegible]

[illegible]

[illegible]

A[illegible]

[illegible] 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 [illegible]

[illegible] STO's unclaimed property database is updated accordingly.

[illegible] STO's Unclaimed Property system. Avenu can set up a daily transmission of the transaction file data to the [illegible]

[illegible]

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

[illegible]

[illegible]

[illegible] STO's dedicated account manager, Vicki Perkins, will coordinate for problem resolution. Once the discrepancy is [illegible]

[illegible]

[illegible] STO's account with a complete description of the transaction including information [illegible]

[illegible]

[illegible]

***File Transfer Protocol* –** [illegible] delivered to Avenu's secure FTP site to initiate transfer requests.

[illegible]'s staff to spend the time [illegible]

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 [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Written Request [illegible] 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 [illegible]

Avenu Extranet – [illegible] can initiate transfer requests using Avenu's online Extranet system. Please refer to Avenu [illegible]

[illegible]

[illegible]

[illegible]'s account with a complete description of [illegible]

[illegible]

Direct registration shares (“DRS”) is a practice that is being increasingly promoted by transfer agents and holding [illegible]’s DTC account.

[illegible]

[illegible] DTC [illegible] DTC [illegible]

[illegible]

[illegible]’s unclaimed property management system. [illegible]

[illegible]

If the position is being transferred to an owner’s account via DTC, the securities will be deposited to the owner’s [illegible] DTC [illegible] to include a place for owners’ brokerage account information on the claim form when [illegible]

[illegible]

[illegible]’s instructions, either directly to the [illegible]

[illegible]

[illegible]

[illegible]	[illegible]
[illegible] (DTC)	[illegible]
[illegible]	[illegible] – 5 [illegible]
[illegible]	10 – 15 [illegible]
[illegible]	5 – 10 [illegible]
[illegible]	10 – 15 [illegible]
[illegible]	10 – [illegible]

[illegible] STO’[illegible]

[illegible] the STO's staff for final [illegible]

M[illegible]d

Avenu will reissue a mutual fund into an owner's name upon receipt of authorized instruction from the [illegible] fund company or broker to have the shares transferred to the owner's account whenever possible.

[illegible] to include a place for an owner's brokerage account information on the claim form for a [illegible]

[illegible]

[illegible]

[illegible] 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 [illegible]

[illegible]

Avenu processes and posts all corporate actions made by issuers of securities which are held in Avenu's custody for the [illegible] any settlements, all receipts are reconciled at the end of each day to ensure that the STO's account has [illegible]

[illegible]

[illegible]

[illegible]

4.3 DELIVERABLE - ACCOUNTING AND REPORTING

[illegible]

[illegible]

[illegible]

[illegible] the STO's needs change [illegible]

[illegible]

[illegible]

[illegible]

[illegible] 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 [illegible]

[illegible]

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.

[illegible]

[illegible]

[illegible] NEXEN® is BNY Mellon's Internet [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible] ’s unclaimed [illegible]

[illegible]

[illegible]

- [illegible]

- [illegible]
- [illegible]

[illegible]

- A detailed report identifying number of [illegible]
- An inventory of the securities held;
- A [illegible]
  - Date of Transaction
  - Number of Units
  - Market Value
- A [illegible]
- 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

[illegible]

[illegible]

- ► [illegible]
  - ✓ [illegible]
  - ✓ [illegible]
  - ✓ [illegible]
- ► [illegible]
  - ✓ [illegible]
  - ✓ [illegible]
- ► [illegible]
  - ✓ [illegible]
  - ✓ [illegible]
- ► [illegible]

[illegible]

- Number of Units
- Issue Name
- Market Value
- Dividends Earned in detail
- Corporate A[illegible]

[illegible]

[illegible]

[illegible]

[illegible]'s current custodian/broker. Avenu will ensure an easy and thorough transition process by [illegible]

- ▶ [illegible]
- ▶ [illegible]
- ▶ [illegible] or successor contractor related to Avenu's prior administration of the [illegible]
- ▶ [illegible]

[illegible]

[illegible] Tr[illegible]rer's Office [illegible]

4.4 DELIVERABLES - OTHER

[illegible]

[illegible]

[illegible]

In order to provide *best-in-class service* [illegible]

[illegible]

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

[illegible]

[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Raymond James & Associates, Inc. (“RJA” or “Raymond James”) has been in [illegible]

[illegible] symbol "RJF", and its shares are currently owned by more than 18,000 individual and institutional investors.

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.

[illegible]

[illegible]

Number of Transactions				Number of Shares				Economics
Calendar Year	Tradeable	Non-Tradeable	Total	Calendar Year	Tradeable	Non-Tradeable	Total	Transaction Dollar Value
2013	22,344	4,063	26,407	2013	47,711,425	8,491,422	56,202,847	$ 569,941,457
2014	23,641	3,637	27,278	2014	142,261,735	47,924,528	190,186,263	$ 570,746,807
2015	27,267	5,222	32,489	2015	109,949,954	234,158,300	344,108,254	$ 787,986,439
2016	28,606	4,401	33,007	2016	47,689,049	92,093,628	139,782,677	$ 542,299,547
2017	34,751	5,526	40,277	2017	45,014,745	317,104,684	362,119,429	$ 746,346,496
2018	31,984	4,403	36,387	2018	76,140,167	279,328,635	355,468,802	$ 763,708,396
2019	25,057	2,342	27,399	2019	79,635,902	99,420,309	179,056,211	$ 524,813,659
2020	26,340	763	27,100	2020	294,621,706	63,135,445	414,601,999	$ 617,384,900
2021	31,286	487	31,773	2021	752,108,172	84,472,069	836,580,241	$ 923,909,114
2022	32,646	283	32,929	2022	737,845,055	20,265,659	758,110,714	$ 678,034,557
Total	**283,922**	**31,127**	**315,046**		**2,332,977,910**	**1,246,394,679**	**3,636,217,437**	**$ 6,725,171,372.21**
Average	**28,392**	**3,113**	**31,346**	**Average**	**233,297,791**	**124,639,468**	**319,789,636**	**$ 672,517,137.22**
Median	**27,267**	**4,063**	**31,773**	**Median**	**79,635,902**	**92,093,628**	**344,108,254**	**$ 617,384,900.29**

[illegible]

[illegible]

[illegible]

Much of RJA's success can be attributed to the firm's commitment to its existing client base and the firm's [illegible] saving opportunities for its clients. RJA's philosophy is to develop long [illegible] or profitability. The State will have access to all of RJA's resources and can call upon their firm to fulfill any of its fin[illegible]

[illegible]	[illegible]
[illegible]	[illegible] N [illegible] M [illegible]
[illegible]	D[illegible]
[illegible] N[illegible]	508[illegible]871[illegible]866[illegible]
D[illegible]	[illegible]
D[illegible] C[illegible]	The Bank of New York Mellon ("BNYMellon") receives, maintains, [illegible] N[illegible]X[illegible]N[illegible] which is BNY's platform[illegible]
I[illegible]	[illegible] N[illegible]X[illegible]N[illegible] [illegible]
[illegible]	[illegible]
T[illegible] C[illegible]	C[illegible] 9 [illegible]
I[illegible] C[illegible]	[illegible]

The Bank of New York Mellon ("BNY Mellon") receives, maintains, and delivers securities and [illegible]

[illegible] 100 m[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

5 [illegible]

[illegible]

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

[illegible]

[illegible]

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

6 [illegible]

[illegible]

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

7 [illegible]

[illegible]

[illegible]

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

8 T[illegible]

[illegible]

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

9 [illegible]

[illegible]

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

10 [illegible]

[illegible]

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

11 MI□C□□□□N□□ □□

□□□□□□ □□□r□□□ M□□□□□□r□ □ □r□□□ □□□ □□r□□r□ □□□□□ □□□□□□ □ □□□r□□□□□□□d□r □ □□□d□□□□□□□□ □□d □ □□□□□□□□ □ □r□□ □r□ □□□□r□□□ □ □□□□□r r□□□□□□□□□□ □□r □□□r□□□□□□ □□d□r□ r□□□□□□□□□□□□□ □□d□r □□□ □□□r□□□□T□□ □□□□r□□□□ □□□□□r □ □□□□□ □□□□□□□□d□r□□ □□r□ □□□□□□□□□□□ □□□r□ □□ □ddr□□□ □□□ □□□□□□ □r □□r□□□ □r □□□□r □□□□□□ r□□□□d □□ □□□ □ □□□r□□□□□□□d□r □□□□d □□□□□□ □□□r□□□ □□□□□r □d □□□ □r □□r □□□□□□□ □□□□r□ □□□□□ □□□□□ □

□□□r□□□M□□□□□r□ D□□□r□□ □r□d

T□□□□□□□ N□□ □r□617□7□□9657

□□□ N□□ □r□617□7□□9660

E□ □□Addr□□□ D□□□r□□□r□d□ □□□□□□□□□□□□□□m

1□ □ □□T □I□□INI□ M□D□T□ □□ □TT□C□M□NT□

□□ □□□C□□□IN□ □□□ID□□IT
□□ □DD□ND□M □C□N□□ □□D□□M□NT □□□M
C□ C□NT□CT □ C□□TI□IC□TI□N

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 SLS Holdings, LLC

Authorized Signature: _____ Date: 01/24/24

State of VIRGINIA

County of FAIRFAX, to-wit:

Taken, subscribed, and sworn to before me this 24 day of JANUARY, 2024.

My Commission expires 10/31/27, 2027.

AFFIX SEAL HERE

DANIEL LOUIS WURZ
NOTARY PUBLIC
REG # 8085084
MY COMMISSION EXPIRES
10/31/2027
COMMONWEALTH OF VIRGINIA

NOTARY PUBLIC _____

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: CRFQ STO2400000003

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.

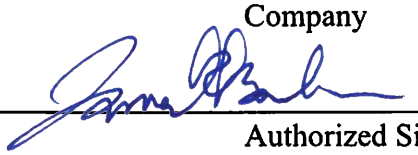
Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[x]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

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.

Avenu SLS Holdings, LLC
Company



Authorized Signature

01/24/24
Date

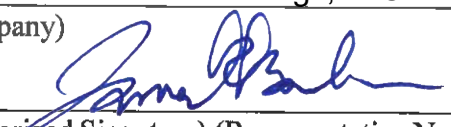
NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

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)

1□ □□□N□ □X□I□IT□

1□ C□□T□D□ C□I□NT □I□T

□□ □DDITI□N□□ □□□□□NN□□ □□□□M□□

□□ N□X□N□ □□□□□□NC□ □□ID□

□□ □XT□□N□T □□□□□□NC□ □□ID□

5□ □□□N□ □□□□□T□

6□ □□C1 □ND □□C□ □□□□□T□ – ***CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE***

7□ □□□IN□□□ C□NTIN□IT□ □□□N □***CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE***

8□ DI□□□T□□ □□C□□□□□ □□□N □***CONFIDENTIAL AND PROPRIETARY NOT FOR PUBLIC DISCLOSURE***

A□□□□□□ □ □□□□□□ □□□□□ S□□□□ Tr□□□□r□r
□□□□□□□ □d □r□□□r□□ □ □□□□□□

C□□d □ r□□□□C□M
D□□□□r□□ □□□□m□d □r□□□r□□ D□□□□□□
□□ □□□ □0□5□0
M□□□□m□r□□□□ □61□0

□□□□5□□□6□7□□□□□□□
C□□d□ r□□□□□ r□□□□r□□□□□m□□□□

□r□□d□d C□□□d□ □□r□□□□□016 □□r□□□□

□□□□□□□□□□□□ □□□□ □□□□ S□□□ Tr□□□r□r
□□□□□□□ □d □r□□□r□□ □ □□□□□□

M□□□□□ □□□□□□□□ □□□□□□ Tr□□□r□r

□ □□□□ □□□□ □□□□ Tr□□□r□r
□□□□d l□□r□ □□□d □ □□□□m□d □r□□□r□□
165 C□□□□□□□ □□□□
□□r□□rd□CT 06106

860□70□□□1□5 □□□□□□□
m□□□□□□□□□□□□□□ □□□□□

□r□□d□d C□□□d□ □□r□□□□□199□ □□r□□□□

□□□r□d□ □ □□□r□□ □□□□□□□□□□□□
□□□□□□□□ □□□ □□□□□□□□ □□□□□ □d □r□□□r□□ – E□□□□□

□r□□d□ □□M□□r□□□
D□□□□r□□ □□□□ □□□□m□d □r□□□r□□
C□r□□□□ r□□□□ □□□□ □□d□□□8□□ □□□r
8□0 N□□r□□□ □□r□□□
□ □m□□□□□□□D□ 19801

□0□577□8691 □□□□□□□
□r□□d□M□□r□□□ d□□□ r□□□□

□r□□d□d C□□□d□ □□r□□□□□1995 – □r□□□□

□□□r□d□ □ □□□r□□ □□□□□□□□□□□□□S□r□□□□
□□r□□□ □□□ □□□□□□ □d □r□□□r□□

□□□ T□□□m□□□□□□□□□dm□□□□r□□□r
D□□□□□□ □□□ □□□m□d □r□□□r□□
□ □□□□ □□C□□□□□□□□□□□ □□□r □mm□ □□r□□□
□□r□d□ D□□□r□m□□□□□□□□□□□□ □r□□□□

850□□1□□56□□ □□□□□□□□

□□□□□□□□□T□□□m□ M□□□r□d□C□□ □□m

□r□□d□d C□□□d□ □□r□□□□□009 □□r□□□□

□□□ □ **Tr□□□□r□r □□S□□□□**
□□□□□□□ □d □r□□□r□□ □ □□□□□□

□□r□□ □□□□□□
C□□□□□□□□□□□□

□□1 □ 1□□□ □r□□□□1□□□□□r

D□□ M□□□□□□□l□□□ 50□19

515□81□7677 □□□□□□□

□□r□□□□□□□□□□ □□□□□□□ □□□□□□

□r□□d□d C□□□d□ □□r□□□□□□ □019 □□r□□□□

□d□□□□ A□□r□□□ □ □□□r□□'□ □ □□□□□
□□□□□□□ □d □r□□□r□□ □ □□□□□□

□m□ T□□ □□dr□□

D□□□□r □□□ □□□□m□d □r□□□r□□ D□□□□□□
□□□ □□□□ □50□
□r□□□□ □□d□IN □61□□

□17□88□□□5□1 □□□□□□□□
□m□□□□□dr□□ □□□□□□□□□

□r□□d□d C□□□d□ □□r□□□□□1990 □□r□□□□

Ar□□□□□ □ □□□r□□ □□□□□□□ □□□□□□□
□□□□□□□ □d □r□□□r□□ □ □□□

□ □□N□□□□
□dm□□□□r□□r
1600 □ □M□□r□□
□□□□□□□□□□ 85007

60□716□60□□ □□□□□□□□
□□□□□□□ □□d□r□□□□

□r□□d□d C□□□d□ □□r□□□□□1990 □□r□□□□

□□□□ □r□ □ □□□r□□ □□□□□□□□□□□□
□□□□□□□□ □□□ □□□□□□□□ □□□□□ □d □r□□□r□□ – E□□□□□

□r□□d□ □□M□□r□□□
D□□□□r□□ □□□□ □□□□m□d □r□□□r□□
C□r□□□□ r□□□□ □□□□ □□d□□□8□□ □□□r
8□0 N□□r□□□ □□r□□□
□ □m□□□□□□□D□ 19801

□0□577□8691 □□□□□□□
□r□□d□M□□r□□□ d□□□ r□□□□

□r□□d□d C□□□d□ □□r□□□□□1995 – □r□□□□

□□□r□d□ □ □□□r□□ □□□□□□□□□□□□□S□r□□□□
□□r□□□ □□□ □□□□□□ □d □r□□□r□□

□□□ T□□□m□□□□□□□□□dm□□□□r□□□r
D□□□□□□ □□□ □□□m□d □r□□□r□□
□ □□□□ □□C□□□□□□□□□□□ □□□r □mm□ □□r□□□
□□r□d□ D□□□r□m□□□□□□□□□□□□ □r□□□□

850□□1□□56□□ □□□□□□□□

□□□□□□□□□T□□□m□ M□□□r□d□C□□ □□m

□r□□d□d C□□□d□ □□r□□□□□009 □□r□□□□

□ □□□□□ □□□□□ □□□□□□ S□□□ Tr□□□□r

□□□□□□□ □□□□□□□
□□d□r □□□□r□□□
900 □□ □□□□□□□□□□□□ □□□ □01
T□□□□□□□□□ 6661□

785□91□17□ □□□□□□□□
□□□□□□□□ r□□□□r□r□□□□□□

□r□□d□d C□□□d□ □□r□□□□□009 □□r□□□□

□d□□□□ A□□r□□□ □ □□□r□□'□ □ □□□□□
□□□□□□□ □d □r□□□r□□ □ □□□□□□

□m□ T□□ □□dr□□
D□□□□r □□□ □□□□m□d □r□□□r□□ D□□□□□□
□□□ □□□□ □50□
□r□□□□ □□d□IN □61□□

□17□88□□□5□1 □□□□□□□□
□m□□□□□dr□□ □□□□□□□□□

□r□□d□d C□□□d□ □□r□□□□□1990 □□r□□□□

[illegible] S[illegible] Tr[illegible]r[illegible]r [illegible]d [illegible]r[illegible] [illegible]r[illegible]r [illegible]r[illegible] M[illegible]r [illegible]m[illegible]d [illegible]r[illegible] D[illegible] 1050 [illegible] 1[illegible]7 [illegible] 100 [illegible]r[illegible]r[illegible] [illegible]0601 800[illegible]65[illegible]7[illegible] [illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]019[illegible]r[illegible]	M[illegible]r[illegible] M[illegible] T[illegible] Tr[illegible] M[illegible]r[illegible] [illegible]r[illegible] C[illegible]m[illegible]d [illegible]r[illegible]r[illegible] [illegible]m [illegible] M[illegible]d[illegible] 1[illegible]5 N[illegible]r[illegible]rd [illegible]r [illegible]MT 596[illegible]0 [illegible]06[illegible]008 [illegible] TM[illegible]r[illegible] m[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1990 – [illegible]r[illegible]
M[illegible]r[illegible]Tr[illegible]r[illegible] [illegible]d [illegible]r[illegible]r[illegible] T[illegible]rr[illegible] [illegible]dm[illegible]r[illegible] M[illegible]r [illegible]r [illegible]m[illegible]d [illegible]r[illegible]r[illegible] [illegible]X [illegible]0756 [illegible]MI [illegible]8909 517[illegible]6[illegible]6[illegible]5[illegible]07 [illegible] [illegible] m[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1990 – [illegible]r[illegible]	M[illegible] S[illegible] Tr[illegible]r[illegible]r[illegible] [illegible]d [illegible]r[illegible]r[illegible] [illegible]C[illegible] [illegible]D[illegible]r[illegible]r [illegible]r[illegible]r[illegible] [illegible]9 [illegible] 111 [illegible]r[illegible]rd [illegible] M[illegible] 0[illegible]00[illegible]9 [illegible]07[illegible]6[illegible]7[illegible]76 [illegible] [illegible]C[illegible] m[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1990 – [illegible]r[illegible]
M[illegible]r[illegible] [illegible] M[illegible]r C[illegible]m[illegible]r[illegible]r 60 C[illegible]m[illegible]r[illegible] [illegible]r[illegible]r[illegible]M[illegible] 0[illegible]18[illegible] 781[illegible]8[illegible]9[illegible]5651 [illegible] [illegible]r[illegible] m[illegible]r[illegible]m [illegible]r[illegible]d[illegible]d [illegible]r[illegible]01[illegible]r[illegible]	M[illegible]Tr[illegible]r[illegible] M[illegible] [illegible]r[illegible] A[illegible] N[illegible] [illegible]D[illegible]r[illegible]r [illegible]C[illegible] M[illegible]m[illegible]r[illegible] [illegible] Tr[illegible]r[illegible]r [illegible]r[illegible] [illegible]M[illegible] 0[illegible]108 617[illegible]67[illegible]9[illegible]19 [illegible] [illegible]r[illegible]m[illegible] [illegible]r[illegible]d[illegible]d [illegible]r[illegible]01[illegible]r[illegible]
M[illegible]r[illegible]S[illegible] Tr[illegible]r[illegible]r[illegible] M[illegible]r[illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible]r D[illegible]r[illegible]r [illegible]m[illegible]d [illegible]r[illegible]r[illegible] [illegible]10 [illegible]r[illegible] C[illegible]M[illegible] 6510[illegible] 57[illegible]751[illegible]08[illegible] [illegible]r[illegible]r[illegible] [illegible]r[illegible]r[illegible]r[illegible]m[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]019 [illegible]r[illegible]	N[illegible]d[illegible] S[illegible] Tr[illegible]r[illegible]r [illegible]d [illegible]r[illegible]r[illegible] D[illegible] D[illegible] Tr[illegible]r[illegible]r 555 [illegible] 5[illegible]00 [illegible]N[illegible] 89101 70[illegible]86[illegible]5[illegible] [illegible]d[illegible]r[illegible]r[illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]006 [illegible]r[illegible]
N[illegible]r[illegible] S[illegible]r[illegible]r [illegible]d [illegible]d[illegible] [illegible]r[illegible] [illegible]r[illegible] D[illegible]r[illegible]r [illegible] C[illegible]m[illegible]r[illegible]r 110 [illegible]r[illegible]8[illegible]r [illegible]N[illegible] 1[illegible]6 518[illegible]7[illegible]60[illegible]9 [illegible] [illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]016[illegible]r[illegible]	N[illegible] M[illegible] T[illegible]d [illegible]r[illegible] [illegible]d [illegible]r[illegible]r[illegible] [illegible] D[illegible]r[illegible]r 1[illegible]00 [illegible]r[illegible] Dr[illegible] [illegible]51[illegible] [illegible]NM 8750[illegible]51[illegible] 505[illegible]8[illegible]7[illegible]076[illegible] [illegible]d[illegible]m[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1990 [illegible]r[illegible]

AVENU INSIGHTS & ANALYTICS

S[illegible]N[illegible] Tr[illegible]r[illegible] A[illegible]d[illegible]d [illegible]r[illegible]r[illegible] [illegible]m[illegible] [illegible]d[illegible]d [illegible]r[illegible]r[illegible] D[illegible]r [illegible]5 C[illegible]r[illegible]m [illegible]05 C[illegible]rd[illegible]N[illegible] 0[illegible]01 60[illegible]71[illegible]1[illegible]99 [illegible] [illegible]m[illegible]r[illegible] [illegible]r[illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1998 – [illegible]r[illegible]	[illegible]r[illegible] S[illegible] Tr[illegible]r[illegible] [illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible]r[illegible] C[illegible]d[illegible] C[illegible] Tr[illegible]r[illegible]r[illegible] D[illegible]r[illegible]r 775 [illegible]mm[illegible]r [illegible]r[illegible]N[illegible] 100 [illegible]m[illegible] 97[illegible]01 50[illegible]986[illegible]5[illegible]8 [illegible] C[illegible]d[illegible]C[illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]015 – [illegible]r[illegible]
[illegible]r[illegible]d [illegible]r[illegible]r[illegible] [illegible] D[illegible] M[illegible]d[illegible]d[illegible] [illegible]d[illegible]C[illegible]r[illegible] [illegible]r[illegible] 600 [illegible]d[illegible] [illegible]1[illegible]9[illegible] [illegible] 00907[illegible]1[illegible]7 787[illegible]7[illegible]1[illegible]1 [illegible] [illegible]d[illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]005 – [illegible]r[illegible]	S[illegible]r[illegible]’[illegible] Tr[illegible]r[illegible]r’s [illegible] D[illegible] D[illegible]r [illegible] Tr[illegible]r[illegible]r 1[illegible]00 [illegible]r[illegible]– [illegible]1[illegible] [illegible]d[illegible]m[illegible]d[illegible] C[illegible]m[illegible]C [illegible]9[illegible]01 80[illegible]7[illegible]68[illegible] D[illegible]D[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]0[illegible]r[illegible]
T[illegible] S[illegible] Tr[illegible]r[illegible]r[illegible] [illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible]D[illegible]r[illegible]r [illegible]dr[illegible]d[illegible] 10[illegible]r N[illegible]TN [illegible]7[illegible]0[illegible] 615[illegible]5[illegible]5[illegible]5[illegible] [illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1990 [illegible]r[illegible]	[illegible]r[illegible] S[illegible] Tr[illegible]r[illegible]r [illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible]C[illegible]rd[illegible]r [illegible]d[illegible] 109 [illegible]r[illegible]r M[illegible]r[illegible]T 05609[illegible]6[illegible]00 80[illegible]8[illegible]8[illegible]18 [illegible] [illegible]r[illegible]rm[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]005 – [illegible]r[illegible]
[illegible]r[illegible]r[illegible] Tr[illegible]r[illegible]r [illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible]d[illegible]r[illegible]D[illegible]r[illegible]r 101 N[illegible]r[illegible] 1[illegible]r[illegible] [illegible]m[illegible] M[illegible]r[illegible]d[illegible]rd [illegible]r [illegible]m[illegible]d[illegible]19 80[illegible]5[illegible]515 [illegible] m[illegible]d[illegible]r[illegible]r[illegible]r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1998 [illegible]r[illegible]	[illegible]r[illegible]r[illegible]d[illegible] [illegible]r[illegible]r[illegible]r[illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible]r Tr[illegible]r[illegible]r 8[illegible]01 [illegible]rd [illegible]r [illegible]T[illegible]m[illegible]r[illegible] I[illegible]d[illegible]0080[illegible] C[illegible]d[illegible] [illegible]r[illegible]r[illegible]0[illegible]
[illegible]r[illegible] [illegible]d [illegible]r[illegible]r[illegible] [illegible]r[illegible] D[illegible]r[illegible]r[illegible]r[illegible]T[illegible]r[illegible] [illegible]1[illegible]5 [illegible]mr[illegible]d 6[illegible]0 M[illegible]d[illegible] I 5[illegible]71[illegible] 608[illegible]61[illegible]5[illegible]5 [illegible] [illegible]r[illegible] r[illegible] [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]1990 [illegible]r[illegible]	[illegible]r[illegible] S[illegible] Tr[illegible]r[illegible]r’[illegible] [illegible]d [illegible]r[illegible]r[illegible] [illegible]C[illegible]m[illegible] [illegible] M[illegible]r [illegible]m[illegible]d [illegible]r[illegible]r[illegible] [illegible] 70[illegible]r[illegible] C[illegible]r[illegible] [illegible]5[illegible]05 [illegible]0[illegible]0[illegible]711 [illegible] [illegible]m[illegible]m [illegible]r[illegible]d[illegible]d C[illegible]d[illegible] [illegible]r[illegible]016 – [illegible]r[illegible]

□dd□□□□□□□□r□□□□□□□ □□□m□□ □□r □□□□□’□ C□□□□□C□□□d□ T□□m

□dd□□□□□□m□m□□r□ □□□venu’s □□□m □□□□□□□□□ □□ □□□□ □T□ □r□ □□□□d □□□□□ □□□□□□’□ □□□m □□ □□□□ □□□□ □□□□□□□□□ □□ □□□□□□□□□ □T□ □□□□ □□□□ □□d □□□□□r□□□□□

M□r□□r□□A□□ □□□□r□□□□□S□r□□□□ □r□□□□□□□□□

□ □□□ □□□□□ □□□□ □010

M□r□□r□□“□□□” □ □□□□r □□ □ □□□□r □□□□□□□M□□□□□r r□□□□□□□□□□ □r □□d □□□ □□□□m□r □□□□□r□□□□□□ □□□□□□ □□ □ □□□□ □□□ □□r□□m□□□□m□□□□□□□r □□r□□□□□□

□□□ □□□ □dm□□□□r□m□□□□□□d □□d D□ □r□□□□□□□ r□□□□□□□□ □r □□□r□□□□d□ □□□□□□T□□□ r□□□□□□□□ □□d□ □□□r□ □□□m□d □□ □□□□□□□r□□□r□□□□□□d□□□□ □□□r□□□ □□d□□□□□ r□r□□□r□□□ r□□□□□□□r□□□□□□□□

□r□r □□ □□□□□□ □□□□□□□□ □□d □□□□□□□ □ □□□ □□□ r□□□□r □□□□□d□r□ □r m□ □□□□ □0 □□r□□□ □□d □□□d□ □r□r□□□□ □□□□□□□ □□C□m□□□r□□r□ □□ □ □□□□□□□ □ □□□T□□m □□□d□r□□ T□□□□□□□□ □r□□□□ T□□m □□□d□r□□ □□□□□m□C□□□r□□□ □□□□□□□□d □ □□□□□□□ □□d □r□d□□□□ □□□r□□□□□

□□□ □r□□□ □ □□□□□ □□□r□□□□r □□□□□ □□r□□□□□□r□□□d □□d□r□□ □□ □r r□□ □□□□□□□ □r□□□□□□□□ □□□ □ □□□□m□d □□□r□□□ C□□□d□ □□□m □□d □□□□□□□□ □□□□’□ □□□□d□ □□□□□□ □ □□ □r□ □□d □□□□ □d□□ □□□□□

□□□r□ M□□□□□ □□□□□S□r□□□□ □r□□□□□□□□□

□ □□□ □□□□□ □□□□ □001 – □ □□□□□ M□

□□□r□ □□ □□ □ □□□□□□□M□□□□□r □□□□□ □□□ □ □□□□m□d □□□□r□□□ C□□□d□ □□□m r□□□□□□□□□ □r □□□ m□□□□m□□□□□□□r□□□□□ □□□□□r□□□□□□□□ □□□ □r□□d□□ d□□□ r□□□□r □□d r□□□□□□□□□□□ □□□□□□r□□□□□□□□m□ □r□□□□□□□r□□□r□□□r□□m r□□□□□□□□ □□d □□□□r □□□□□ r□□□□d □□ □□d□□□□m□□□□□ □r□□□□□□ □ □□□□□□□□ □□□□□□m□d □r□□□r□□□

□□□r□ □□□□d □□□□□ □□ □001 □□□r□□□ □□r □□r□r □□ □m□□□□□r □□ □□□□ D□□□□r□ D□□□r□m□□□□ □□□r□ □□□□ □□m□□□d d□□□m□□□□□□□ □□□□d□d □□r □□□□ □□□□□□□d□□□□r□ □□d □□□□□r□d□□□□r□ □□□□□□□r□□□□ □□ □□□□□□□□□ □□r □□□□□r□□□□□ DTC□□□□□□□□□□□□r□□□□□□□□□ □□d D□ □M□ □□□□□m□□□□□

□□□□r□ □r□□r□□□□d □□ □□□□ □ □□□□□m□d □□□□r□□□□ C□□□d□ □□□m □□□□d □□□ □□r □r□□□□ □□□□□ □□d□□ □□d □□□□□r□□□d□ □□□r□ □□□□ □□□□□ □ □□□ □□□□□ □□□□□ □□□□□m□r □□□001 □□d □r□□d□□ d□□□ □□□□□□□□□□□□ □□r □□□□□□□ □□ □□□□□r□□□□□r □□□□□□m□d □r□□□r□□ □r□□r□m □□d r□□□□□□□□□□□□□ □□□□□□r□□□□ □□d M□□□□□□□□□d□ r□m □□d□r□ □□□□ □□□□rd□□□□□□ □□□□ □□□□□ □□□□□□□r□□□□□□□□□m □r□□□□□□□□r□□□□r□□ □□d □r□□□□m r□□□□□□□□□□

□□□□r□ □□r□□d □bachelor’s degree □□ □□□□□□□□□ □ □□□□□□□□□□□ □□ 198□ r□m Tr□□□□ □ □□□□r□□□□□□□□□□

□□□□ □□□□□□□ □□□□□□ □r □□r□A□□□□□□□□□ □□

□ □□□ □□□□□ □□□□□ □019 – □ □□□□□□M□

□□□□C□□□ □□ □C□□□□m□r C□r□ □□□□□□□□□□r□□□□□□□□□□ □□r □□□□d□□□ □□□□□□r□□□□□□□□□ □□□□□□□□□□□□d□□□□m □□□□□□ □□□d r□□□□□□□□□□□□ □□□ □ □□□□□□ □□r□□□□ □□□ □□□□ □□□□□□□□r□□□□□r□□ □□r □□□□□r□□□□□r□□□□□□□□□□□□□□dd□□□□□□□ □□r□□□□□ □□□□d□d □□□ □□□□ □□□□□□d □□ □□r□r□□□ □□□□□□□□□□r□□□□□□□□□d r□□□□□□□□□□□□ □□□□□□□r□□□□ □□□m □□d□r□□□□□□ □□□□□□□r□□□□ □□d □□□□m □r□□□□□□□□□□ m□□□□□m□□□□m□□□□□d □r□□□□m r□□□□□□□□□□□□

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Robinson’s background includes trading financial markets. He facilitated the opening of self[illegible]

[illegible]

[illegible]

[illegible]

Borana Pjetri is a Client Service Associate III of Avenu’s Unclaimed Securities Custody group and is [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

M[illegible] S[illegible]

[illegible] 00[illegible]

[illegible] 00 M[illegible] [illegible] [illegible] [illegible] [illegible] M[illegible] [illegible] Tr[illegible] C[illegible] [illegible] [illegible] [illegible] [

N□X□N□ □□□□r□□□□ □ □□d□

AVENU
INSIGHTS & ANALYTICS

NEXEN®
Reference Guide

Request Trades and Monitor
Transactions of Your Unclaimed
Securities Portfolio Online

September 2021

AVENU
INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

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.

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

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

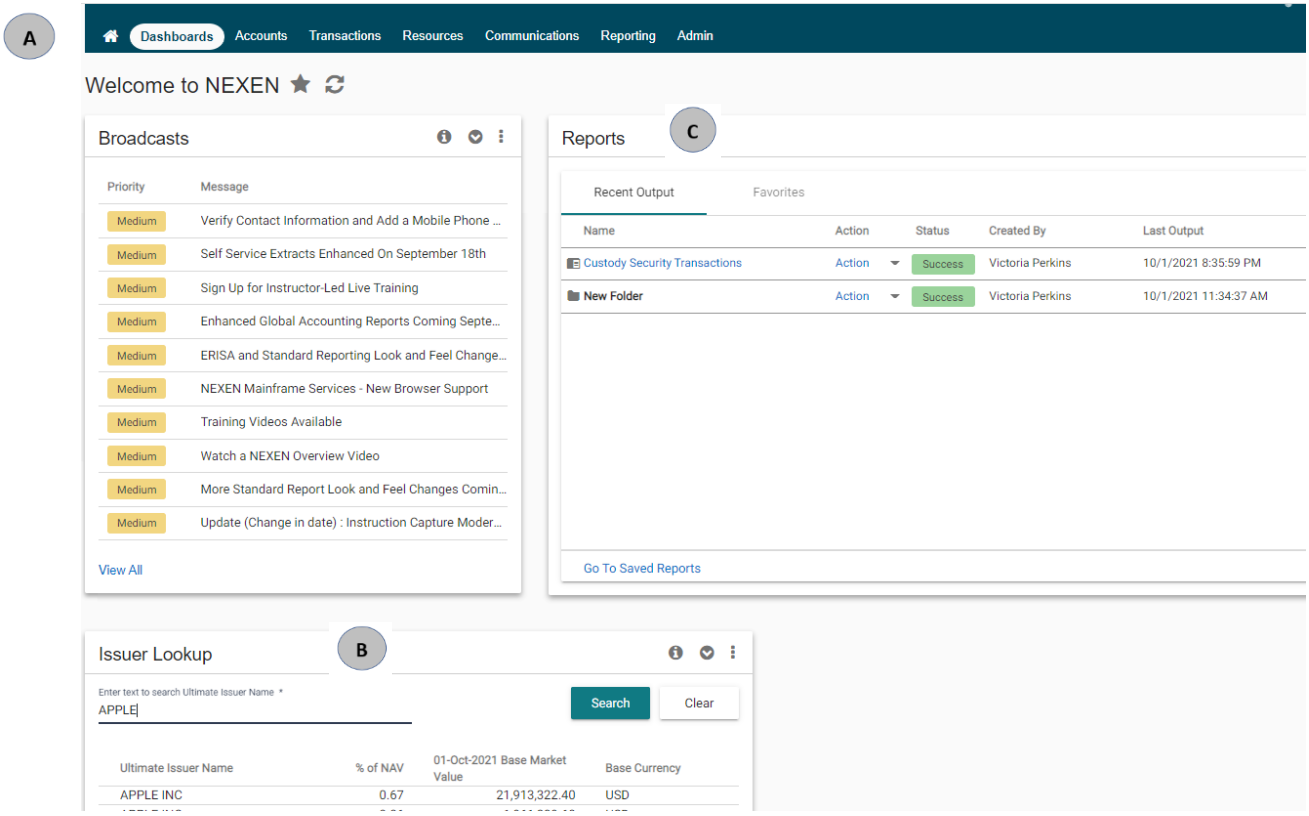
Table of Contents

Contents

NEXEN® Homepage

State clients will have authorized access to NEXEN®. 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.



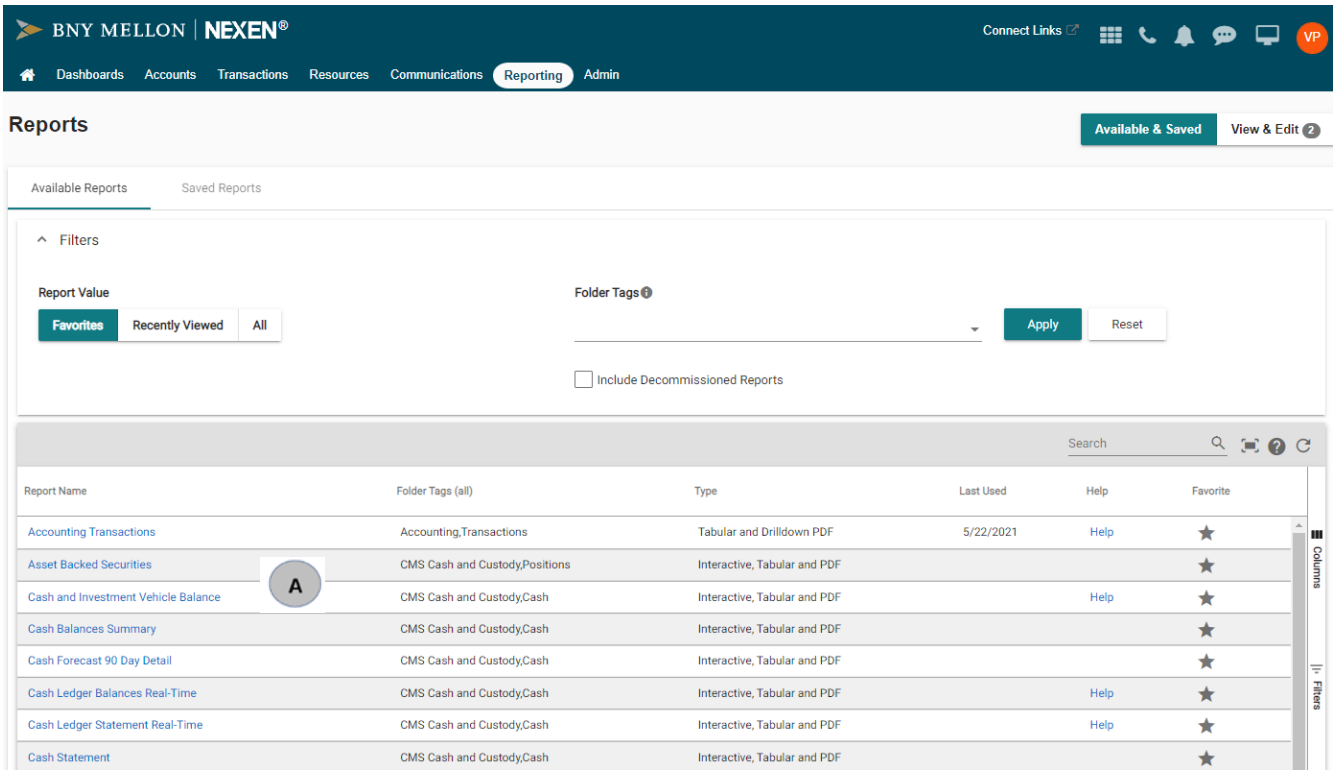
A Reporting Options Tool Bar

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®. 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® 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.

AVENU INSIGHTS & ANALYTICS

Custody Holdings
By Security - Details By Status

Report ID: ICUS0016

99999 - AUZF STATE 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 Deliver Shares/Par
US20461S1087	COMPOSITE TECHNOLOGY CORP USD 0.001	USD	US	AVAILABLE	NIB	NIB8	16,250.0000	16,250.0000		
US2057503003	COMSTOCK MNG INC USD 0.000666	USD	US	AVAILABLE	DTC	DTC	2.0000	2.0000		
US2057634022	COMSTOCK P COMSTOCK CAPITAL VALUE F	USD	US	AVAILABLE	MUT	MAC		100.3370		100.3370
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	DTC	DTC	430.0000	430.0000		
				AVAILABLE	NIB	NIB8	101.6630	101.6630		
US20602D1019	CONCENTRIX CORP USD 0.0001	USD	US	AVAILABLE	DTC	DTC	132.0000	132.0000		
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

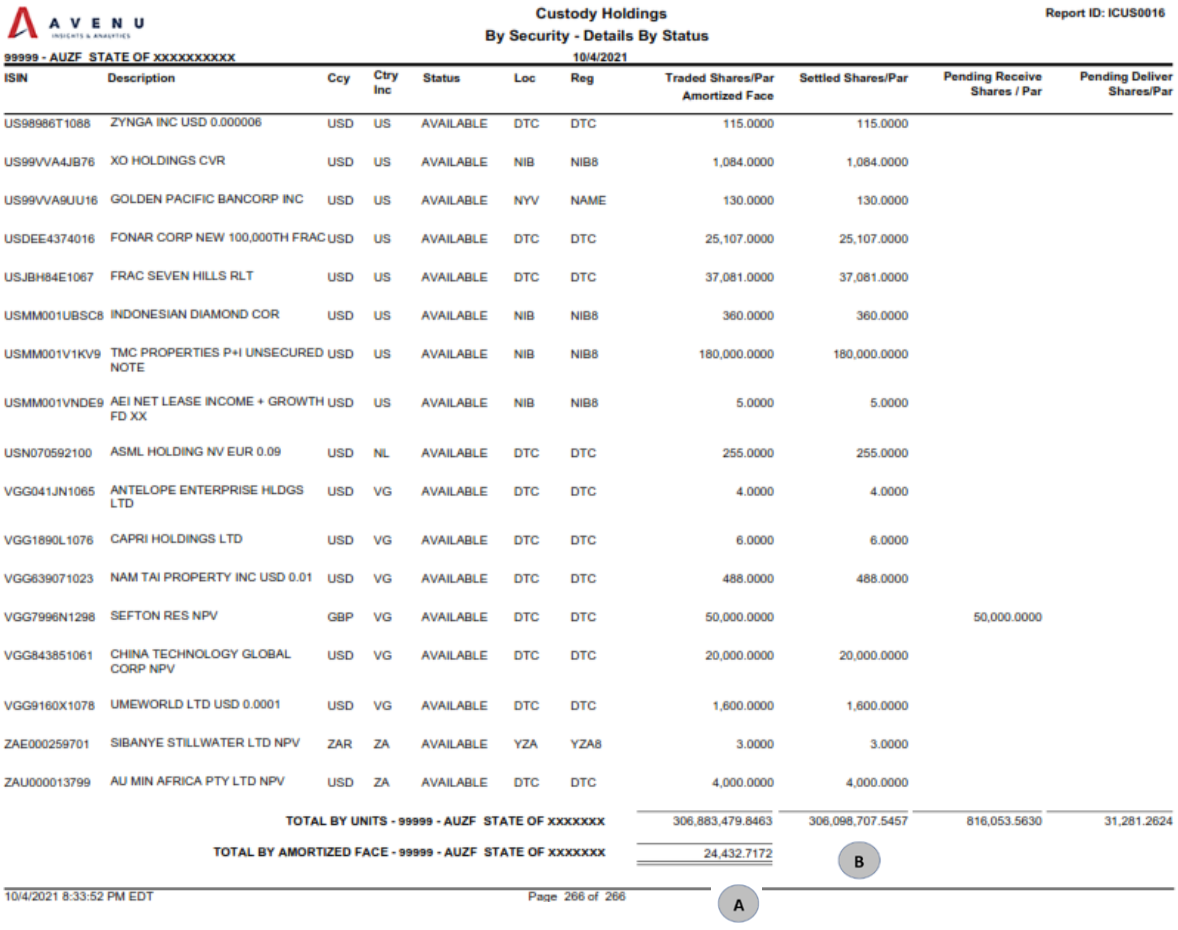
B Shows Pending Trades (Delivery and Receipt)

C Total Share Amount for Traded and Settled Positions

D 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.



AVENU INSIGHTS & ANALYTICS

Custody Holdings
By Security - Details By Status

Report ID: ICUS0016

99999 - AUZF STATE OF XXXXXXXXXX — 10/4/2021

ISIN	Description	Ccy	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 FRAC	USD	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	USD	US	AVAILABLE	NIB	NIB8	180,000.0000	180,000.0000		
USMM001VNDE9	AEI NET LEASE INCOME + GROWTH FD XX	USD	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		
	TOTAL BY UNITS - 99999 - AUZF STATE OF XXXXXXX						306,883,479.8463	306,098,707.5457	816,053.5630	31,281.2624
	TOTAL BY AMORTIZED FACE - 99999 - AUZF STATE OF XXXXXXX						24,432.7172	B		

10/4/2021 8:33:52 PM EDT — Page 266 of 266 — A

A Total Share Amount Including Pending and Actually Settled Shares

B Total Share Amount Actually Settled

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

AVENU INSIGHTS & ANALYTICS

Custody Valuation
By Asset Type

Report ID: ICUS0017
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXXX

Posted Basis - 10/12/2021

ISIN (A)	Description	Ctry Inc	Loc (B)	Ccy	Units / Amortized Face	Local Price	Market Value Local	Market Value Reporting Currency
EQUITIES								
AUSTRALIAN DOLLAR (Exchange Rate : 0.7357500000)								
AU000000LSA2	LACHLAN STAR LTD NPV	AU	YAS	AUD	40,000.0000	0.030000	1,200.00	882.90
CANADIAN DOLLAR (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
(A)	**TOTAL BY UNITS - CANADIAN DOLLAR**				**292,622.0000**		**203,161.81**	**163,110.14**
(A)	**TOTAL BY AMORTIZED FACE - CANADIAN DOLLAR**				**0.0000**			
EURO (Exchange 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 AMORTIZED FACE - EURO**				**0.0000**			
HONG KONG DOLLAR (Exchange Rate : 0.1285220000)								
BMG524181036	KERRY LOGISTICS NETWORK LTD HKD 0.5	BM	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 UNITS - HONG KONG DOLLAR				**380.0000**		**7,817.50**	**1,004.72**
	TOTAL BY AMORTIZED FACE - HONG 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
BMG9618E1075	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

AVENU INSIGHTS & ANALYTICS

Custody Valuation
By Asset Type

Report ID: ICUS0017
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXXXXXX — Posted Basis - 10/12/2021

ISIN	Description	Ctry Inc	Loc	Ccy	Units / Amortized Face	Local Price	Market Value Local	Market Value Reporting Currency
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		
US98986T1088	ZYNGA INC USD 0.000006	US	DTC	USD	1.0000	7.330000	7.33	7.33
X9X9USDDGCM3	DREYFUS GOVT CM INST 289	US	GSF	USD	12,277.0400	1.000000	12,277.04	12,277.04
	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**			
	TOTAL BY UNITS - EQUITIES				**4,269,153.5720**			**12,821,881.05**
	TOTAL BY AMORTIZED FACE - EQUITIES				**0.0000**			
MISC DEBT								
UNITED STATES DOLLAR (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**			
	TOTAL BY UNITS - MISC DEBT				**898.0000**			**26,371.04**
	TOTAL BY AMORTIZED FACE - MISC DEBT				**0.0000**			
	TOTAL BY UNITS - ACCOUNT 999999 - AUZF STATE OF XXXXXXX				**4,270,051.5720**	A	B	**12,848,252.09**
	TOTAL BY AMORTIZED FACE - ACCOUNT 999999 - AUZF STATE OF XXXXXXX				**0.0000**			

A — Total Share Amount for Settled Shares

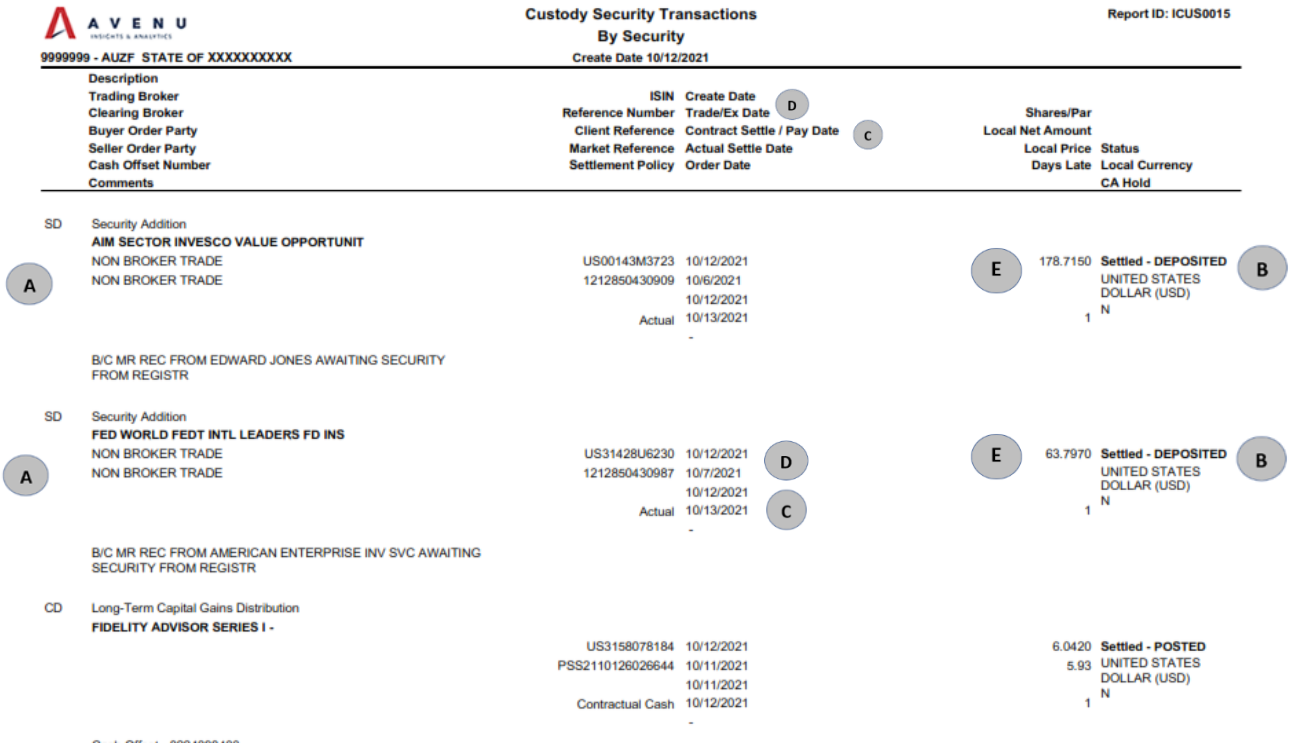
B — Total Market Value for Securities Held as of Report Date

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®.



AVENU INSIGHTS & ANALYTICS

Custody Security Transactions
By Security

Report ID: ICUS0015

9999999 - AUZF STATE OF XXXXXXXXXX
Create Date 10/12/2021

	Description / Trading Broker / Clearing Broker / Buyer Order Party / Seller Order Party / Cash Offset Number / Comments	ISIN / Reference Number / Client Reference / Market Reference / Settlement Policy	Create Date / Trade/Ex Date (D) / Contract Settle / Pay Date (C) / Actual Settle Date / Order Date	Shares/Par / Local Net Amount / Local Price / Days Late	Status / Local Currency / CA Hold
SD	Security Addition **AIM SECTOR INVESCO VALUE OPPORTUNIT** NON BROKER TRADE NON BROKER TRADE (A) B/C MR REC FROM EDWARD JONES AWAITING SECURITY FROM REGISTR	US00143M3723 1212850430909 Actual	10/12/2021 10/6/2021 10/12/2021 10/13/2021 -	178.7150 (E) 1	**Settled - DEPOSITED** (B) UNITED STATES DOLLAR (USD) N
SD	Security Addition **FED WORLD FEDT INTL LEADERS FD INS** NON BROKER TRADE NON BROKER TRADE (A) B/C MR REC FROM AMERICAN ENTERPRISE INV SVC AWAITING SECURITY FROM REGISTR	US31428U6230 1212850430987 Actual	10/12/2021 (D) 10/7/2021 10/12/2021 10/13/2021 (C) -	63.7970 (E) 1	**Settled - DEPOSITED** (B) UNITED STATES DOLLAR (USD) N
CD	Long-Term Capital Gains Distribution **FIDELITY ADVISOR SERIES I -**	US3158078184 PSS2110126026644 Contractual Cash	10/12/2021 10/11/2021 10/11/2021 10/12/2021 -	6.0420 5.93 1	**Settled - POSTED** UNITED STATES DOLLAR (USD) N

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

AVENU INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

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.

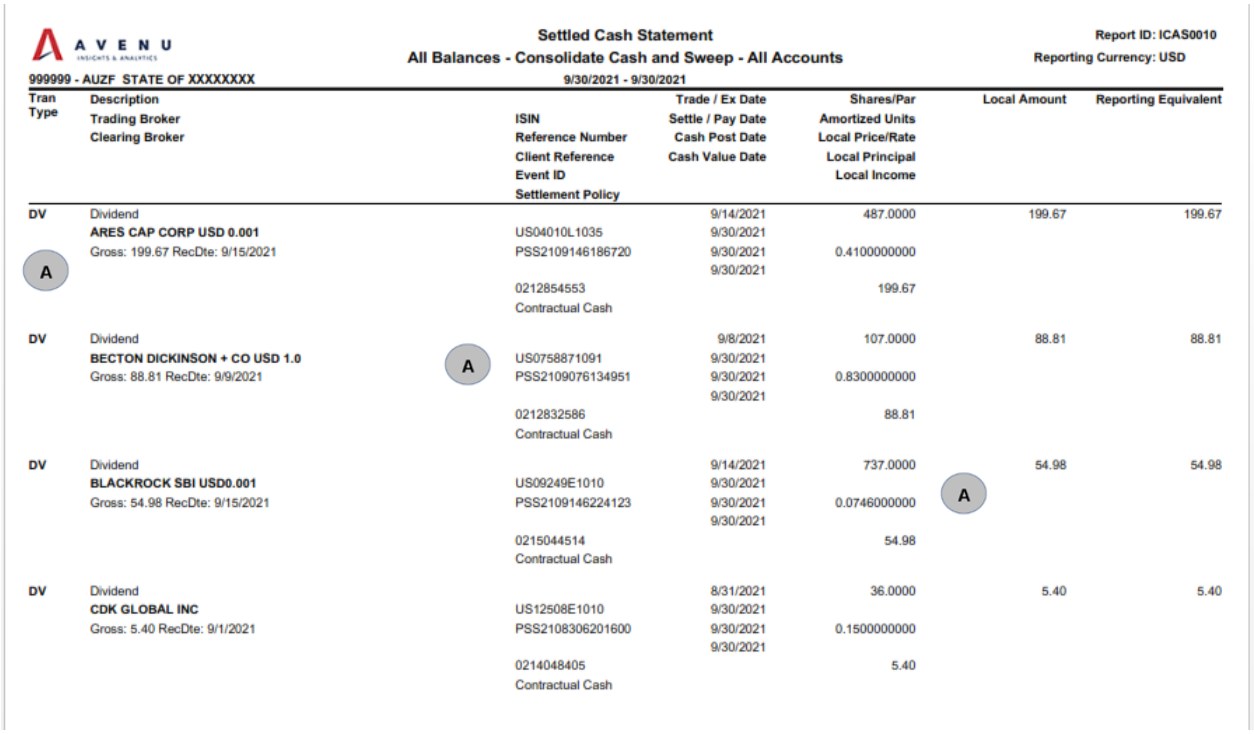
Cash Inquiry

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®

AVENU INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

Settled Cash Statements



AVENU INSIGHTS & ANALYTICS

Settled Cash Statement
All Balances - Consolidate Cash and Sweep - All Accounts
9/30/2021 - 9/30/2021

Report ID: ICAS0010
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXX

Tran Type	Description / Trading Broker / Clearing Broker		ISIN / Reference Number / Client Reference / Event ID / Settlement Policy	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
DV	Dividend			9/14/2021	487.0000		199.67	199.67
	ARES CAP CORP USD 0.001		US04010L1035	9/30/2021				
	Gross: 199.67 RecDte: 9/15/2021		PSS2109146186720	9/30/2021	0.4100000000			
A				9/30/2021				
			0212854553		199.67			
			Contractual Cash					
DV	Dividend			9/8/2021	107.0000		88.81	88.81
	BECTON DICKINSON + CO USD 1.0	A	US0758871091	9/30/2021				
	Gross: 88.81 RecDte: 9/9/2021		PSS2109076134951	9/30/2021	0.8300000000			
				9/30/2021				
			0212832586		88.81			
			Contractual Cash					
DV	Dividend			9/14/2021	737.0000		54.98	54.98
	BLACKROCK SBI USD0.001		US09249E1010	9/30/2021		A		
	Gross: 54.98 RecDte: 9/15/2021		PSS2109146224123	9/30/2021	0.0746000000			
				9/30/2021				
			0215044514		54.98			
			Contractual Cash					
DV	Dividend			8/31/2021	36.0000		5.40	5.40
	CDK GLOBAL INC		US12508E1010	9/30/2021				
	Gross: 5.40 RecDte: 9/1/2021		PSS2108306201600	9/30/2021	0.1500000000			
				9/30/2021				
			0214048405		5.40			
			Contractual Cash					

A Details by Transaction

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

AVENU INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

Settled Cash Balances

AVENU INSIGHTS & ANALYTICS

Settled Cash Balances
All Balances - Consolidate Cash and Sweep - All Accounts
9/30/2021 - 9/30/2021

Report ID: ICAS0008
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXX

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	**22**	**2,958.33**	**37.67**	**2,996.00**		**2,958.33**	**37.67**	**2,996.00**
UNITED STATES DOLLAR (USD) AUZF STATE OF XXXXXXXX - 999999999								
9/30/2021	26	7,377.33	489.11	7,866.44	1.0000000000	7,377.33	489.11	7,866.44
Period Summary	**26**	**7,377.33**	**489.11**	**7,866.44**		**7,377.33**	**489.11**	**7,866.44**
BACK VALUED AMOUNT				**0.01**				
TOTAL CASH AND SWEEP						**10,339.34**	**523.39**	**10,862.73**

A

B

AVENU INSIGHTS & ANALYTICS

Settled Cash Balances
All Balances - Consolidate Cash and Sweep - All Accounts
9/30/2021 - 9/30/2021

Report ID: ICAS0008
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXX

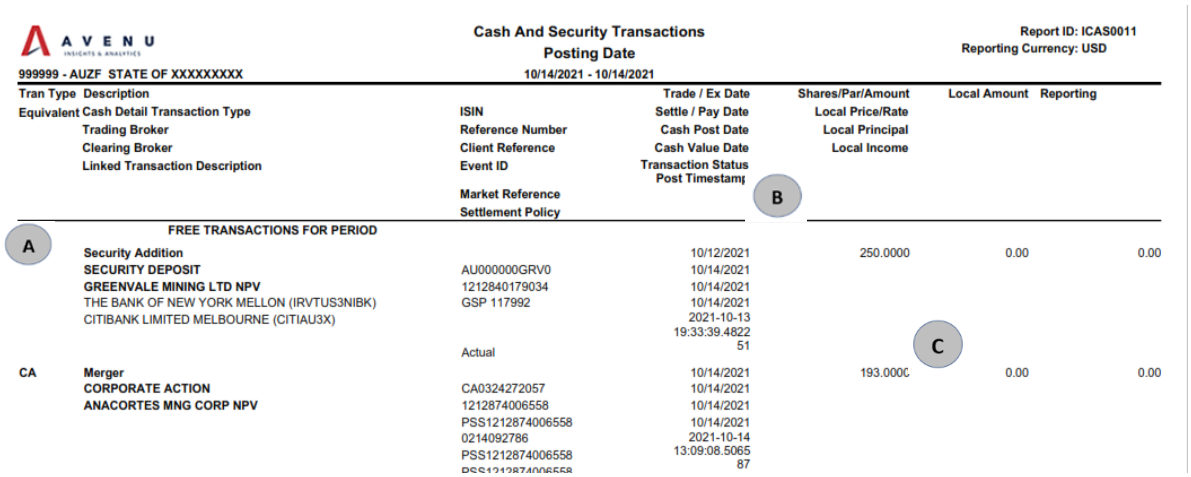
Date	Count	Beginning Balance Local	Net Activity Local	Ending Balance Local	Exchange Rate Reporting Currency	Beginning Balance Reporting Currency	Net Activity Reporting Currency	Ending Balance Reporting Currency
Period Summary	**0**	**0.00**	**0.00**	**0.00**		**0.00**	**0.00**	**0.00**
NEW ISRAELI SHEKEL (ILS) AUZF STATE OF XXXXXXXX - 999999999								
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 (ILS) AUZF STATE OF XXXXXXXX - 999999999								
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 STATE OF XXXXXXX - 999999999								
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 STATE OF XXXXXXX - 999999999								
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**
POUND STERLING (GBP) AUZF STATE OF XXXXXXX - 999999999								
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 -999999999								
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**

A Beginning Balance Details

B Ending Balance Details

AVENU INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

Cash & Security Transactions



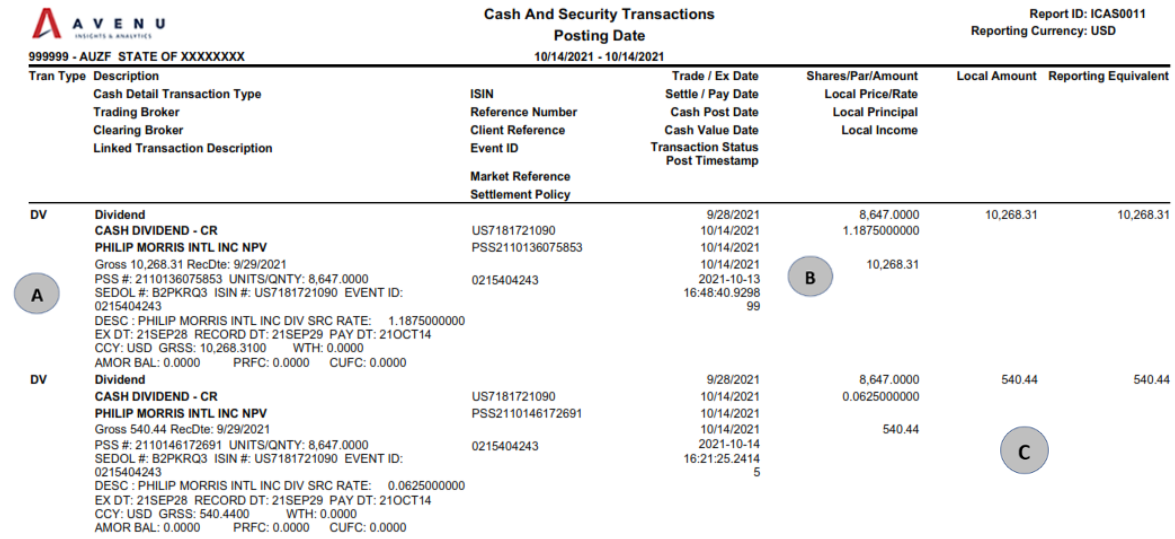
AVENU INSIGHTS & ANALYTICS

Cash And Security Transactions
Posting Date
10/14/2021 - 10/14/2021

Report ID: ICAS0011
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXX

Tran Type	Description / Equivalent			Trade / Ex Date	Shares/Par/Amount	Local Amount	Reporting
	Cash Detail Transaction Type	ISIN		Settle / Pay Date	Local Price/Rate		
	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			
		Market Reference					
		Settlement Policy					
	FREE TRANSACTIONS FOR PERIOD						
	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 19:33:39.4822 51			
		Actual					
CA	**Merger**			10/14/2021	193.0000	0.00	0.00
	CORPORATE ACTION	CA0324272057		10/14/2021			
	ANACORTES MNG CORP NPV	1212874006558		10/14/2021			
		PSS1212874006558		10/14/2021			
		0214092786		2021-10-14 13:09:08.5065 87			
		PSS1212874006558					



AVENU INSIGHTS & ANALYTICS

Cash And Security Transactions
Posting Date
10/14/2021 - 10/14/2021

Report ID: ICAS0011
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXX

Tran Type	Description			Trade / Ex Date	Shares/Par/Amount	Local Amount	Reporting Equivalent
	Cash Detail Transaction Type	ISIN		Settle / Pay Date	Local Price/Rate		
	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			
		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		
	PSS #: 2110136075853 UNITS/QNTY: 8,647.0000	0215404243		2021-10-13 16:48:40.9298 99			
	SEDOL #: B2PKRQ3 ISIN #: US7181721090 EVENT ID: 0215404243						
	DESC : PHILIP MORRIS INTL INC DIV SRC RATE: 1.1875000000						
	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						
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	0215404243		2021-10-14 16:21:25.2414 5			
	SEDOL #: B2PKRQ3 ISIN #: US7181721090 EVENT ID: 0215404243						
	DESC : PHILIP MORRIS INTL INC DIV SRC RATE: 0.0625000000						
	EX DT: 21SEP28 RECORD DT: 21SEP29 PAY DT: 21OCT14						
	CCY: USD GRSS: 540.4400 WTH: 0.0000						
	AMOR BAL: 0.0000 PRFC: 0.0000 CUFC: 0.0000						

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

AVENU INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

Cash Inquiry

AVENU INSIGHTS & ANALYTICS

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

Report ID: ICAS0021
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXX

Opening Balance					**Opening Balance** 0.00	**Reporting Equivalent Opening Balance** 0.00
South African Rand (ZAR) AUZF STATE OF XXXXXXXXX- 9999999999 Exchange Rate 0.0683964119						
Opening Balance				A	**Opening Balance** 0.00	**Reporting Equivalent Opening Balance** 0.00
Swedish Krona (SEK) AUZF STATE OF XXXXXXXXX - 9999999999 Exchange Rate 0.1160840216						
Opening Balance					**Opening Balance** 0.00	**Reporting Equivalent Opening Balance** 0.00
Swedish Krona (SEK) AUZF STATE OF XXXXXXXXX - 9999999999 Exchange Rate 0.1160840216						
Opening Balance					**Opening Balance** 0.00	**Reporting Equivalent Opening Balance** 0.00
Swiss Franc (CHF) AUZF STATE OF XXXXXXXXX - 9999999999 Exchange Rate 1.0834823121						
Opening Balance				A	**Opening Balance** 0.00	**Reporting Equivalent Opening Balance** 0.00
Swiss Franc (CHF) AUZF STATE OF XXXXXXXXX - 9999999999 Exchange Rate 1.0834823121						
Opening Balance					**Opening Balance** 0.00	**Reporting Equivalent Opening Balance** 0.00
United States Dollar (USD) AUZF STATE OF XXXXXXXXXX- 9999999999 Exchange Rate 1.0000000000						
Opening Balance					**Opening Balance** 2,021.48	**Reporting Equivalent Opening Balance** 2,021.48
Settled Transactions						
Transaction Type	**ISIN**	**Update Date - Timestamp Reference Number Event ID**	**Posted Date Value Date**	**Shares/Par 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	10/14/2021	0.00		
		0216535757	10/14/2021			
			Total CORPORATE 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			

AVENU INSIGHTS & ANALYTICS

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

Report ID: ICAS0021
Reporting Currency: USD

999999 - AUZF STATE OF XXXXXXXX

PHILIP MORRIS INTL INC NPV		10/14/2021 04:12 PM		101.00	6.31	6.31
	US7181721090	PSS2110146170854	10/14/2021	0.00		
		0215404243	10/14/2021			
PHILIP MORRIS INTL INC NPV		10/14/2021 04:10 PM		0.00	-126.25	-126.25
	US7181721090	PSS2110146165245	10/14/2021	0.00		
			10/14/2021			
NORDIC AMERICAN TANKER LTD 0.01 USD		10/14/2021 10:16 AM		445.00	4.45	4.45
	BMG657731060	PSS2109226102955	10/14/2021	0.00	C	
		0214323960	10/14/2021			
TAIWAN SEMICONDUCTOR M TWD 10.0 ADR		10/13/2021 08:00 PM		132.00	51.23	51.23
	US8740391003	PSS2109156147295	10/14/2021	0.00		
		0210976027	10/14/2021			
PHILIP MORRIS INTL INC NPV		10/13/2021 08:00 PM		0.00	126.25	126.25
	US7181721090	PSS2109276169396	10/14/2021	0.00		
			10/14/2021			
			Total DIVIDEND:		1,000.41	1,000.41
			Total Settled Transactions	B	1,016.93	1,016.93
			Projected Ending Balance		21,553.12	21,553.12

A Opening Balance for Each Currency Type

B Ending Cash Balance

C Cash Deposited into the Account for Specified Transaction Type

AVENU INSIGHTS & ANALYTICS
succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

AVENU
INSIGHTS & ANALYTICS

The Extranet
Reference Guide

An Online Portal for
Managing Your Unclaimed
Securities Portfolio

September 2021

AVENU
INSIGHTS & ANALYTICS

succeed@avenuinsights.com
5860 Trinity Parkway #120 | Centreville, VA 20120

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.

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

2. Table of Contents

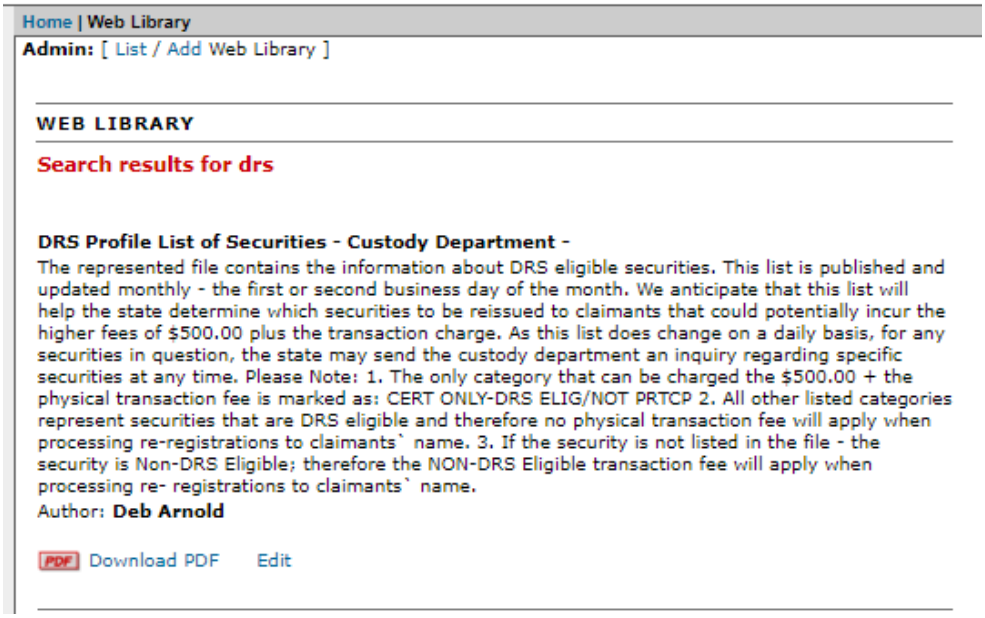
3. Navigating the System

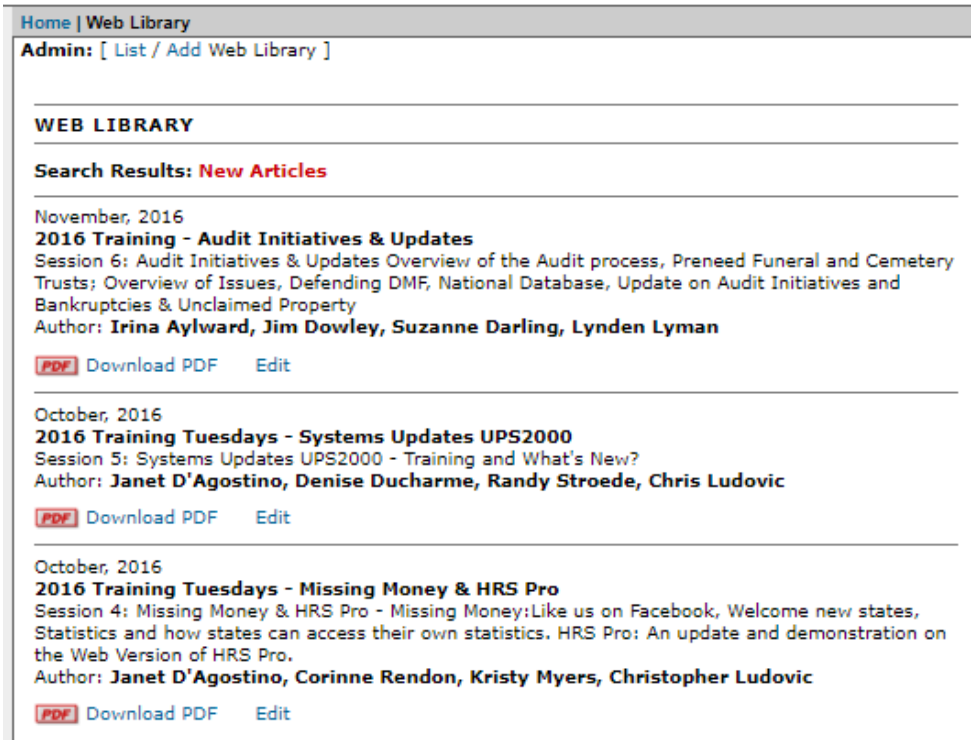
After logging on to the Extranet via our web-based system, www.unclaimedproperty.com the user will be presented with an easy-to-use side navigation bar that provides access to all sub-sections of the Extranet. Access to the different sections within the site will be controlled by a unique user login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

Web Library:	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.

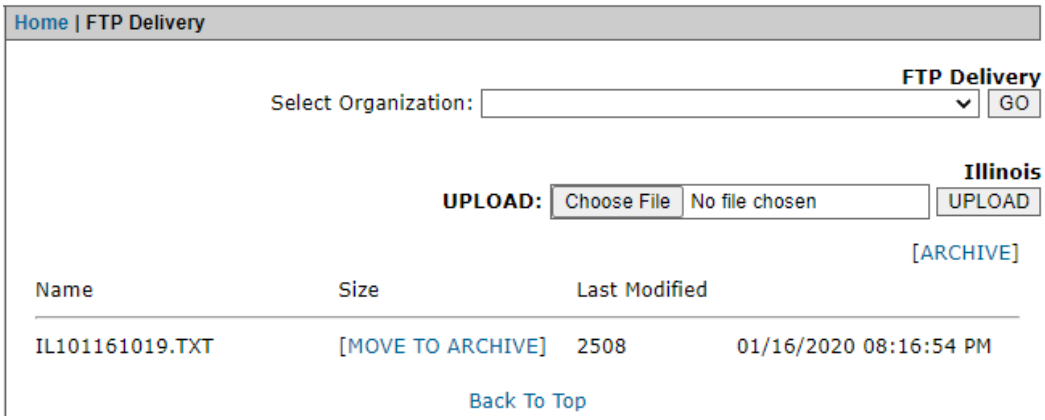




5. FTP Delivery

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.



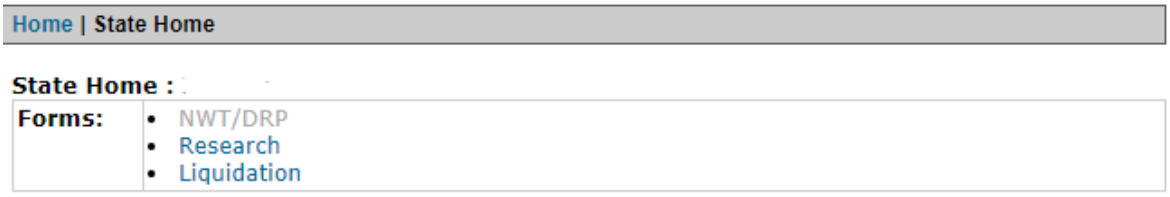
6. State Home

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:

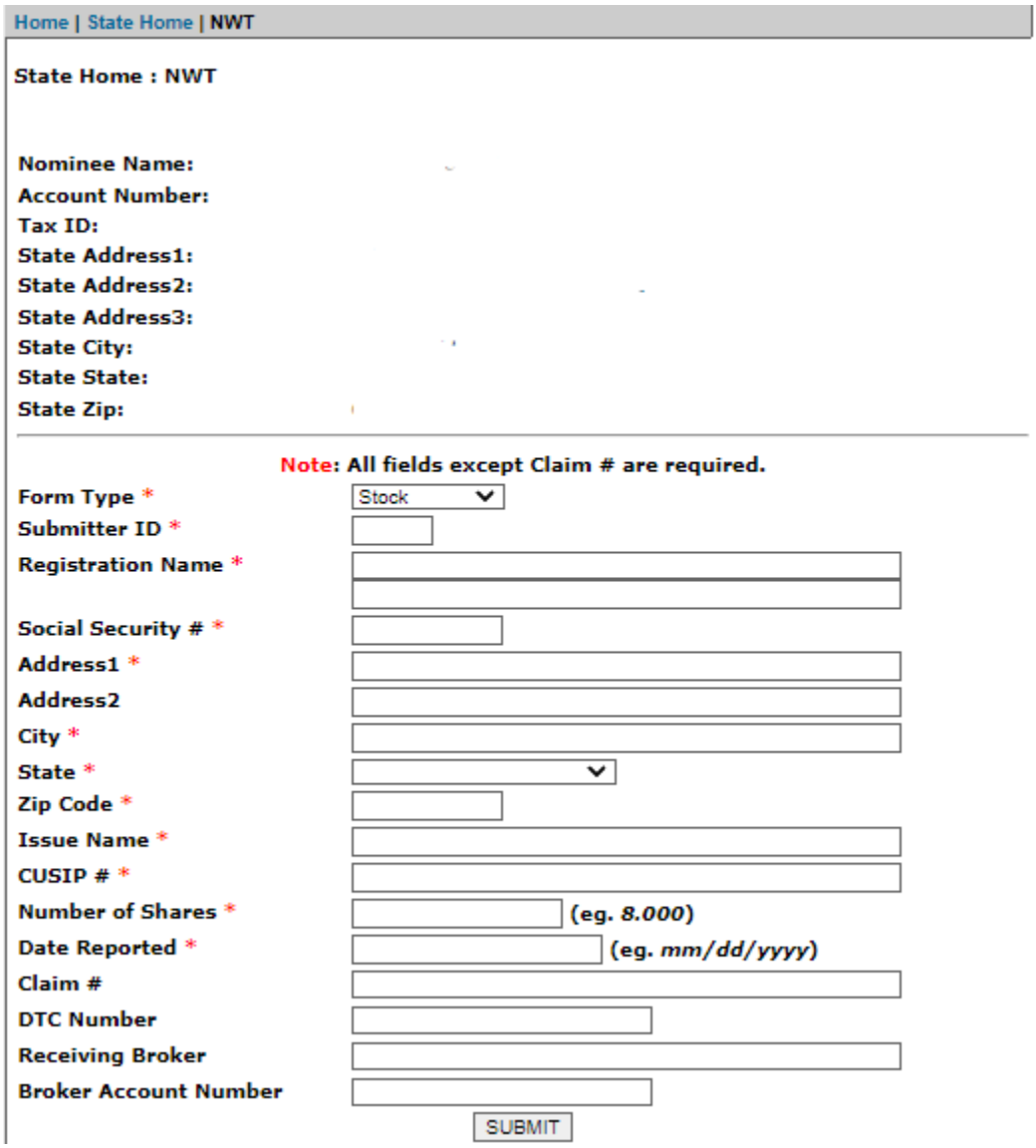


State Home - NWT

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:

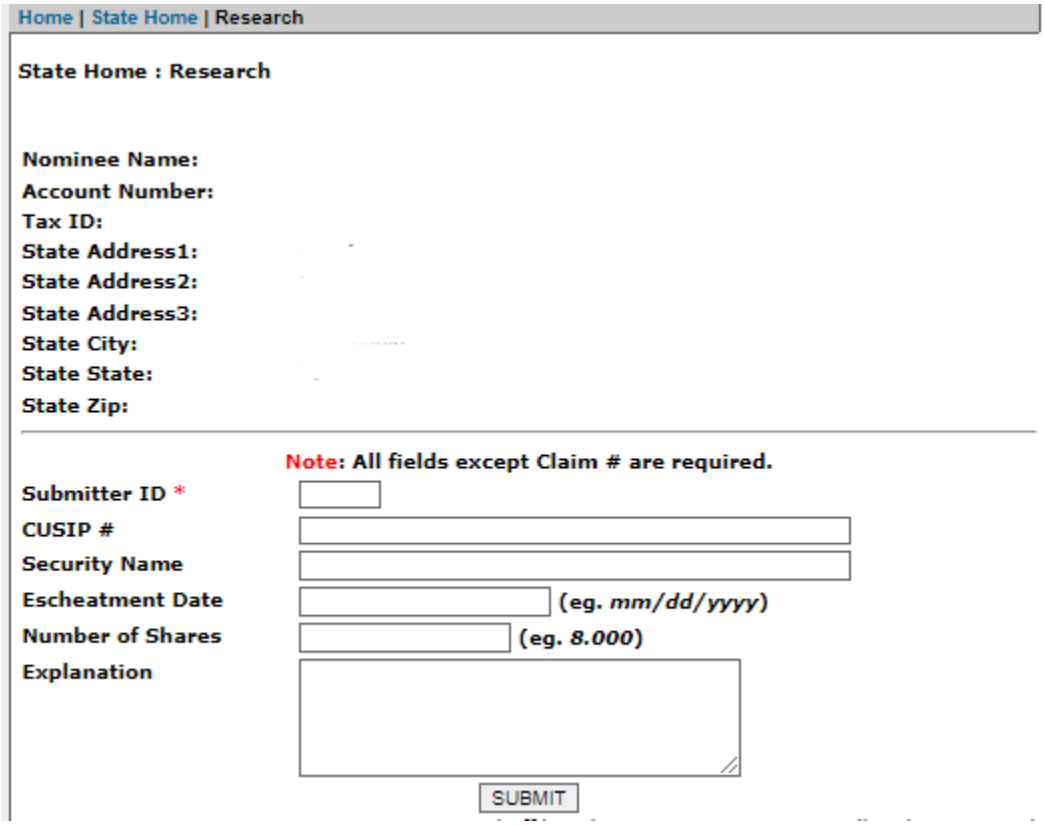
1. NWT/DRP
2. Research
3. Liquidation

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



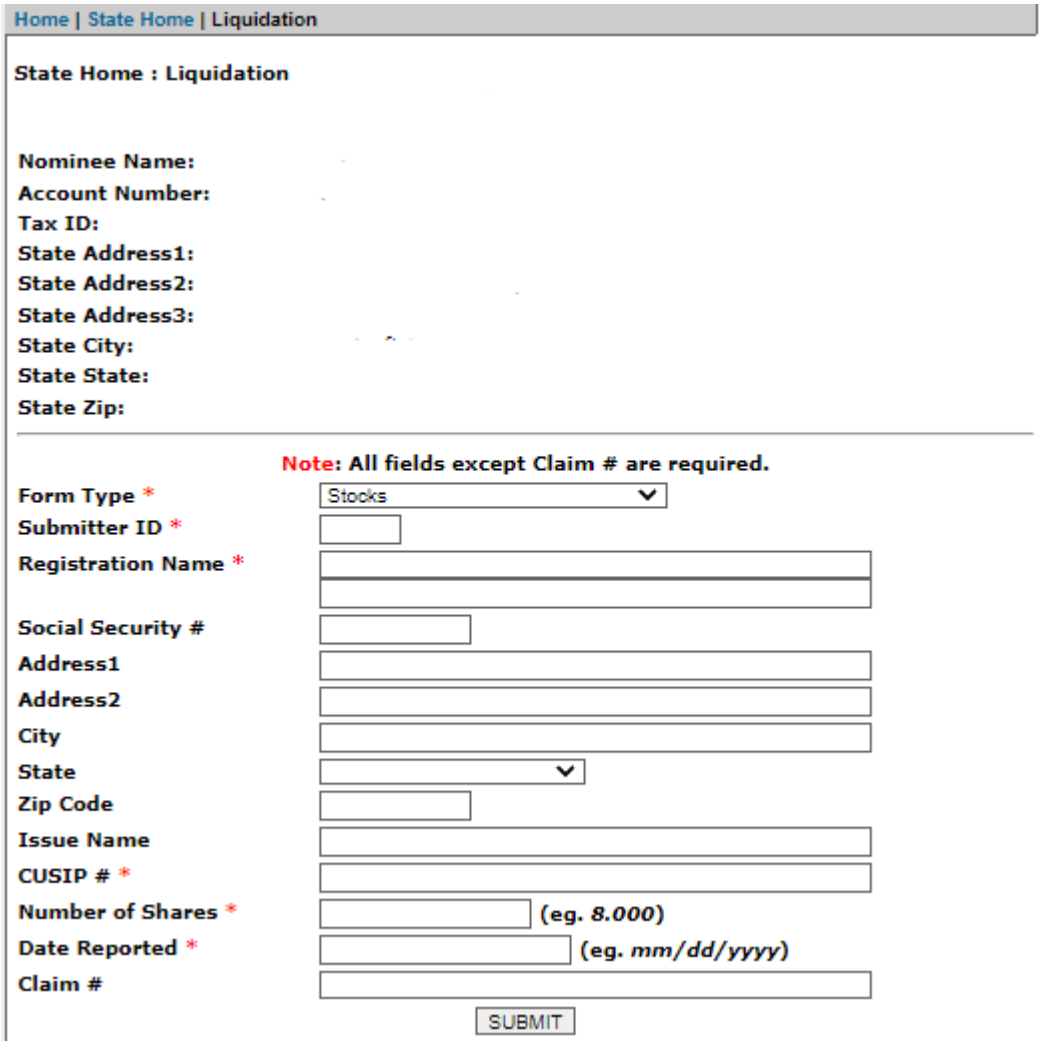
State Home - Research

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



State Home – Liquidation

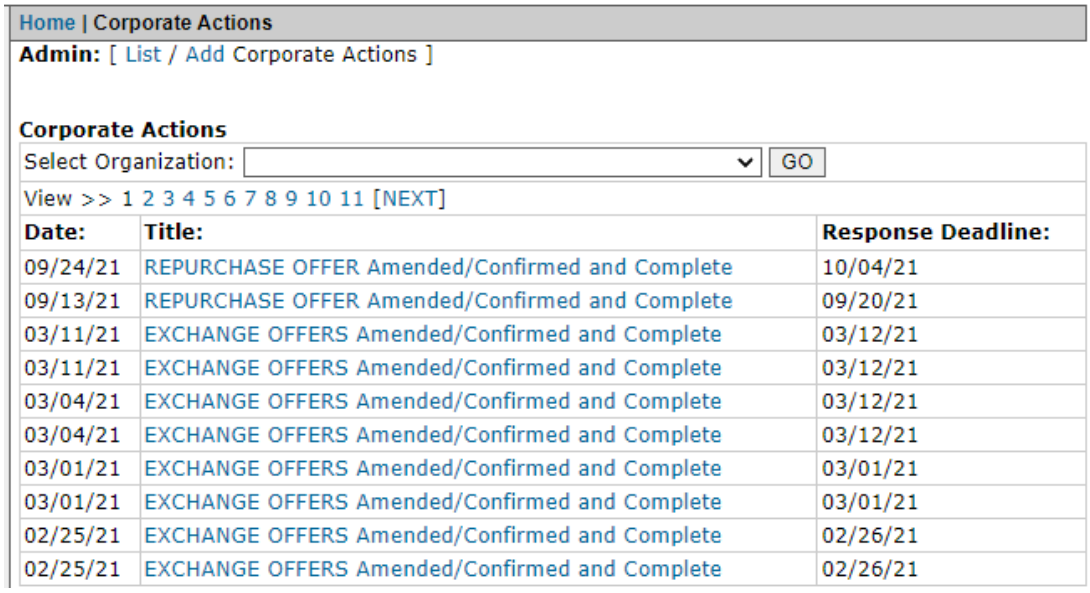
3. Form: Please fill in the fields and click Submit



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:

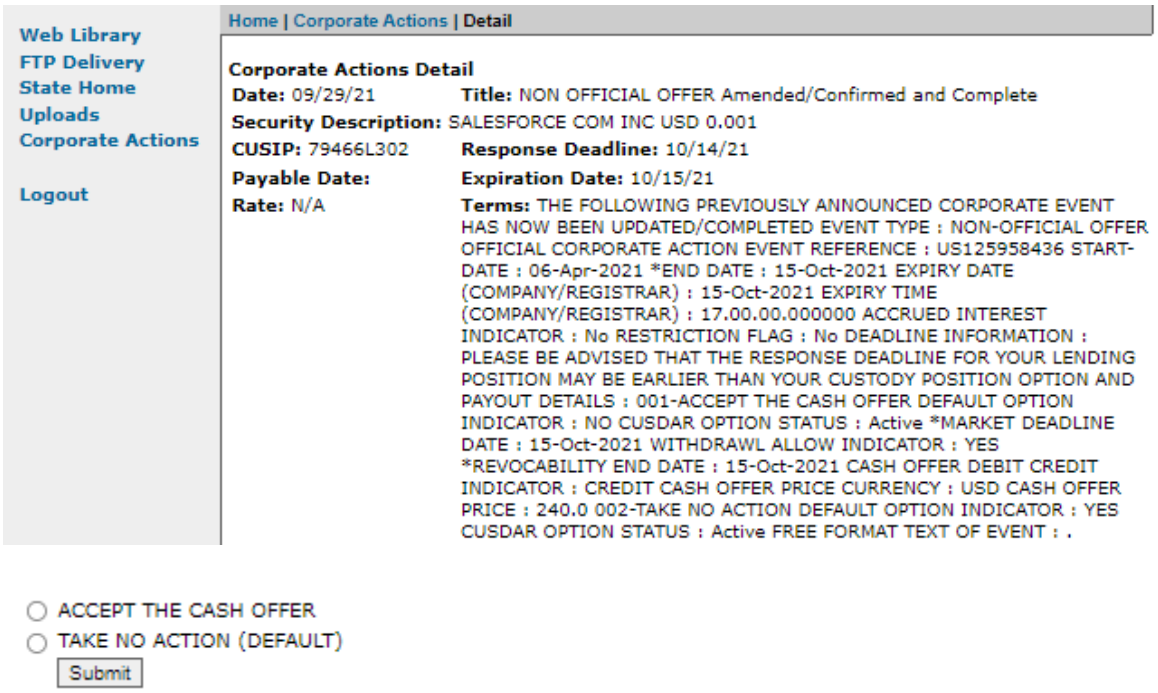


The user has the ability to see all voluntary Corporate Actions associated with the user's state/organization.

***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

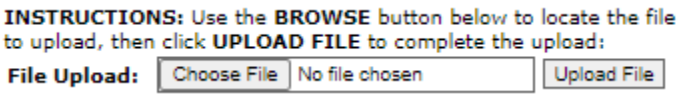
By clicking on a specific Corporate Action, the user will see all information associated with the action such as: the name of the security (title), cusip number, response deadline, posting and expirations dates, the rate, a description of the action (term) and the options available. The following is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



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.



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".

□□□□ □ □□□r□□

Class Actions Report

.PDF Format

AVENU INSIGHTS & ANALYTICS

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., Securities Litigation		**N/A**	**7/19/2023**	**8/21/2023**	**11/4/2013**	**6/27/2017**	**USD**	**74,000,000.0000**
XXXXX	□T□T□ N□M□	**6/9/2016**	6/1/2023	OPEN	PREPARATION IN			0
WELLS FARGO & COMPANY, Securities Litigation (18CWHO)		**N/A**	**7/27/2023**	**8/21/2023**	**11/3/2016**	**8/3/2017**	**USD**	**300,000,000.0000**
		NO SELECTED ACCOUNTS AFFECTED						
ARCONIC INC., Securities 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	DNF NO ELIGIBLE TRANSACTIONS		0
ARCONIC INC., Securities Litigation		**N/A**	**7/19/2023**	**8/21/2023**	**11/4/2013**	**6/27/2017**	**USD**	**74,000,000.0000**
		NO SELECTED ACCOUNTS AFFECTED						
WELLS FARGO & COMPANY, Securities Litigation (18CV03948WHO)		**N/A**	**7/27/2023**	**8/21/2023**	**11/3/2016**	**8/3/2017**	**USD**	**300,000,000.0000**
XXXXX	□T□T□ N□M□	**6/9/2016**	5/31/2023	OPEN	NOT-FILED	DNF NO ELIGIBLE TRANSACTIONS		0
TACTILE SYSTEMS TECHNOLOGY. INC, Securities Litigation		**N/A**	**8/2/2023**	**8/23/2023**	**5/7/2018**	**6/8/2020**	**USD**	**5,000,000.0000**
		NO SELECTED ACCOUNTS AFFECTED						
SUNLANDS TECHNOLOGY GROUP, Securities Litigation		**N/A**	**9/6/2023**	**8/28/2023**	**2/23/2018**	**9/18/2018**	**USD**	**6,200,000.0000**
		NO SELECTED ACCOUNTS AFFECTED						
KRAFT HEINZ COMPANY, Fair Fund		**N/A**	**N/A**	**8/31/2023**	**2/26/2016**	**2/21/2019**	**USD**	**62,000,000.0000**
		NO SELECTED ACCOUNTS AFFECTED						

*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

ISIN	Description	Ctry Inc	Loc	Ccy	Units 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 30OCT05	BR	DTC	USD	50,000.0000			
				TOTAL BY UNITS - DEBT	50,000.0000			
				TOTAL BY AMORTIZED FACE - DEBT	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
EURO (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 BY UNITS - EURO	100,275.0000			
				TOTAL BY AMORTIZED FACE - EURO	0.0000		7.00	7.79
SWISS FRANC (Exchange Rate: 1.0326310000)								
CH0244767585	UBS GROUP AG CHF 0.1	CH	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	CH	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	IE	DTC	USD	3.0000	54.650000	163.95	163.95
IE00BD845X29	ADIENT PLC USD 0.001	IE	DTC	USD	1.0000	44.200000	44.20	44.20
IE00BLS09M33	PENTAIR PLC USD 0.01	IE	DTC	USD	3.0000	54.700000	164.10	164.10
IE00BTN1Y115	MEDTRONIC PLC USD 0.1	IE	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	IE	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

ISIN	Description	Ctry Inc	Loc	Ccy	Units 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 - UNITED STATES DOLLAR				39,293.4780			
	TOTAL BY AMORTIZED FACE - UNITED STATES DOLLAR				0.0000		206,551.14	206,551.14
	TOTAL BY UNITS - EQUITIES				142,044.4780			
	TOTAL BY AMORTIZED FACE - EQUITIES				0.0000			239,607.79
	TOTAL BY UNITS - ACCOUNT XXXXXX - AUZF STATE NAME				192,044.4780			
	TOTAL BY AMORTIZED FACE - ACCOUNT XXXXXX- AUZF 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

	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	Trade Date / Contract Settle Date / Order Date	Shares/Par / Local Net Amt / Local Price	Status / Local Currency / Comments
SD	Security Addition	CA0559341031	10/20/2019	166.0000	Failing - SETTLEMENT FAILURE
	BPI ENERGY HOLDINGS INC	1163010205943	10/20/2019		UNITED STATES DOLLAR (USD)
	FIRST CLEARING, LLC	26931837.6			26876390.338 B/C A, REC FROM FIRST CLEARING AWAITING SECURITIES FROM CPY 1163010101840
	FIRST CLEARING, LLC				
	AWSH	Actual			
	AWAITING SECURITIES FROM CPY				
SD	Security Addition	CA1344226099	10/20/2019	20.0000	Failing - SETTLEMENT FAILURE
	CAMPBELL R COM NPV	1163010206055	10/20/2019		UNITED STATES DOLLAR (USD)
	FIRST CLEARING, LLC	26931837.19			26876390.352 B/C A, REC FROM FIRST CLEARING AWAITING SECURITIES FROM CPY 1163010101883
	FIRST CLEARING, LLC				
	AWSH	Actual			
	AWAITING SECURITIES FROM CPY				
SD	Security Addition	CA6565685089	12/8/2019	1.0000	Pending - VERIFIED
	NORTEL NETWORKS CORP NEW NPV	1163090300390	12/8/2019		UNITED STATES DOLLAR (USD)
	OPTIONSXPRESS, INC.	27016545.129			B/C A RECEIVE FROM OPTIONXPRESS
	OPTIONSXPRESS, INC.				
		Actual			
SD	Security Addition	CA67000B1040	10/28/2019	13.0000	Failing - VERIFIED
	NOVANTA INC NPV	1162990284984	10/28/2019		UNITED STATES DOLLAR (USD)
	NATL FINANCIAL SERVICES LLC	26925435.589			B/C A, REC FROM FIDELITY AWAITING SECURITIES FROM CPY 1162990130269
	NATL FINANCIAL SERVICES LLC				
	AWSH	Actual			
	AWAITING SECURITIES FROM CPY				

	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	Trade Date / Contract Settle Date / Order Date	Shares/Par / Local Net Amt / Local Price	Status / Local Currency / Comments
SD	Security Addition **CONTRA BACKWEB TECHNOLOGIES NPV** OPTIONSXPRESS, INC. OPTIONSXPRESS, INC.	USM15CNT9972 1163090300360 27016545.121 Actual	1/8/20□0 1/8/20□0	300.0000	Pending - VERIFIED UNITED STATES DOLLAR (USD) B/C A RECEIVE FROM OPTIONXPRESS
	TOTAL SECURITY DEPOSIT (7)			**499.0720**	**Shares/Par**
SW	Security Withdrawal **CONTRA BACKWEB TECHNOLOGIES NPV** RAYMOND, JAMES & ASSOC., INC. RAYMOND, JAMES & ASSOC., INC.	USM15CNT9972 1163000246904 Actual	10/25/2019 10/25/2019	-600.0000	Failing - VERIFIED UNITED STATES DOLLAR (USD) B/C C SALE OF SHARES DOC 26935128
	TOTAL XXXXXX - STATE NAME(242)			**4,325,418.3410**	**Shares/Par**
	REPORT TOTAL (242)			**4,325,418.3410**	**Shares/Par**

Securities Liquidation Report

	Description	CUSIP/CINS		Shares/Par	
	Trading Broker	ISIN	Create Date		
	Clearing Broker	Reference Number	Trade/Ex Date	Local Net Amount	
	Buyer Order Party	Client Reference	Contract Settle/Pay Date	Local Price	Status
	Seller Order Party	Market Reference	Actual Settle Date	Days Late	Local Currency
	Cash Offset Number	Settlement Policy	Order Date		
	Comments				

S	Sale- Mutual Fund order	746853100	12/2/2019	-227.0000	Settled - **ACTUAL**
	PUTNAM PRE SBI NPV	US7468531006	12/1/2019	1,090.72	**SETTLEMENT**
	RAYMOND JAMES & ASSOC INC	1163070106776	12/4/2019	4.8300881000	UNITED STATES
	RAYMOND JAMES & ASSOC INC	GTN1611020006458	12/4/2019	0	DOLLAR (USD)
			-		
		Actual			
	Cash Offset - XXXXX08400				
	SPRO//RVA 63 1/01/19 1163070076550				
S	Sale	878520204	12/2/2019	-5.0000	Settled - **ACTUAL**
	TECHNICOLO NPV ADR	US8785202040	12/1/2019	28.81	**SETTLEMENT**
	RAYMOND JAMES & ASSOC INC	1163070106738	12/4/2019	5.7900000000	UNITED STATES
	RAYMOND JAMES & ASSOC INC	GTN1611020006452	12/4/2019	0	DOLLAR (USD)
			-		
		Actual			
	Cash Offset - XXXXX08400				
	SPRO//RVA 70 1/01/19 1163070076565				
S	Sale	882508104	12/2/2019	-17.	Settled - **ACTUAL**
	TEXAS INSTRS INC USD 1.0	US8825081040	12/1/2019	1,174.07	**SETTLEMENT**
	0000 RAYMOND JAMES & ASSOC INC	1163070106723	12/4/2019	69.0900000000	UNITED STATES
	RAYMOND JAMES & ASSOC INC	GTN1611020006448	12/4/2019	0	DOLLAR (USD)
			-		
		Actual			

Shares Liquidated includes number of shares, date, price, commission, net proceeds and more.

Some fee information may be missing from this report for up to an hour after a trade has been made.

Description	**CUSIP/CINS**		
Trading Broker	**ISIN**	**Create Date**	
Clearing Broker	**Reference Number**	**Trade/Ex Date**	**Shares/Par**
Buyer Order Party	**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**
Seller Order Party	**Market Reference**	**Actual Settle Date**	**Local Price Status**
Cash Offset Number	**Settlement Policy**	**Order Date**	**Days Late Local Currency**
Comments			

Cash Offset - XXXXX08400

SPRO// □□□N□ UNCLAIMED PROPERTY
CLEARING AVERAGE PRICE TRADE 2255 RVA
71 11/01/16 1163070076560

TOTAL SELL (1)	**-17.0000 Shares/Par**
TOTAL TEXAS INSTRS INC USD 1.0 (1)	**-17.0000 Shares/Par**
TOTAL XXXXXX - STATE NAME	**-249.0000 Shares/Par**
(3)	

Some fee information may be missing from this report for up to an hour after a trade has been made.

Mutual Fund Sales Report

Mutual Fund Sales

AVENU INSIGHTS & ANALYTICS

XXXXXX - STATE NAME

Custody Security Transactions

By Security

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

Report ID ICUS0015

Description		**CUSIP/CINS**			
Trading Broker		**ISIN**	**Create Date**		
Clearing Broker		**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party		**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party		**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number		**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments					

S	Sale- Mutual Fund order	001413103	12/2/2019	-107.1730	Settled **- ACTUAL**
	AIM EQUITY INVSC CHRTR FD A	US0014131033	12/1/2019	1,955.91	**SETTLEMENT**
		1163070082128	12/2/2019	18.2500256000	UNITED STATES DOLLAR (USD)
		26968011	12/2/2019	0	
			-		
			Actual		
	Cash Offset - XXXXX08400				
	1163060158808 10-31-19 SALE REQUEST SALE OF SHARE 1163060158808 10-31-19 SALE REQUEST SALE OF SHARE				
S	Sale- Mutual Fund order	001413194	12/2/2019	-60.3620	Settled **- ACTUAL**
	AIM EQUITY INVSC DVSFD INV	US0014131942	12/1/2019	1,129.37	**SETTLEMENT**
		1163070082055	12/2/2019	18.7099499000	UNITED STATES DOLLAR (USD)
		TSR1611018827027	12/2/2019	0	
			-		
			Actual		
	Cash Offset - XXXXX08400				
	1163060195152 10-31-19 SALE REQUEST SALE OF 1163060195152 10-31-19 SALE REQUEST SALE OF SHARES UNEXECUTED DOC 26968011				

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

TOTAL XXXXXX - STATE NAME(2) -167.5350 Shares/Par

Some fee information may be missing from this report for up to an hour after a trade has been made.

List of Assets Report

.XLS

LIST OF ASSETS

AVENU INSIGHTS & ANALYTICS

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	774,235.1800	1.000000	774,235.18	[illegible]				
[illegible]	[illegible]	[illegible]	[illegible]	3,951.0000	0.225000	888.98	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	60.0000	0.090000	5.40	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	10,000.0000	0.740000	7,400.00	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	2,158.0000	0.010000	21.58	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	701.0000	0.235000	164.74	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	42.0000	1.000000	42.00	[illegible]				
[illegible]	[illegible]	[illegible]	[illegible]	4,000.0000	0.000001	0.01	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	253.0000	1.410000	356.73	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	30.0000	2.150000	64.50	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	5,000.0000	94.566000	4,728.30	[illegible]				
[illegible]	[illegible]	[illegible]	[illegible]	70.0000	2.911168	203.78	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	35.0000	1.510000	52.85	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	1,400.0000	14.340000	20,076.00	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	6.0000	37.730000	226.38	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	10.0000	4.380000	43.80	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	8,633.0000	0.040000	345.32	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	599.0000	42.590000	25,511.41	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	1.0000	11.370000	11.37	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	1,173.0000	0.080343	94.24	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	1,798.0000	0.680000	1,222.64	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	391.0000	9.630000	3,765.33	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	10.0000	0.085000	0.85	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	1.0000	3.330000	3.33	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	7,342.0000	16.690000	122,537.98	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	4,800.0000	0.185000	888.00	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	462.0000	0.830000	383.46	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	10.0000	2.470000	24.70	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	4.0000	0.490000	1.96	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	168.0000	0.022500	3.78	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	4.0000	19.730000	78.92	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	12.0000	0.045000	0.54	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	45.0000	65.280000	2,937.60	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	3,000.0000	0.205000	615.00	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	4.0000	55.530000	222.12	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	25.0000	6.640000	166.00	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	2,500.0000	0.005500	13.75	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	672.0000	30.410000	20,435.52	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	64.0000	10.140000	648.96	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	215.0000	16.150000	3,472.25	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	60.0000	30.490000	1,829.40	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	150.0000	14.230000	2,134.50	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	18.0000	7.340000	132.12	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	50.0000	11.080000	554.00	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	10.0000	0.320000	3.20	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	11.0000	10.690000	117.59	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	34.0000	10.360000	352.24	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	1,743.0000	0.000700	1.22	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	100.0000	1.536153	153.62	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	100.0000	0.002600	0.26	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	109.0000	73.650000	8,027.85	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	68.0000	18.415000	1,252.22	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	204.0000	17.590000	3,588.36	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	20.0000	7.960000	159.20	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	545.0000	0.401100	218.60	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	34.0000	178.360000	6,064.24	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	444.0000	83.100000	36,896.40	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	9.0000	3.660000	32.94	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	16.0000	13.970000	223.52	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	18.0000	174.930000	3,148.74	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	18.0000	19.090000	343.62	[illegible]	[illegible]	[illegible]	[illegible]	

Settled Cash Balances Report

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 - XXXXXXXXX								
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- XXXXXXXXX								
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

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
TOTAL CASH AND SWEEP						3,773.74	211.65	3,985.39

Free Receive via DTC Report

Free Receive via DTC

AVENU INSIGHTS & ANALYTICS

Custody Security Transactions

By Security

Actual Settle Date 1/4/2020

Report ID ICUS0015

XXXX - STATE OF STATE NAME

Description					
Trading Broker		**ISIN**	**Create Date**		
Clearing Broker		**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party		**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party		**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number		**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments					
SD	Security Addition	US5024241045	1/2/20□0	2.0000	Settled **- ACTUAL SETTLEMENT**
	L-3 COMMUNICATIONS CORP. USD 0.01	1163070283769	1/4/20□0		UNITED STATES DOLLAR (USD)
	NATL FINANCIAL SERVICES LLC	26987790.12	1/4/20□0		
	NATL FINANCIAL SERVICES LLC		1/4/20□0	0	
		Actual	-		

Shares received from holder. Holder Name and Broker name included.

B/C A, REC FROM NFS 1163070125684

SD	Security Addition	US7043261079	1/4/20□0		Settled **- ACTUAL SETTLEMENT**
	PAYCHEX INC USD 0.01	1163090208548	1/4/20□0		UNITED STATES DOLLAR (USD)
	1.0000 INTERNAL TRANSFER	TRF-FRM 822428	1/4/20□0		
	BANK OF NY CUST CLEARANCE		1/4/20□0	0	
		Actual			

Shares received from holder via DTC. Avenu Report- Internal Transfer with report ID number for easy reconciliation.

B/C A XFER TO XXXXX 049480516-20161101
1163090108127

AVENU INSIGHTS & ANALYTICS

Custody Security Transactions

By Security

Actual Settle Date 1/4/2020

Report ID ICUS0015

XXXXXX- STATE OF STATE NAME

Description			
Trading Broker	**ISIN**	**Create Date**	
Clearing Broker	**Reference Number**	**Trade/Ex Date**	**Shares/Par**
Buyer Order Party	**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**
Seller Order Party	**Market Reference**	**Actual Settle Date**	**Local Price** **Status**
Cash Offset Number	**Settlement Policy**	**Order Date**	**Days Late** **Local Currency**
Comments			

B/C A, REC FROM NFS 26987790.14
1163090090949

TOTAL SECURITY DEPOSIT (1) **2,000.0000 Shares/Par**

TOTAL STANDARD E COM USD0.01 (1) **2,000.0000 Shares/Par**

SD	Security Addition	US9840171030	1/2/20□0	270.000	Settled **- ACTUAL SETTLEMENT**
	XENIA HOTE COM USD0.01	1163070283852	1/4/20□0		UNITED STATES DOLLAR (USD)
	0 NATL FINANCIAL SERVICES LLC	26987790.15	1/4/20□0	0	
	NATL FINANCIAL SERVICES LLC		1/4/20□0		
		Actual	-		

B/C A, REC FROM NFS 1163070125709

TOTAL XXXXXX- AUZF STATE OF XXX(6) **2,476.0000 Shares/Par**

Free Receipt DRS Report

Free Receive - via DRS

AVENU INSIGHTS & ANALYTICS

Custody Security Transactions

By Security

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

Report ID ICUS0015

XXXXXX - STATE OF STATE NAME

	Description	CUSIP/CINS			
	Trading Broker	ISIN	Create Date		
	Clearing Broker	Reference Number	Trade/Ex Date	Shares/Par	
	Buyer Order Party	Client Reference	Contract Settle/Pay Date	Local Net Amount	
	Seller Order Party	Market Reference	Actual Settle Date	Local Price	Status
	Cash Offset Number	Settlement Policy	Order Date	Days Late	Local Currency
	Comments				
SD	Security Addition	46625H100	12/28/2019	3.0000	Settled - **ACTUAL SETTLEMENT**
	JPMORGAN CHASE + CO USD 1.0	US46625H1005	12/28/2019		UNITED STATES DOLLAR (USD)
	JPMORGAN CHASE BANK	1163020203255	12/28/2019		
	JPMORGAN CHASE BANK	JP MORGAN	12/31/2019	3	
			-		
			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				
SD	Security Addition	906548508	12/31/2019	2.0000	Settled - **ACTUAL SETTLEMENT**
	UNION ELEC CO 4.5 CUM PFD	US9065485081	12/31/2019		UNITED STATES DOLLAR (USD)
	AMEREN SERVICES COMPANY/DRS	1163050316378	12/31/2019		
	AMEREN SERVICES COMPANY/DRS		12/31/2019	2	
			-		
			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**

Some fee information may be missing from this report for up to an hour after a trade has been made.

Free Receive – via DWAC Report

RECEIPT OF DWAC

AVENU INSIGHTS & ANALYTICS

XXXXXX - STATE NAME

Custody Security Transactions

By Security

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

Report ID ICUS0015

Description	**CUSIP/CINS**			
Trading Broker	**ISIN**	**Create Date**		
Clearing Broker	**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party	**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party	**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number	**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments				

SD	Security Addition	039483102	9/26/2019	65.0000	Settled **- ACTUAL SETTLEMENT**
	ARCHER DANIELS MIDLAND CO NPV	US0394831020	9/26/2019		UNITED STATES DOLLAR (USD)
	DWAC-DTC DEPOSITS/WITHDRAWALS	1162700208079	9/26/2019		
	DWAC-DTC DEPOSITS/WITHDRAWALS	NRF1609262261400	9/26/2019	0	
			-		
			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

Some fee information may be missing from this report for up to an hour after a trade has been made.

Free Receive - Mutual Funds

Free Receive of Mutual Funds

AVENU INSIGHTS & ANALYTICS

XXXXXX - STATE NAME

Custody Security Transactions

By Security

Actual Settle Date 1/4/2020

Report ID ICUS0015

Description					
Trading Broker		**ISIN**	**Create Date**		
Clearing Broker		**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party		**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party		**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number		**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments					

SD	Security Addition	IE00BDB6Q211	1/4/20□0	17.0000	Settled **- ACTUAL SETTLEMENT**
	WILLIS TOWERS WATSON P USD 0.000305	1163090208540	1/4/20□0		UNITED STATES DOLLAR (USD)
	INTERNAL TRANSFER	TRF-FRM XXXXX	1/4/20□0	0	
	BANK OF NY CUST CLEARANCE		1/4/20□0		
		Actual	-		
	B/C A OR XFER TO XXXXX G96655108-20161101 1163090108126				
SD	Security Addition	US6706788873	1/3/20□0	260.	Settled **- DEPOSITED**
	NUVEEN INV DIVID VALUE FD CL A	1163080261452	1/1/20□0		UNITED STATES DOLLAR (USD)
	0290 NON BROKER TRADE	27005275.052	1/3/20□0		
	NON BROKER TRADE		1/4/20□0	1	
		Actual	-		
	B/C MR REC FROM FIRST CASH/CASH AWAITING SECURITY FROM REGISTR				

Mutual Fund Receipt – Includes delivering party, dividend payment option, trade & settle date

TOTAL XXXXXX - STATE(2) 277.0290 Shares/Par

Receipt of Physical

Certificate Report

Receipt of Physical Certificate

AVENU INSIGHTS & ANALYTICS

XXXXXX- STATE NAME

Custody Security Transactions

By Security

Actual Settle Date 1/4/2020

Report ID ICUS0015

Description				
Trading Broker	**ISIN**	**Create Date**		
Clearing Broker	**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party	**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party	**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number	**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments				

SD	Security Addition	US29413C2026	1/3/20□0	7.0000	Settled **- ACTUAL SETTLEMENT**
	ENVIROTECHNOLIGIES, INC USD .001	1163090141149	1/3/20□0		
	CUSTOMER	27012828.26	1/3/20□0		UNITED STATES DOLLAR (USD)
	CUSTOMER		1/4/20□0	1	
		Actual	-		

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

REC BY □□□N□ FROM NFS
020620516/111116 26987790.109 ES0757
1163090090979

TOTAL XXXXXX- STATE NAME (1) 7.0000 Shares/Par

Transfer to Claimant Report

Re-Reg

AVENU INSIGHTS & ANALYTICS

XXXXXX - STATE NAME

Custody Security Transactions

By Security

Actual Settle Date 1/4/2020

Report ID ICUS0015

Description				
Trading Broker	**ISIN**	**Create Date**		
Clearing Broker	**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party	**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party	**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number	**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments				

SW	Security Withdrawal	US8251071051	10/28/2019	-7.0000 Settled **- ACTUAL SETTLEMENT**
	SHORE BANCSHARES INC USD 0.01	1163020153768	10/28/2019	UNITED STATES DOLLAR (USD)
	SHIP TO CUSTOMER-STMT ONLY	172318	10/28/2019	7
	SHIP TO CUSTOMER-STMT ONLY		1/4/20□0	
			Actual -	

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

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

SW	Security Withdrawal	US88579Y1010	10/28/2019	-2.0000 Settled **- ACTUAL SETTLEMENT**
	3M CO USD 0.01	1163020154295	10/28/2019	UNITED STATES DOLLAR (USD)
	SHIP TO CUSTOMER-STMT ONLY	177723	10/28/2019	7
	SHIP TO CUSTOMER-STMT ONLY		1/4/20□0	
			Actual -	

CL 177723 JANE ANDERSON, 100 HANCOCK STREET, QUINCY MA 02171 □□□N□

TOTAL XXXXXX- STATE NAME (2) -9.0000 Shares/Par

Cash Dividends Report

Tran Type	Description / Trading Broker / Clearing Broker / Linked Transaction Description	CUSIP/CINS / ISIN / Reference Number / Client Reference / Event ID / Market Reference / Settlement Policy	Trade / Ex Date / Settle / Pay Date / Cash Post Date / Cash Value Date	Shares/Par/Amount / Local Price/Rate / Local Principal / Local Income	Local Amount	Reporting Equivalent
UNITED STATES DOLLAR (USD) AUZF STATE NAME - XXXXXXXXX						
1/4/2019 - Posted	**Exchange Rate 1.0000000000**					
DIVIDEND						
DV	**Dividend** **CRH PLC EUR 0.3** Gross 0.82 RecDte: 9/9/2019 Source W/H -0.16 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: 0JAN04 CCY: USD GRSS: 0.8200 WTH: 0.1600 AMOR BAL: 0.0000 PRFC: 0.0000 CUFC: 0.0000	G25508105 IE0001827041 PSS1611020000627 0112443205	9/9/2019 12/4/2019 12/4/2019 12/4/2019	4.0000 0.2051633500 0.66	0.66	0.66
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 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	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
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	19765N401 US19765N4016 PSS1611046018899 0113349658	8/31/2019 8/31/2019 12/4/2019 8/31/2019*	41.7940 1.06	1.06	1.06
				SUBTOTAL DIVIDEND (3)	16.12	16.12

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

*Back Valued Transaction

Corporate Action Activity Report

AVENU INSIGHTS & ANALYTICS

XXXXXX- STATE NAME

Custody Security Transactions

By Security

Actual Settle Date 1/4/2020

Report ID ICUS0015

Description				
Trading Broker	**ISIN**	**Create Date**		
Clearing Broker	**Reference Number**	**Trade/Ex Date**	**Shares/Par**	
Buyer Order Party	**Client Reference**	**Contract Settle/Pay Date**	**Local Net Amount**	
Seller Order Party	**Market Reference**	**Actual Settle Date**	**Local Price**	**Status**
Cash Offset Number	**Settlement Policy**	**Order Date**	**Days Late**	**Local Currency**
Comments				

CA Receipt of Rights
SG1DC4000002 **CHARISMA ENERGY SERVIC RITS 22NOV19**
1163054005692
10/31/2019
1/1/20□0
1/1/20□0
1/4/20□0
Actual -
180.0000 Settled **- ACTUAL SETTLEMENT** SINGAPORE DOLLAR (SGD)
3

C/DECL// SG2B54957198 114485890 C/DECL// SG2B54957198 114485890 ORIG EVENT: SG2B54957198 NEW CODE: RATIO: 000001.000000/000010.000000

Corporate Action Activity – Includes rate, type, payable date, event ID and more

CA Name Change
ALCOA INC USD 1.0
US0138175072
1163094004290
1/4/20□0
1/1/20□0
1/4/20□0
1/4/20□0
Actual -
-3,705.0000 Settled **- ACTUAL SETTLEMENT** UNITED STATES DOLLAR (USD)
0

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
1163054007461
10/31/2019
1/1/20□0
1/4/20□0
1/4/20□0
Actual -
1,235.00 Settled **- ACTUAL SETTLEMENT** UNITED STATES DOLLAR (USD)
0

Weekly/Monthly Wire

AVENU
INSIGHTS & ANALYTICS

Weekly/Monthly Sale Wire Report - Sample

Actual Settle Date	CUSIP/CINS	Security Short Description	Shares / Par	Local Price/Rate	Local Principal Amount	Commission	Local Income Amount	Miscellaneous Fees	Foreign Exchange Fees	Local Amount	Transaction Type Name	Transaction Description 1		Transaction Description 2
12/29/2019	52469H115	LEGG MASON CLEARBRIDGE DIVIDEND STR	-102.629	$ 22.89	$ 2,349.18	$ (14.37)	$ -	$ -	$ -	$ 2,334.81	SELL	1181780289545		SALE 6-22-18 SALE OF SHARES
12/16/2019	4812C2601	JP MORGAN INVESTOR CONSERVATIV	-496.733	$ 12.68	$ 6,298.57	$ (69.54)	$ -	$ -	$ -	$ 6,229.03	SELL	1181940123132		SALE 7-11-18 SALE OF SHARES
12/16/2019	641224100	NEUBERGER GENESIS FUND	-480.840	$ 62.03	$ 29,826.51	$ (67.32)	$ -	$ -	$ -	$ 29,759.19	SELL	1181940123861		SALE 7-11-18 SALE OF SHARES
12/5/2019	939330106	WASHINGTON MUTUAL INVESTORS FUND	-74.284	$ 44.28	$ 3,289.30	$ (10.40)	$ -	$ -	$ -	$ 3,278.90	SELL	GSP #:1181860157475 UNITS/QNTY:	74.2840	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019	939330106	WASHINGTON MUTUAL INVESTORS FUND	-4.621	$ 44.28	$ 204.62	$ (0.65)	$ -	$ -	$ -	$ 203.97	SELL	GSP #:1181860160230 UNITS/QNTY:	4.6210	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019	19765P638	COLUMBIA FUNDS SERIES TRUST I -	-1349.665	$ 20.02	$ 27,020.29	$ (188.95)	$ -	$ -	$ -	$ 26,831.34	SELL	GSP #:1181860160890 UNITS/QNTY:	1,349.6650	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019	746704105	PUTNAM DIVERSIFIED INCOME TRUST SHS	-19.629	$ 7.04	$ 138.19	$ (2.75)	$ -	$ -	$ -	$ 135.44	SELL	GSP #:1181860161539 UNITS/QNTY:	19.6290	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019	746745108	PUTNAM EQUITY INCOME FUND SHS -A-	-86.350	$ 24.44	$ 2,110.39	$ (12.09)	$ -	$ -	$ -	$ 2,098.30	SELL	GSP #:1181860162098 UNITS/QNTY:	86.3500	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019	746745108	PUTNAM EQUITY INCOME FUND SHS -A-	-0.357	$ 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 INCOME FUND SHS -A-	-10.882	$ 24.44	$ 265.96	$ (1.52)	$ -	$ -	$ -	$ 264.44	SELL	GSP #:1181860164060 UNITS/QNTY:	10.8820	TRADE DT:18JUL03 CONT SET DT:18JUL05 CALL/MAT DT:
12/5/2019	746745108	PUTNAM EQUITY INCOME FUND SHS -A-	-26.048	$ 24.44	$ 636.61	$ (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 HEALTH CARE FUND,	-168.471	$ 51.14	$ 8,615.61	$ (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 HEALTH CARE FUND,	-37.072	$ 51.14	$ 1,895.86	$ (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 - RBC ENTERPRISE	-3.596	$ 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 - RBC ENTERPRISE	-0.770	$ 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 USD1	-3.212	$ 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 USD1	-2869.568	$ 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 FOCUS FUND SHS	-253.119	$ 43.44	$ 10,995.49	$ (35.44)	$ -	$ -	$ -	$ 10,960.05	SELL	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 0.01	-208.000	$ 0.00	$ 0.64	$ (0.01)	$ -	$ -	$ -	$ 0.63	SELL	SPRO//MXA 17 07/13/18		1181970059381
12/17/2019	37426X204	GET REAL USA INC USD 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	$ 471.20	$ (0.01)	$ -	$ -	$ -	$ 471.19	SELL	SPRO//MXA 19 07/13/18		1181970059350
12/17/2019	949090104	WELBILT INC USD 0.01	-7.000	$ 23.56	$ 164.92	$ (0.98)	$ -	$ -	$ -	$ 163.94	SELL	SPRO//RVA 11 07/13/18		1181970059365
12/17/2019	961684107	WESTWATER RES INC USD 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 BIOSCIENCES CORP USD 0.01	-3.000	$ 1.12	$ 3.36	$ (0.42)	$ -	$ -	$ -	$ 2.94	SELL	SPRO//RVA 21 07/05/18		1181860116081
12/9/2019	746909100	PUTNAM MAS SBI NPV	-706.000	$ 4.59	$ 3,240.61	$ (98.84)	$ -	$ -	$ -	$ 3,141.77	SELL	SPRO//RVA 23 07/05/18		1181860116084
12/9/2019	746922103	PUTNAM MUN COM SBI NPV	-3.000	$ 11.66	$ 34.98	$ (0.42)	$ -	$ -	$ -	$ 34.56	SELL	SPRO//RVA 24 07/05/18		1181860116086
12/9/2019	812578102	SEATTLE GE COM USD0.001	-52.000	$ 67.99	$ 3,535.49	$ (7.28)	$ -	$ -	$ -	$ 3,528.21	SELL	SPRO//RVA 25 07/05/18		1181860116088
12/9/2019	949746101	WELLS FARGO + CO NEW USD 1.666	-4.000	$ 55.35	$ 221.41	$ (0.56)	$ -	$ -	$ -	$ 220.85	SELL	SPRO//RVA 26 07/05/18		1181860116091
12/9/2019	925550105	VIAVI SOLUTIONS INC USD 0.001	-10.000	$ 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	$ 1,805.43	$ 7,221.72	$ (0.56)	$ -	$ -	$ -	$ 7,221.16	SELL	SPRO//RVA 4 07/13/18		1181970059375
12/17/2019	46138G706	INVESCO EX SOLAR ETF	-1.000	$ 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 USD 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 0.01	-120.000	$ 35.30	$ 4,236.00	$ (16.80)	$ -	$ -	$ -	$ 4,219.20	SELL	SPRO//RVA 9 07/13/18		1181970059358
12/9/2019	656811106	NORTH AMERN CONSTR GROUP LTD NPV	-9.000	$ 5.80	$ 52.20	$ (1.26)	$ -	$ -	$ -	$ 50.94	SELL	SPRO// CNDT STATE LOCAL SOLUTIONS		UNCLAIMED PROPERTY
12/17/2019	09368L100	BLOCKCHAIN INDS INC USD 0.001	-200.000	$ 4.31	$ 862.00	$ (28.00)	$ -	$ -	$ -	$ 834.00	SELL	SPRO// CNDT STATE LOCAL SOLUTIONS		UNCLAIMED PROPERTY
12/17/2019	24373L102	DEEP GREEN WASTE + RECYCLING IN NPV	-22.000	$			$ -	$ 0.15	$ 3.30	$ (3.08)	SELL	SPRO// CNDT STATE LOCAL SOLUTIONS		UNCLAIMED PROPERTY
12/17/2019	92846K100	VITA MOBILE SYS INC NPV	-100.000	$ 0.03	$ 3.00	$ (0.01)	$ -	$ -	$ -	$ 2.99	SELL	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				

AVENU
INSIGHTS & ANALYTICS

AVENU INSIGHTS & ANALYTICS

Weekly/Other Proceeds Wire Report - Sample Report

Actual Settle Date	CUSIP/CINS	Security Short Description	Shares / Par	Local Price	Local Rate	Local Principal Amount	Commission	Local Income Amount	Miscellaneous Fees	Foreign Exchange Fees	Local Amount	Transaction Type Name	Transaction Description 1	Transaction Description 2
12/6/2019	31641P302	FIDELITY SYSTEMATIC INVT PLANS	0.941	$ -	$	(40.65)	$ -	$ -	$ -	$ -	$ (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)	$ -	$ -	$ -	$ -	$ (0.03)	CORPORATE ACTION	C/DECL// US3536126820 150527561	C/DECL// US3536126820 150527561
12/2/2019	354014102	FRANKLIN M COM USD0.01	0.020	$ -	$	(0.02)	$ -	$ -	$ -	$ -	$ (0.02)	CORPORATE ACTION	C/DECL// US3540141021 149655680	C/DECL// US3540141021 149655680
12/2/2019	416645596	THE HARTFORD MUTUAL FUNDS, INC. -	0.150	$ -	$	(3.68)	$ -	$ -	$ -	$ -	$ (3.68)	CORPORATE ACTION	C/DECL// US4166455968 149656027	C/DECL// US4166455968 149656027
12/3/2019	46131G406	INVESCO SE CLASS IB	2.942	$ -	$	(19.80)	$ -	$ -	$ -	$ -	$ (19.80)	CORPORATE ACTION	C/DECL// US46131G4064 149933834	C/DECL// US46131G4064 149933834
12/12/2019	37733W105	GLAXOSMITHKLINE PLC 25P ADR	1.000	$ 0.50	$	-	$ -	$ 0.50	$ -	$ -	$ 0.50	DIVIDEND	PSS #: 1805096075612 UNITS/QNTY: 1.0000	SEDOL #: 2374112 ISIN #: US37733W1053 EVENT ID: 0145628242
12/29/2019	060505104	BK OF AMER COM USD0.01	132.000	$ 0.12	$	-	$ -	$ 15.84	$ -	$ -	$ 15.84	DIVIDEND	PSS #: 1805306079309 UNITS/QNTY: 132.0000	SEDOL #: 2295677 ISIN #: US0605051046 EVENT ID: 0145647639
12/29/2019	713448108	PEPSICO INC USD 0.017	3.000	$ 0.93	$	-	$ -	$ 2.78	$ -	$ -	$ 2.78	DIVIDEND	PSS #: 1805306092757 UNITS/QNTY: 3.0000	SEDOL #: 2681511 ISIN #: US7134481081 EVENT ID: 0146270822
12/29/2019	74251V102	PRINCIPAL COM USD0.01	42.000	$ 0.52	$	-	$ -	$ 21.84	$ -	$ -	$ 21.84	DIVIDEND	PSS #: 1806046016649 UNITS/QNTY: 42.0000	SEDOL #: 2803014 ISIN #: US74251V1026 EVENT ID: 0145664920
12/17/2019	23355L106	DXC TECHNOLOGY CO USD 0.01	62.000	$ 0.19	$	-	$ -	$ 11.78	$ -	$ -	$ 11.78	DIVIDEND	PSS #: 1806046111071 UNITS/QNTY: 62.0000	SEDOL #: BYXD7B3 ISIN #: US23355L1061 EVENT ID: 0147286359
12/5/2019	745867101	PULTE GROUP INC	541.000	$ 0.09	$	-	$ -	$ 48.69	$ -	$ -	$ 48.69	DIVIDEND	PSS #: 1806056056935 UNITS/QNTY: 541.0000	SEDOL #: 2708841 ISIN #: US7458671010 EVENT ID: 0146764669
12/2/2019	320517105	FIRST HORIZON NATL CORP USD 0.625	5.000	$ 0.12	$	-	$ -	$ 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	$ 0.18	$	-	$ -	$ 28.62	$ -	$ -	$ 28.62	DIVIDEND	PSS #: 1806066137254 UNITS/QNTY: 159.0000	SEDOL #: B0SRLH6 ISIN #: US1248572026 EVENT ID: 0147350873
12/5/2019			24.810	$ 1.31	$	-	$ -	$ -	$ -	$ -	$ 24.81	FOREIGN EXCHANGE	PSS1805230005012	EXCH RATE : 1.31425510000 THEIRS TRADE DT :29JUN18
12/5/2019			-18.880	$ 1.31	$	24.81	$ -	$ -	$ -	$ -	$ 24.81	FOREIGN EXCHANGE	PSS1805230005012	EXCH RATE : 1.31425510000 OURS TRADE DT :29JUN18
12/16/2019	312903SA6	FEDERAL HOME LN MTG 6.5195 15JUL21	20000.000	$ 0.00	$	-	$ -	$ 0.16	$ -	$ -	$ 0.16	INTEREST	PSS #: 1806146213965 UNITS/QNTY: 20,000.0000	SEDOL #: ISIN #: US312903SA62 EVENT ID: 0147010204
12/16/2019	06050XA94	BANK AMER CORP SUB INT 6.05 15FEB38	150000.000	$ 0.01	$	-	$ -	$ 756.25	$ -	$ -	$ 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	$ -	$ -	$ 0.51	INTEREST	PSS #: 1806296354572 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	$ 0.00	$	-	$ -	$ 0.62	$ -	$ -	$ 0.62	INTEREST	PSS #: 1806296580764 UNITS/QNTY: 25,000.0000	SEDOL #: ISIN #: US36203LBX91 EVENT ID: 0146695674
12/12/2019	26842F103	E-DIRECT INC NPV	1344.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	INTERNAL MOVEMENT	1181920119206	
12/12/2019	26842F103	E-DIRECT INC NPV	-1344.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	INTERNAL MOVEMENT	DTC ARF # 20171009DTC 9002	AWAITING SECURITY FROM REGISTR
12/5/2019	918231101	VHGI HLDGS INC USD 0.0001	100000.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	INTERNAL MOVEMENT	DTC ARF # 20171009DTC 9010	1181860102907
12/5/2019	918231101	VHGI HLDGS INC USD 0.0001	-100000.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	INTERNAL MOVEMENT	DTC ARF # 20171009DTC 9010	AWAITING SECURITY FROM REGISTR
			0.000	$ -	$	-	$ -	$ 0.34	$ -	$ -	$ 0.34	OTHER	CR INTEREST-ACCOUNT 9124838400	
			0.000	$ -	$	-	$ -	$ 0.01	$ -	$ -	$ 0.01	OTHER	CR INTEREST-ACCOUNT 9124838401	
12/16/2019	312903SA6	FEDERAL HOME LN MTG 6.5195 15JUL21	20000.000	$ -	$	2.65	$ -	$ -	$ -	$ -	$ 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	$ -	$	0.88	$ -	$ -	$ -	$ -	$ 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	$ -	$ -	$ -	$ -	$ 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	$ -	$	-	$ -	$ -	$ -	$ -	$ -	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	$ -	$	-	$ -	$ -	$ -	$ -	$ -	SECURITY DEPOSIT	B/C A REC FROM MORGAN STANLEY	AWAITING SECURITIES FROM CPY
12/29/2019	N72482123	QIAGEN NV EUR 0.01	296.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	SECURITY DEPOSIT	B/C A REC FROM MORGAN STANLEY	AWAITING SECURITIES FROM CPY
12/5/2019	896887106	TROILUS GOLD CORP NPV	-2.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	SECURITY WITHDRAWAL	6/29/19 SALE, PROCEEDS POST	SEPERATE
12/9/2019	4812A4385	JP MORGAN STRG INCM CL A	-1150.501	$ -	$	-	$ -	$ -	$ -	$ -	$ -	SECURITY WITHDRAWAL	CL 1018837, LUCINDA J MAR 27	TH ST RENTON MA 98056 W-9 NOT
12/29/2019	140193103	CAP INC BU SBI NPV	-167.149	$ -	$	-	$ -	$ -	$ -	$ -	$ -	SECURITY WITHDRAWAL	CL 11881, CAROL LIMIAS 32	6TH AVE NW SEATTLE WA 98117 W-9
12/12/2019	22160K105	COSTCO WHOLESALE CORP NEW USD 0.005	-1100.000	$ -	$	-	$ -	$ -	$ -	$ -	$ -	SECURITY WITHDRAWAL	FERN TRUCANO DTC 104	A/C 5680992
											$ 835.08			

AVENU INSIGHTS & ANALYTICS

Position – Unable to Trade Report

AVENU INSIGHTS & ANALYTICS

Position - Unable to Trade Report

AC #	Security Description	Days	Units	CUSIP	Location	Comments
xxxxxx	ACT TELECONFERENCING INC	381.00	810.000	000955104	NYC	private company - no market
xxxxxx	ADEX MINING INC	786.00	540.000	006903207	NYC	chilled for deposit has value cannot sell
xxxxxx	ALL STATE PROPERTIES HOLDINGS	1,660.00	1.000	016663205	NYCR	RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
xxxxxx	ALTAIR NANOTECHNOLOGIES INC NPV	88.00	223.0000	021373303	DTC	RESTRICTED FROM TRADING PER BROKER
xxxxxx	ANDALAY SOLAR INC USD 0.001	94.00	75.0000	033355108	DTC	RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
xxxxxx	ARETE INDS INC NPV	101.00	3.0000	040098303	DTC	RESTRICTED - RAYMOND JAMES CANNOT SELL THEM
xxxxxx	ATLANTIC WIND & SOLAR INC	324.00	72.000	049127103	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		1.0000	053801304	DTC	restricted from trading per raymond james
xxxxxx	B-FAST CORP	381.00	570.000	055413108	DTC	restricted from trading per raymond james
xxxxxx	BETTWORK INDS INC USD 0.001	94.00	1.0000	087766101	DTC	restricted from trading per raymond james
xxxxxx	BIG BUCK B COM USD0.01	86.00	24.0000	089072300	DTC	restricted from trading per raymond james
xxxxxx	BIOSYNERGY INC NPV	72.00	4,000.0000	090917105	DTC	restricted from trading per raymond james
xxxxxx	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	125286104	DTC	restricted from trading per raymond james
xxxxxx	CAMPBELL R COM NPV	1,526.00	10.0000	134422609	YCA	cant be sold has no value on foreign marekt
xxxxxx	CANNABIS SCIENCE INC	304.00	170.000	137648101	DTC	this security is restricted from trading
xxxxxx	CARDIOVASCULAR BIOTHERAPEUTICS	157.00	780.000	141607101	NYC	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 COM	2,151.00	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

LOT LEVEL VALUATION REPORT

Reporting Account Name	Reporting Account Number	CUSIP	Security Description	Ticker	ISIN	Units	Base Price	Base Market Value	Reported Date
STATE OF MAINE	AUZFXXXXXXXX	88579Y101	3M CO	MMM	US88579Y1010	24.000	153.650000	3,687.60	4/30/2018
STATE OF MAINE	AUZFXXXXXXXX	1785L302	727 COMMUNICATIONS INC	SVNJ	US1785L3024	6.000	0.000000	0.00	11/9/2019
STATE OF MAINE	AUZFXXXXXXXX	00282410	ABBOTT LABORATORIES	ABT	US0028241000	10.000	94.950000	949.50	10/8/2016
STATE OF MAINE	AUZFXXXXXXXX	00282410	ABBOTT LABORATORIES	ABT	US0028241000	14.000	94.950000	1,329.30	8/9/2019
STATE OF MAINE	AUZFXXXXXXXX	00287Y109	ABBVIE INC	ABBV	US00287Y1091	25.000	84.690000	2,117.25	4/6/2020
STATE OF MAINE	AUZFXXXXXXXX	00287Y109	ABBVIE INC	ABBV	US00287Y1091	10.000	84.690000	846.90	11/4/2019
STATE OF MAINE	AUZFXXXXXXXX	00287Y109	ABBVIE INC	ABBV	US00287Y1091	14.000	84.690000	1,185.66	11/4/2019
STATE OF MAINE	AUZFXXXXXXXX	003 26L100	ABERDEEN TTL DYN DIVID	AOD	US003 26L1008	224.000	7.040000	1,576.96	3/30/20 20
STATE OF MAINE	AUZFXXXXXXXX	00350 1103	ABIL TY HOLDING CORP	AYHC	US00350 11032	681.000	0.000000	0.00	3/30/20 20
STATE OF MAINE	AUZFXXXXXXXX	0043 1N108	ACCESS-POWER INC	ACCR	US0043 1N1081	3,100.000	0.000000	0.00	2/2/2016
STATE OF MAINE	AUZFXXXXXXXX	0043 1N108	ACCESS-POWER I C	ACCR	US0043 1N1081	15,000.000	0.000000	0.00	3/10/2015
STATE OF MAINE	AUZFXXXXXXXX	0075 1Y106	ADVANCE AUTO PARTS INC	AAP	US0075 1Y1064	4.000	118.950000	475.80	10/31/2019
STATE OF MAINE	AUZFXXXXXXXX	0075 1Y106	ADVANCE AUTO PARTS INC	AAP	US0075 1Y1064	69.000	118.950000	8,207.55	11/25/2019
STATE OF MAINE	AUZFXXXXXXXX	0075 1Y106	ADVANCE AUTO PARTS INC	AAP	US0075 1Y1064	69.000	118.950000	8,207.55	10/2/2019
STATE OF MAINE	AUZFXXXXXXXX	007903 107	ADVANCED MICRO DEVICES INC	AMD	US007903 1078	4.000	56.490000	225.96	10/4/2019
STATE OF MAINE	AUZFXXXXXXXX	007903 107	ADVANCED MICRO DEVICES INC	AMD	US007903 1078	5,100.000	56.490000	288,099.00	12/2/2019
STATE OF MAINE	AUZFXXXXXXXX	140543 109	AF CAP WLRD GR &INC-A	CWGI	US 140543 1099	250.512	44.720000	11,202.90	12/27/2019
STATE OF MAINE	AUZFXXXXXXXX	140543 109	AF CAP WLRD GR &INC-A	CWGI	US 140543 1099	2.134	44.720000	95.43	12/2/2019
STATE OF MAINE	AUZFXXXXXXXX	140543 109	AF CAP WLRD GR &INC-	CWGI	US 140543 1099	138.221	44.720000	6,181.24	12/2/2019
STATE OF MAINE	AUZFXXXXXXXX	140543 109	AF CAP WLRD GR &INC-	CWGI	US 140543 1099	0.694	44.720000	31.04	10/5/2019
STATE OF MAINE	AUZFXXXXXXXX	140543 109	AF CAP WLRD GR &INC-	CWGI	US 140543 1099	24.684	44.720000	1,103.87	9/3/2019
STATE OF MAINE	AUZFXXXXXXXX	008 27A108	AFFILIATED RESOURCES CORP	AFFL	US008 27A1088	750.000	0.000000	0.00	9/30/2019
STATE M	AUZFXXXXXXXX	0 8474 18	AGN O AGLE M TD	M	CA008474 185	18.000	60.820000	1,094.76	10/11/219
STATE OF MAINE	AUZFXXXXXXXX	0 1387 2106	ALCOA ORP	AA	US0 1387 21065	8.000	7.370000	58.96	11/29/2019
STATE OF MAINE	AUZFXXXXXXXX	0 1479R 100	ALEXANDRIA ADVANTAGE WARRANTY	AAWC	US0 1479R 1005	3.000	0.002000	0.00	12/31/2019
STATE OF MAINE	AUZFXXXXXXXX	0 1479R 100	ALEXANDRIA ADVANTAGE WARRANTY	AAWC	US0 1479R 1005	1.000	0.002000	0.01	3/2/20 20
STATE OF MAINE	AUZFXXXXXXXX	0 1535P 106	ALEXCO RESOURCE CORP	AXU	CA0 1535P 1062	300.000	1.540000	462.00	10/2019
M	01 58 11 8		M		18 11 2	4.000	41.390000	165.56	4/13/20 20
STATE OF MAINE	AUZFXXXXXXXX	0 1891947 2	ALLI NZGI TECHNOLOGY-	RAGT	US0 1891947 25	76.061	56.760000	4,317.22	4/6/20 20
STATE OF MAINE	AUZFXXXXXXXX	0 1988P 108	ALLSCRIPTS HEALTHCARE SOLUTION	MDRX	US0 1988P 1084	121.000	6.680000	808.28	4/20/20 20
STATE OF MAINE	AUZFXXXXXXXX	0 1988P 108	ALLSCRIPTS HEALTHCARE SOLUTION	MDRX	US0 1988P 1084	121.000	6.680000	808.28	4/27/20 20
STATE NA ME	AUZFXXXXXXXX	200 21014	ALLSTATE ORP HE	ALL	US 200 210 14	444.000	103.090000	45,771.96	4 2 20
STATE OF MAINE	AUZFXXXXXXXX	2209S 103	ALTRI GROUP I C	M	US0 2209S 1033	1.000	39.750000	39.75	4/3/20 20
SAT M	AZFX XXX X	2209 10	OUP I C	M	S 22 S1 3	16.000	39.750000	636.00	4/14/20 20
STAT M	AZFXXXXXXXX	2209S 10	ALTR OUP I C	M	US 220 S103	16.000	39.750000	636.00	4/17/20 20
STATE OF MAINE	AUZFXXXXXXXX	23135106	AMAZON.CO M INC	AMZN	US0 23135 1067	39.000	2,376.000000	92,664.00	4/20/20 20
STATE M	AUZFXXXXXXXX	23375 108	AMCAP UND	AMCP	US 23375 10 2	249.598	31.090000	7,760.00	4/21/20 20
STATE OF MAINE	AUZFXXXXXXXX	23436 108	AMEDISYS INC	AMED	US0 23436 1089	38.000	191.990000	7,295.62	4/22/20 20
STATE OF MAINE	AUZFXXXXXXXX	36080 2102	AMER FND FND MNTL INVST	ANCF	US36080 21024	363.378	53.860000	19,571.54	4/23/20 20
STATE OF MAINE	AUZFXXXXXXXX	36080 2102	AMER FND FND MNTL INVST	ANCF	US36080 21024	152.392	53.860000	8,207.83	4/24/20 20
M	3 21 2		M M		60 21 24	38.561	53.860000	2,076.90	4/27/20 2
STATE OF MAINE	AUZFXXXXXXXX	399874 106	AMER FND GRW FD AM-A	AGTH	US399874 1066	335.042	48.970000	16,407.01	12/28/2018
STATE OF MAINE	AUZFXXXXXXXX	399874 106	AMER FND GRW FD AM-A	AGTH	US399874 1066	190.026	48.970000	9,305.57	10/1/2016
STATE OF MAINE	AUZFXXXXXXXX	399874 106	AMER FND GRW FD AM-A	AGTH	US399874 1066	47.164	48.970000	2,309.62	10/31/2019
STATE OF MAINE	AUZFXXXXXXXX	399874 106	AMER FND GRW FD AM-A	AGTH	US399874 1066	13.042	48.970000	638.67	11/2019
STATE OF MAINE	AUZFXXXXXXXX	399874 106	AMER FND GRW FD AM-A	AGTH	US399874 1066	27.328	48.970000	1,338.25	10/2/2019
STATE OF MAINE	AUZFXXXXXXXX	46 1308 108	AMER FND INV CO OF A M-A	AVS	US46 1308 1086	604.420	35.170000	21,257.46	11/5/2019
STATE OF MAINE	AUZFXXXXXXXX	46 1308 108	AMER FND INV CO OF A M-A	AVS	US46 1308 1086	175.964	35.170000	6,188.65	10/28/2019
STATE OF MAINE	AUZFXXXXXXXX	83 16811 01	AMER FND S MALLCAP WRLD-A	SMCW	US83 16811012	484.828	51.190000	24,818.34	10/2/2019
STATE OF MAINE	AUZFXXXXXXXX	83 16811 01	AMER FND S MALLCAP WRLD-A	SMCW	US83 16811012	54.284	51.190000	2,778.80	10/6/2019

Worthless Report

.XLS Format

Worthless Report

						50,000.0000	0.000000	0.00	0.00
						2,844.0000	0.000000	0.00	0.00
						1,471.0000	0.000000	0.00	0.00
						20.0000	0.000000	0.00	0.00
						11,378.0000	0.000000	0.00	0.00
						50.0000	0.000000	0.00	0.00
						2,991.0000	1.000000	2,991.00	2,991.00
						150.0000	0.000000	0.00	0.00
									2,991.00

Entitlement Calculations

Claimant: **First/Last Name**
CUSIP: 028837102
Original # of shares: 2.5470 4/22/1997
Claim# **763855**

ISSUE NAME	TYPE	RATE	RECORD DATE	PAYMENT DATE	SHARE BALANCE	CASH DIVIDEND	SHARE PRICE	SHARE DIVIDEND
Ending Balance					**7.017**			
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0	12/27/2017	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	12/28/2016	12/31/2016	6.513	$ 0.90	$ 14.79	0.061
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Dividend	0.388	11/30/2015	11/30/2015	6.343	$ 2.46	$ 14.43	0.171
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0	12/31/2010	12/31/2010	6.343	$ -	$ -	0.000
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Omitted	0	12/31/2009	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	12/30/2008	1/5/2009	4.913	$ 7.72	$ 5.40	1.430
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	0.2976	12/26/2007	1/2/2008	4.770	$ 1.42	$ 14.07	0.101
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Dividend	0.1252	12/26/2007	1/2/2008	4.770	$ 0.60	$ 14.07	0.042
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Dividend	0.03995	12/28/2006	12/28/2006	4.122	$ 0.16	$ 12.57	0.013
AMERICAN PENSION INVS TRUST -CUSIP 028837870	Capital Gain	1.93606	12/28/2006	12/28/2006	4.122	$ 7.98	$ 12.57	0.635

10/27/2004 Exchange class shares from CUISP 028837102 / class C to 028837870 / class A rate 1:0.9962.

					4.137			
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.543	12/28/2001	12/31/2001	3.921	$ 2.13	$ 9.84	0.216
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.3	12/27/2000	12/29/2000	3.829	$ 1.15	$ 12.52	0.092
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.4	6/5/2000	6/6/2000	3.505	$ 4.91	$ 15.11	0.325
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.22	12/29/1999	12/31/1999	3.457	$ 0.76	$ 15.97	0.048
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.52	9/29/1999	10/1/1999	3.093	$ 4.70	$ 12.91	0.364
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.046	12/17/1998	12/28/1998	2.864	$ 3.00	$ 13.08	0.229
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	0.22	12/29/1997	1/9/1998	2.816	$ 0.62	$ 12.97	0.048
AMERICAN PENSION INVS TRUST-CUSIP 028837102	Capital Gain	1.35	11/13/1997	11/14/1997	**2.547**	$ 3.44	$ 12.78	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: **Last/First Name**
CUSIP: 74441R508
Original # of shares: 120.0000
Type: **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	12/31/2019	12/31/2019	123.140	$ 3.17		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02633	11/29/2019	11/29/2019	123.140	$ 3.24		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02637	10/31/2019	10/31/2019	123.140	$ 3.25		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02382	09/30/2019	09/30/2019	123.140	$ 2.93		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02828	08/30/2019	08/30/2019	123.140	$ 3.48		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.0279	06/31/2019	06/31/2019	123.140	$ 3.44		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02528	05/28/2019	05/28/2019	123.140	$ 3.11		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02886	05/31/2019	05/31/2019	123.140	$ 3.55		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02659	04/30/2019	04/30/2019	123.140	$ 3.27		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02687	03/29/2019	03/29/2019	123.140	$ 3.31		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02434	02/28/2019	02/28/2019	123.140	$ 3.00		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02665	01/31/2019	01/31/2019	123.140	$ 3.28		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02485	12/31/2018	31 DEC 18	123.140	$ 3.06		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.00107	12/20/2018	21 DEC 18	123.140	$ 0.13		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02703	11/30/2018	30 NOV 18	123.140	$ 3.33		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02603	10/31/2018	10/31/2018	123.140	$ 3.21		
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02281	9/28/2018	9/28/2018	122.879	$ 2.80	$ 10.75	0.2607
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02816	8/31/2018	8/31/2018	122.560	$ 3.45	$ 10.79	0.3199
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02499	7/31/2018	7/31/2018	122.276	$ 3.06	$ 10.76	0.2841
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02668	6/29/2018	6/29/2018	121.973	$ 3.25	$ 10.76	0.3024
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02552	5/31/2018	5/31/2018	121.686	$ 3.11	$ 10.80	0.2875
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02369	4/30/2018	4/30/2018	121.419	$ 2.88	$ 10.78	0.2669
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02592	3/29/2018	3/29/2018	121.129	$ 3.14	$ 10.82	0.2901
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02253	2/28/2018	2/28/2018	120.878	$ 2.72	$ 10.85	0.2511
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02483	1/31/2018	1/31/2018	120.603	$ 2.99	$ 10.91	0.2744
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02502	12/29/2017	12/29/2017	120.329	$ 3.01	$ 10.98	0.2741
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.00602	12/21/2017	12/22/2017	120.263	$ 0.72	$ 10.97	0.0660
PRUDENTIAL SHORT-TERM CORPORAT	Dividend	0.02411	11/30/2017	11/30/2017	**120.000**	$ 2.89	$ 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	TYPE	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 CUSIP 018918649	**312.231**
Liq proceeds:	**$8,945.42**
Dividends Paid in Cash	**$0.00**
TOTAL:	**$8,945.42**

S□□ □ □r□ □□ttle□e□t □□l□□l□to□ □□□l□s□s

[illegible]	□r□□□□□□□□□□□	[illegible]	□□□□r□□□□ □	[illegible]	[illegible]	□r□□□	□□□□r□□□□d□	[illegible]	[illegible]
[illegible]	Sell	[illegible]	□W□R□ □□□ M□SS □SD □□□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Sell	[illegible]	□M□R□□□ S□P□R□O□D□□TOR □O □SD □□□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Sell	[illegible]	□O□□ □ORP □□□ □□□ □DR	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Sell	[illegible]	□ROO□S □□TOM□T□O□ □□□ □□W □SD □□□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Sell	[illegible]	T□MO□L□ □S □□□ □SD □□□□□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	□L	[illegible]	T□MO□L□ □S □□□ □SD □□□□□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
								[illegible]	□□□□□□2□3□21

[illegible]

[illegible]

[illegible]	9□□□□□
[illegible]	1□□□□9
□M□□□□□□r□□□□□□□d□	1□□□□□
[illegible]	□□□□□□□□□2□

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

FORVIS

An Independent Service Auditor Report issued by
FORVIS, LLP

Table of Contents

FORVIS

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.

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 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.

FORVIS

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

AVENU
INSIGHTS & ANALYTICS

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;

        b. 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:

1. 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 twenty-nine 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, re-registration, 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 time-sensitive 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 co-location 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: • Controls around the physical security of the Data Centers hosting the in-scope applications, and • Controls around the environmental protections at the Data Centers hosting the in-scope applications.	Control Objective 1*

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Control Objectives
	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.	
The Bank of New York Mellon Corporation ("BNY Mellon")	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: • Controls around the design and operation of holding securities in support of user entities, and • Controls around the design and operation of account maintenance in support of user entities. 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.	Control Objective 6* Control Objective 7* Control Objective 11*

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Control Objectives
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: • Controls around the design and operation of processing liquidations and accurately applying commission and SEC charges to processed transactions, and • Controls around the design and operation of accurately performing the research and portfolio valuations in compliance with internal controls. 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.	Control Objective 9*

* 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*

* 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 of the control
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its 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

Control Objective 1			
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.			
Control 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.

Control Objective 1			
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.			
Control 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.

Control Objective 2			
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.			
Control 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.	Observed the production, development, and 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.

Control Objective 3			
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.			
Control 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 in-scope 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.

Control Objective 3			
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.			
Control Activity Description		**Tests Performed by Service Auditor**	**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.	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.	No exception noted.
3.05	On an annual basis, all changes to the production environment related to the in-scope 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 Software Engineer II 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.

Control Objective 4			
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.			
Control 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.

Control Objective 4			
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.			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		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.	No exceptions noted.
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.	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.	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.	Observed the password configurations that governed user access to the network infrastructure and operating system resources to determine that password parameters for the network infrastructure and operating system resources were configured to require: • Expiration, • Minimum length, • History, • Complexity, and • Lockout after unsuccessful login attempts. Further, inquired of the Senior Engineer Servers, Storage, Virtualization to determine that these configurations were in place throughout the specified period.	No exceptions noted.

Control Objective 5			
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**
5.01	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 in-scope 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.

Control Objective 5			
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.

Control Objective 5			
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**
5.07	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.	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.			
Control 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 amounts are posted to the state's account via NEXEN®, which is reviewed by an Account Administrator.	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.
		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 received from BNY Mellon to help ensure that property is properly credited to state accounts.	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.
		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.			
Control 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.

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.			
Control 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, 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.	Inspected the remittance summary spreadsheets related to a sample of entitlement calculations and claim payments to determine that, for participating states, a remittance summary spreadsheet, including entitlement calculations and/or claim payments, was prepared by an Account Administrator and was reviewed by the unit manager of custody or an appropriate designee for accuracy for each selected entitlement calculation and/or claim payment. 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.	No exceptions noted.
8.02	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.	Inspected the state instructions, check approval, and transmission documentation related to a sample of check claim payments for participating states to determine that for each selected check claim payment for participating states, if cash was due to the owner and the state had elected Avenu to pay the owner (claimant), a check for the amount due was approved by the unit manager of custody or an appropriate designee and was forwarded to the owner upon settlement, in accordance with state instructions.	No exceptions noted.

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 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.	Inspected the confirmation and approval documentation related to a sample of liquidation requests received via Avenu extranet or eFax to determine that authorized state signatures were confirmed by management for each selected liquidation request and that each selected request was approved by the unit manager of custody or an appropriate designee for trade entry.	No exceptions noted.
9.02	Each liquidation request is reviewed by an Account Administrator to confirm posting in accordance with state instructions. Any identified discrepancies are researched and resolved.	Inspected the liquidation request documentation related to a sample of liquidation requests to determine that each selected liquidation request 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 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**	**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 e-mail, 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.			
Control Activity Description		**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

FORVIS

An Independent Service Auditor Report issued by
FORVIS, LLP

Table of Contents

FORVIS

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.

FORVIS

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.

FORVIS

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

AVENU
INSIGHTS & ANALYTICS

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 Server
UPS2000	Delphi-based software	Microsoft Windows Server
Holder Reporting Website	Web-based SaaS	Microsoft Windows Server
MissingMoney.com	Web-based SaaS	Microsoft Windows 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.

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-Applicable Trust Services Criteria		**Avenu Insights & Analytics' Rationale**
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: • Controls around the physical security of the Data Centers hosting the in-scope applications, • Controls around the environmental controls at the Data Centers hosting the in-scope applications to support the disaster recovery processes, and • Controls around the antivirus, patching, and server management for the Data Centers hosting the in-scope applications. 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.	CC 6.1*, CC 6.4*, CC 6.8*, CC 8.1*

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: • Controls around the physical security of the Data Centers hosting the in-scope applications, • Controls around logical access and change management of the infrastructure supporting the in-scope applications, and • Controls around the environmental controls at the Data Centers hosting the in-scope applications to support the disaster recovery processes. 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.	CC 6.1*, CC 6.2*, CC 6.4*, CC 7.5*, CC 8.1*, CC 9.2*

* 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*, CC 6.8*

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*

* 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, for accuracy of 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.

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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and 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			
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 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, and annually thereafter.	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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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, e-mail, 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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, 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.	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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity 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 include the applicable security practices and commitments.	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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
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.
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 CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity 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 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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity 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 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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 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, implementation, and operation of systems affecting system security.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
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			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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 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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
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 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity 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 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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
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 nature of the suspected ethics/policy violation claim or suspected security incident.	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.
		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 Activity 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, e-mail, 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
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.
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
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, 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.
		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.	

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
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 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
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, e-mail, 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
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.
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity 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 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.
		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 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
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 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.
		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.

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 3.1-02	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.

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 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
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.

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 3.2-02	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.

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 include the applicable security practices and commitments. (CC 1.3-03)	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.
		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.

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**
		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 3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
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.

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 3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
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.

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**
		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.

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 3.4-04	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 noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control 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. (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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity 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.
CC 4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity 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.
		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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity 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 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.

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 5.1 - 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.	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 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.

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**
		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 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 5.1-05	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 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.
		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.

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 5.1-06	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.
CC 5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
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 Activity 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 in-scope 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 Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.2-04	The Company has documented a formal Change Management Policy which governs the design, implementation, modification, and management of the in-scope applications and related databases.	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.
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.

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 5.2-07	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 in-scope applications, and the related databases to determine that a valid user ID and password were required to access the Company's network, in-scope 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.
CC 5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
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 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	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 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.

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 5.3-04	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.

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**
		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, e-mail, 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.

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**
		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 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 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 CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-04	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 in-scope 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 6.1-05	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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-07	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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-09	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 in-scope applications, and the related databases to determine that a valid user ID and password were required to access the Company's network, in-scope 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.
CC 6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.2-02	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 in-scope 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 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
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 in-scope 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.5 - 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.
CC 6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6-03	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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6-05	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 in-scope 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 - 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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)	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 6.7-09	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 in-scope 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 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 6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
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 in-scope 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 in-scope 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8-03	On an annual basis, all changes to the production environment related to the in-scope 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 in-scope 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 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 CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8-06	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.

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 7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
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.
CC 7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
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.
		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 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.

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**
		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.

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 7.3-05	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 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.
		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.

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**
		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.

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 7.4 - 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.	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 7.4-02	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.

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**
		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.

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 7.4-05	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 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.
		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.

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**
		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 7.4-07	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.

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 7.5 - 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 Activity 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.

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**
		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 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 Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1-03	Access to promote changes into the production environment related to the in-scope 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 in-scope 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.2 - The entity assesses and manages risks associated with vendors and business 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity 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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**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 include the applicable security practices and commitments. (CC 1.3-03)	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.
		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.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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

Confidential

STOP

I an **D M**
D R or noti i ation o a **D R**
D R D lease ro eed to
r

Security and Privacy Directive

Table o Contents

Contents

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 [redacted] Canton Street [redacted] floor Quincy, MA. It is intended to define the scope, with descriptions of 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 [redacted] Canton 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 [redacted] 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 [redacted] 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 [redacted] have received training in their respective areas of expertise. Avenu UPS products and services are based on proprietary processes and systems.

Avenu UPS performs core unclaimed property administration services that consist of the following:

- Unclaimed Property Management System
- 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

BCP	Business Continuity Plan
UPS	Unlaiaed Proerty Solutions
DRP	Disaster Reoery Plan
ICRC	Inident and Crisis Resonse Center
IMT	Inident Manaeent Tea
PHI	Personal ealth Inormation
PII	Personally Identiiable Inormation
RPO	Reoery Point Obeti e
RTO	Reoery Ti e Obeti e

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 delimited 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 fully 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 coordinated documented procedures so that recovery of the production environment is within predefined recovery time objectives.

2.2 Emergency Incident Procedures

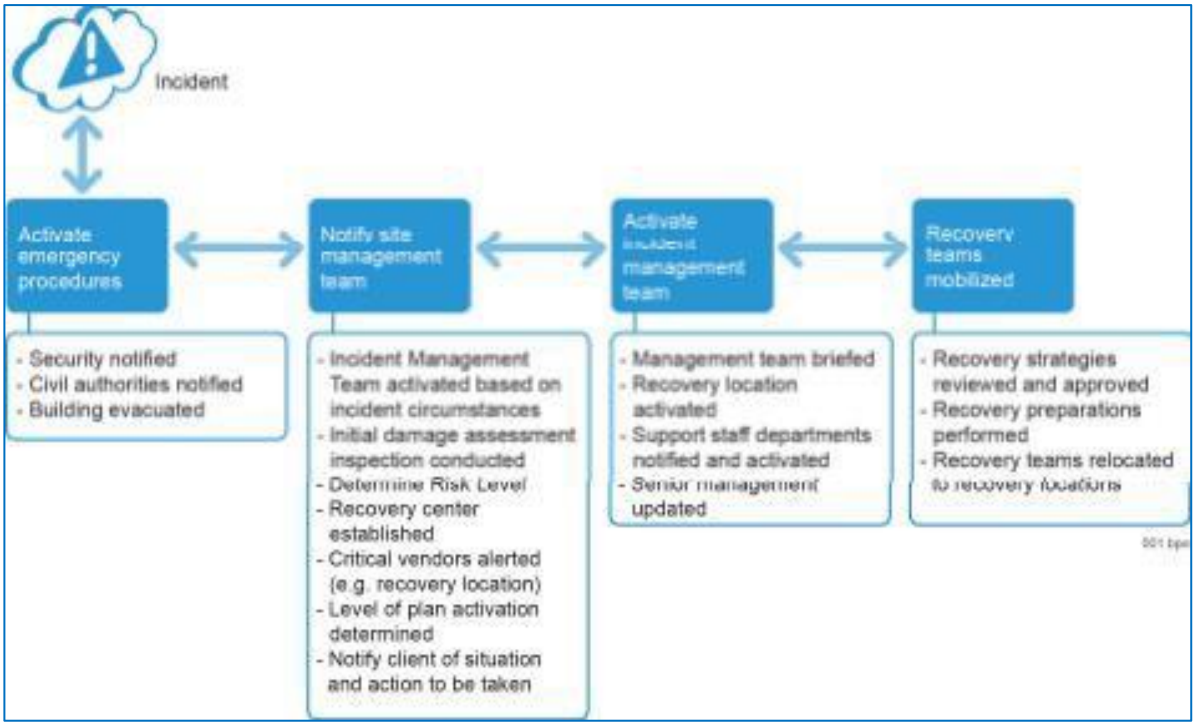
Emergency incident procedures refer to the predetermined actions that are performed immediately following an emergency incident. These procedures include coordination of the site initial response and recovery actions. Emergency incidents include but not limited to fire, medical emergency and/or illness, bomb threat, tornado, other 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, 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, 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.



[illegible]

2.3 Site Strategy Summary

This plan will provide established procedures for managing 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 reestablishing technical/telecommunications 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 (Agenu IT)
- Install Operating Systems (Agenu IT)
- End Systems to Restricted State (Agenu UT)
- Restore User Profiles (Agenu IT)
- Restore Configuration Objects (Agenu IT)
- Restore Libraries (NONSYS (Agenu IT)
- Restore Documents and Folders (Agenu IT)
- Restore Directories (Agenu IT)
- Verify All Production Data Restored (Agenu UPS)
- Restore Any Production Objects not Restored (Agenu IT)
- Restore Private Authorities (Agenu IT)
- Re-Configure Communications Resource (Agenu IT and UPS)
- Perform an Unattended IPL (Agenu IT)
- Verify System Integrity (Agenu IT and UPS)
- Turnover to Client for Application Testing (Agenu UPS)
- Add Temporary Application License Keys (Agenu IT)
- Application Verification (Agenu UPS)
- User Application Testing Complete (Agenu UPS)
- User Application Testing – Client (Agenu UPS)
- Tentative Testing Completion Praise (Agenu UPS)
- System Turnover (Agenu 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 for a temporary staffing and/or technical services agency or shift focus to other Agenu Insights Analytics, LLC locations.

In t□e e□ent t□at □rodu□tion o□erations relo□ates to anot□er □a□ility□e□ □loyees and□or te□ □orary □ersonnel □ill be res□onsible □or trans□ortin□ t□e□ sel□es to t□e alternate site or □or□in□ re□otely□

3 □UPS Incident Management Team

□ □en nor□al business o□erations are disru□ted by any e□ent□ t□ere are t□ree t□in□s t□at □a□e to be a□□o□ □is□ed i□ □ediately□

- Ensure t□e sa□ety and □el□are o□e□ □loyees□□ontra□tors and □artners o□A□enu Insi□□ts □ Analyti□s□ LLC UPS in t□e e□ent o□an e□er□en□y□
- E□e□ute t□e noti□i□ation □ro□ess to alert Site Mana□e□ent and to noti□y A□enu □ana□e□ent□
- Ma□in□use o□t□e resour□es at t□e lo□al □a□ility t□at □as been a□e□ted□assess t□e da□a□e □ui□□ly and deter□ine i□t□e site □ay be restored to □ull □rodu□tion status □it□in t□e establis□ed re□o□ery ti□e ob□e□ti□e□

A□enu Insi□□ts □ Analyti□s□LLC UPS □as establis□ed an In□ident Mana□e□ent Tea□ □IMT□ □or t□e UPS lo□ation at □□□ □an□o□□ Street□□uin□y□MA□T□is tea□ is res□onsible □or in□esti□atin□ and assessin□ t□e in□ident□□on□errin□ □it□ot□er su□□ort areas to □er□or□ an initial e□aluation and da□a□e assess□ent□□lannin□□ □oordinatin□□and e□e□utin□ t□e re□o□ery a□ti□ities□ Based u□on t□e In□ident Mana□e□ent Tea□ assess□ent□□lan a□ti□ation □ro□edures are eit□er initiated or ter□inated□ □ ile t□e □o□ □osition o□t□e tea□ □aries a□□ordin□ to the site's needs, it □enerally in□ludes Site Mana□e□ent□Senior Te□□ni□al and O□erational Mana□ers □ro□ t□e de□art□ents t□at □a□e been dire□tly a□e□ted by t□e in□ident□and □e□bers o□ t□e A□enu Insi□□ts □ Analyti□s□LLC UPS Ser□i□e Continuity Deli□ery Tea□ □ Ea□□ □e□ber o□t□e In□ident Mana□e□ent Tea□ is □ro□ided □it□ a □o□y o□t□e A□enu UPS Business Continuity □lan□

3.1 □UPS Incident Management Team Role and Participants

T□e UPS In□ident Mana□e□ent Tea□ is res□onsible □or □ana□in□ internal and e□ternal □o□□uni□ations□ dire□tin□ res□onse and re□o□ery a□ti□ities□□onitorin□ t□e re□o□ery □ro□ress□and □ro□idin□ or reallo□atin□ re□o□ery resour□es□T□e IMT □ill inter□a□e □it□ a□□ro□riate □i□l aut□orities as di□tated by t□e in□ident□

T□e UPS IMT leader's responsibilities include contacting all members of the UPS IMT a□ter bein□ noti□ied o□ the situation, determine with the team's input if a disaster should be declared, and communicating the situation □it□ t□e A□enu Insi□□ts □ Analyti□s□LLC Ser□i□e Continuity Deli□ery Tea□ and A□enu UPS E□e□uti□e Mana□e□ent□ A□enu UPS E□e□uti□e Mana□ers □ust be □onsulted □rior to any de□ision o□ disaster de□aration□ [redacted]

Ot□er UPS IMT □e□bers are □i□en t□e res□onsibility to □o□ □uni□ate to t□e essential in□ident tea□ leads t□at a disaster □as been de□lared and t□e dire□ti□es ro□ t□e IMT, do□u□ent t□e re□o□ery □ro□ress, □or□ □it□ □R on resol□in□ □ersonnel issues and□or □on□erns, address □inan□ial and □o□ □ensation issues, do□u□ent re□o□ery □osts, □oordinate internal □o□ □uni□ations a□on□ t□e in□ident re□o□ery tea□ s□and □oordinate □edia and e□ternal □o□ □uni□ations □it□ □lients and t□e A□enu Insi□□ts & Analyti□s, LLC Co□ □uni□ations & Publi□ Relations Mana□er.

Table 3-1 Se□ rvice Con inuity Delive ry Team □

Position □	Name □
A□enu, CTO	□re□ □ra□a□
A□enu, □i□e President, Te□□nolo□y	□o□an Milbrin□
A□enu, Dire□tor, Net□or□ O□erations IT In□rastru□ture	Mar□ Terrill
A□enu, Dire□tor o□ Se□urity	Allari□□ □reer
A□enu, □i□e President, So□t□are En□ineerin□	□ose□□ At□ell
A□enu, So□t□are En□ineer II	□ere□y Rosine

Table 3-2 Site Management Team □

Avenu Insights & Analytics, LLC	Name □
Mana□in□ Dire□tor	Da□id Le□oine
Dire□tor	Mar□ Ca□□rini
Dire□tor	Debora□ Arnold

Ea□□ □e□ber o□ t□e IMT s□ould □a□e a desi□nated ba□□u□alternate t□at □an □arry on in t□e e□ent o□ illness □durin□ or be□ore t□e e□er□en□y) or una□ailability. T□is □i□es □e□bers o□ t□e tea□ a □□an□e to rest i□ re□o□ery a□ti□ities are □ontinuous o□er an e□tended □eriod o□ ti□e. All a□□ro□riate □onta□t nu□bers □ust be do□u□ented □or ea□□ alternate.

It should be noted that all Agenu 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 Agenu 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 Agenu 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 Agenu Insights & Analytics, LLC Service Continuity Delivery Team and Agenu 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 Agenu Insights & Analytics, LLC Service Continuity Delivery Team and Agenu 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 Agenu will follow the Incident Response Policy

Throughout this process, it is essential that internal Agenu Insights & Analytics, LLC UPS communications occur freely between the damaged site, the recovery backup site, the Incident Management Team, and the Agenu Insights & Analytics, LLC Service Continuity Delivery Team. During the restoration process, it is imperative that internal status updates be provided at predefined intervals. See [illegible] Directory for office phone numbers and email 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 Agenu 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 Plans 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.

Recovery Director Address

Address

Plan Updates, Property Solutions	David Levine	Primary
Director, Claims, Calls, Holders Reports	Mary Cantrini	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, call down tree or notification software products 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 how any 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 take 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 [illegible]) will immediately notify the Avenu Insights & Analytics, LLC Service Continuity Delivery Team. (See Table [illegible]) 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 [illegible] for information on determining the location of the Crisis Command Center and [illegible].

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 [illegible] for office phone numbers and email 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 [illegible] for the procedures for communicating to the press/media.

[illegible]

[illegible]	[illegible]
Avenu Insights & Analytics, LLC Corporate Marketing & PR 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 Resource Management.

[illegible]

[illegible]	[illegible]
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. [illegible] 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 email 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 [illegible] 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 o[illegible]limits then the UPS Management team will contact all IMT members to report to Best Western Ada's Inn.

  The UPS IMT will designate this location as the "Command Center" until the damage assessment has been received. Based on the damage assessment report initiation of the plan will be determined. Refer to [illegible] **r[illegible]d[illegible]r[illegible]d[illegible]r**.

- 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 Co[illegible]and Center location for instructions on relocating production operations to another facility. The IMT leader will instruct the other IMT members to co[illegible]unicate 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 deal with what has happened and to begin the disaster recovery processes.

7.1 Facilities / Security Team Assignment

In 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. In 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. In the Business Continuity Coordinator or Account Manager is unavailable contact the Avenu Insights Analytics LLC Service Continuity Delivery Team (see Table [illegible]) to assist in designating a Facilities/Security Team. This team will normally be comprised of a small group of 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 [illegible] for [illegible]).

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 anything broken out are people really 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 is/not actually be a disaster or not. Not all emergency conditions result in a disaster. In this initial assessment phase, initial 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, later as much information as possible from what resources are available. This could be witnesses, local authorities, or property management, later all details about of the situation noting the source and credibility. Use the Disaster Assessment Checklist as a tool to document details. (See [illegible] Document [illegible]).

While conducting a physical inspection, be aware of water exposed electrical, mechanical, fire, smoke, or other 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.

Data Center 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 costing 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 coming to backup locations. If the event 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 communication to staff.

□endors and □lients□i□ □a□ted□l□ne□essary□ □ro□eed to ne□t ste□□ □□□□□□□□□□7□□□□□ □□□□□□□□□□□□□□d□□□□ **M**□□□□□□ □□□□□□□□ □and be□in to noti□ □e□bers o□t□e Site Mana□e□ent Tea□ □

7.3□Activate Incident Management Team (Site Management Team):

T□e Site Mana□e□ent Tea□ □ill deter□ine i□t□e In□ident Mana□e□ent Tea□ s□ould be a□ti□ated and i□ne□essary□

Noti□y In□ident Mana□e□ent Tea□ Me□bers□

- In□or□ation □ay in□lude □on□eren□e brid□e in□or□ation□ □eetin□ □Crisis Center lo□ation□ situation des□ri□tion□ brie□ da□a□e assess□ent and initial re□o□ery re□o□ □endations□ Re□uest t□ose unable to □eet at t□e Crisis Co□ □and Center □arti□i□ate □ia a □on□eren□e □all □it□ s□□eduled ti□e□
- I□□ossible□send an e□ail □it□ ne□essary in□or□ation to IMT □e□bers□

A□ti□ate t□e Crisis Co□ □and Center □See □□□□□□□□□□□□□□□□r□□□□□□□□□□□□ □ □□d□□□□□□r□□□□□□□□□□□□□□□

7.4□Evaluate Disaster Impact (Site Management Team):

In□ident Mana□e□ent Tea□ Me□bers □ill □eet to re□ie□ and assess a□ailable in□or□ation to deter□ine t□e □ourse o□a□tion□

□a□e t□e □a□ility Assess□ent tea□ or IMT Leader re□ie□ t□e situation and t□e □reli□inary □□ysi□al assess□ent o□t□e □a□ility □it□ t□e IMT □e□bers□ I□ di□ital □□otos are a□ailable□distribute t□e □□otos to t□e tea□ □or □urt□er □lari□ation o□t□e situation□

Deter□ine i□t□e se□erity o□t□e i□ □a□t re□uires i□ □le□entation o□t□e business □ontinuity □lan

Deter□ine re□o□ery ob□e□ti□es in□ludin□□

- □r□□r□□□□□□Re□o□nition o□□un□tions t□at □ay be able to be □ontinued at t□e □a□ility i□ □ediately or □it□in a □ day e□ort □ill be noted□
- **R**□□□□□□r□□□□r□□□□□□□□□□□onsiderin□ t□e □ontra□tual Ser□i□e Le□el A□ree□ents □SLA□and Re□o□ery Ti□e Ob□e□ti□e □RTO□obli□ations□
- □□□□□□□□□□□□□□□Re□ie□ □ossible situations t□at □ay best utili□e a□ailable resour□es□
- **D**□□□□□□□□□as to alertin□ o□additional □e□bers o□Site Mana□e□ent and In□ident Tea□ 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:

- Current situation as decided in Section 7 Activate Disaster Recovery
- Direct to Members of IMT. These may include initial contact to staff regarding emergency one message escalation of recoverable assets in implementation of procedures regarding portfolio etc.
- Request designated site team members are to report on recovery staff availability coordination of site availability etc.
- Provide procedures and make decisions on how to handle communications between team members. Designate central contact one 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 etc.

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 [illegible]).

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 [illegible] for office phone numbers and email addresses

- Conduct detailed damage assessment. Refer to [illegible]
- 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) take 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

Durin□ sal□a□e and re□o□ery o□erations□□ eal□s□or □ood ser□i□e □ay be □ro□ided to □ersonnel at t□e da□ a□ed and□or alternate o□eration lo□ations□ T□is de□ision □ill be at t□e dis□retion o□t□e IMT Leader □i□e□A□□ount Mana□er□and A□enu UPS E□e□uti□e Mana□e□ent□ Any e□□enditure □ould be □□ar□es usin□ a □redit □ard □it□ as □u□□ detail as □ossible re□ardin□ sta□□or □ersonnel in□ol□ed□

7.6.7 Information Technology (IT)

- Condu□t and re□ie□ □o□ □uter syste□ □ser□ers□a□□li□ations□databases and tele□o□ □uni□ations da□ a□e assess□ent
- A□ti□ate alternate o□eratin□ lo□ations □or syste□ re□o□ery□
- Re□o□er □o□ □uter syste□s and net□or□en□iron□ents□
- A□□uire and install re□la□e□ent □o□ □uter e□ui□□ent
- Re□establis□ data net□or□ □onne□tions to e□ternal resour□es □re□ote lo□ations□□endors□
- I□ □le□ent all tele□□one res□onse □lans □re□routin□ □riti□al tele□□one nu□bers□
- Ensure all syste□ se□urity de□i□es and □ro□edures are in □la□e

7.6.8 Offices Services (Mailroom, Shipping / Receiving)

- Re□establis□□ □ail and s□i□□in□ ser□i□es
- Re□dire□t all □ail and □ar□el re□ei□ts to alternate o□eratin□ lo□ations

7.6.9 Purchasing

- Mana□e all in□ident related □ur□□asin□□
- A□□uire o□i□e su□□lies□□or□ s and e□ui□□ent □or a□e□ted business units□
- I□ □le□ent any ne□essary s□ort□ter□ □inan□ial tra□□in□ □ontrols□usin□ desi□nated □ost □enters□
- I□ □le□ent any ne□essary s□ort□ter□ □inan□ial tra□□in□ □ontrols□ usin□ desi□nated □ost □enters□
- Coordinate all □inan□ial transa□tions □it□ t□e IMT Leaders□Business Continuity Coordinator□A□enu UPS □ana□e□ent and A□enu Insi□□ts □ Analyti□s□LLC C□O□

7.6.10 Vital Records Management

- Coordinate □it□ business units in retrie□in□ all o□site do□u□entation and □edia□
- Be□ause o□t□e □otential o□PII do□u□ent e□□osure□only aut□ori□ed □ersonnel i□e□A□enu UPS sta□□or t□ose □it□ □re□establis□ed aut□ori□ation□s□ould be allo□ed into t□e site□Ob□iously e□er□en□y □or□ers □oli□e□i□re□and res□ue□□a□e □re□eden□e in order to re□establis□ a sa□e en□iron□ent □or sta□□ □o□e□er any assistan□e by t□ese indi□iduals in re□o□ery or se□urin□ o□ do□u□ents or P□I□PII related ite□s s□ould be dis□oura□ed□
- Coordinate do□u□entation retrie□al and do□u□ent restoration□

7.6.11 Physical Security

- Coordinate onsite se□urity □or a□e□ted □a□ilities and all alternate o□eratin□ lo□ations
- Control a□□ess to a□e□ted □a□ilities
- Monitor e□ui□□ ent and re□ords bein□ re□ o□ed □ro□ □a□ilities

7.6.12 Transportation

- Pro□ide lo□al trans□ortation durin□ res□onse and re□o□ery a□ti□ities as re□uired□
- Pro□ide tra□el arran□e□ ents and a□□o□ □odations □or e□ □loyees tra□elin□ to re□ ote re□o□ery lo□ations□

7.6.13 Financial Considerations

T□e A□□ount Mana□er□A□enu UPS Mana□e□ ent and A□enu Insi□□ts □ Analyti□s□LLC C□O □ill re□ie□ any e□□enses t□at □ ay start o□□urrin□ durin□ t□e e□er□en□y re□o□ery and establis□□ ent □or re□ establis□□ ent□o□t□e site□ It is ad□isable to utili□e □endors □□o □a□e establis□ed A□enu Insi□□ts □ Analyti□s□LLC a□□ounts in order to □ini□i□e out o□□o□□et or □redit □ard transa□tions□

I□ tra□el arran□e□ ents and a□□o□ □odations are re□uired □or e□ □loyees tra□elin□ to re□ ote re□o□ery lo□ations□ □ollo□ □o□ □any tra□el □oli□y to se□ure reser□ations□ T□e A□□ount Mana□er□ □inan□ial Analyst□and□or t□e Senior Re□ional □P □ould be res□onsible □or t□e □inan□ial arran□e□ ents o□su□□ transa□tions□

7.7□Track Incident Status and Recovery Progress (IMT Leader):

- Condu□t □eriodi□ debrie□in□ sessions □it□ re□o□ery tea□s to □onitor □ro□ress and deter□ine □roble□ areas
- Reallo□ate and□or □ro□ide resour□es
- T□e UPS IMT Leader □re□ares a status re□ort □or A□enu UPS E□e□uti□e Mana□e□ ent□A□enu UPS E□e□uti□e Mana□e□ ent s□ould □a□e a detailed status re□ort □it□in □□□ □ours □ro□ □□en t□e UPS IMT Leader □as □irst □onta□ted□

8□UPS Operations Recovery Procedures

8.1□Server Recovery

In t□e e□ent o□a ser□er outa□e□an e□aluation and deter□ination o□t□e usability o□all data □ro□essin□ □ard□are□□Ms □ill be □er□or□ ed□ T□is e□aluation s□ould in□ol□e t□e □endor re□resentati□e□ U□on □o□ □letion o□t□e e□aluation and t□e esti□ated ti□e□ra□e □or re□air and□or re□la□e□ ent □ard□are□□Ms re□o□ □endations □ill be □resented to t□e IMT as to □□at ste□s s□ould be □er□or□ ed to resu□e □rodu□tion o□erations□

I□relo□ation to anot□er □a□ility is re□uired and□or ne□ ser□er □ard□are□□Ms or ot□er e□ui□□ent is re□uired□ t□e A□enu UPS tea□ □ill □or□ □it□ A□enu Insi□□ts □ Analyti□s□LLC □ana□e□ent and □endors □o□e to t□e ba□□u□ data □enter lo□ation and en□iron□ent in t□e e□ent o□any Disaster Re□o□ery □lan bein□ e□e□uted□

8.2□Telecommunications Recovery

Tele□o□ □uni□ations bet□een A□enu Insi□□ts □ Analyti□s□LLC UPS lo□ations is establis□ed usin□ Mitel MiCloud Conne□t Ser□i□e□O□i□e des□ □□ones □an be dire□ted to □obile □□ones i□re□uired and all □oi□e □essa□es are sent to sta□□by e□ail to ensure □alls are □a□tured at all ti□es□So□t□□ones □an be used i□needed□

8.3□DSS Recovery

T□e UPS □a□ility does not a□□ess or utili□e any Data □are□ouse or De□ision Su□□ort Syste□ □DSS□ ser□ers□

8.4□EDI Clearinghouse Recovery

T□e UPS □a□ility does not a□□ess t□e Ele□troni□Data Inter□□an□e ser□ers□

8.5□Desktop Personal Computer Recovery Procedures

In t□e e□ent o□a te□□orary or lon□□ter□ outa□e re□uirin□ relo□ation o□□rodu□tion o□erations to □a□ility□ In□rastru□ture Ser□i□es □rou□ □ill □ur□□ase t□e ne□essary re□la□e□ent des□to□s and□or la□to□s □or re□o□ery□ Re□la□e□ent e□ui□□ent □ill be □□ar□ed ba□□ to t□e a□□ro□riate Cost Center□

8.6□Mail Center Recovery

In t□e e□ent o□a situation t□at re□uires t□e relo□ation o□t□e Mail Center o□erations□t□e Mail O□erations Lead □ill noti□y t□e lo□al U□S□Postal o□i□e to reroute all in□o□in□ □ail to t□e alternate re□o□ery lo□ation□A□enu Insi□□ts □ Analyti□s□LLC e□□loyees □ill □ontinue to □i□□u□t□e □ail at t□e Post O□i□e until t□e Post O□i□e is able to □or□ard t□e □ail to t□e re□o□ery lo□ation□T□e United States Postal Ser□i□e □USPS□□as □on□ir□ed t□at t□ey are able to reroute □ail □it□in □□ to □□ □ours o□noti□i□ation□

Contact Avenu Insights & Analytics, LLC' mail□in □ouse □endor □or □rodu□tion relo□ations and □ ailin□ o□all internal □orres□onden□e□

In t□e □ase o□a disaster resultin□ in t□e s□atterin□ o□do□u□ents □ontainin□ Personal □ealt□ In□or□ation □P□I□or Personally Identi□iable In□or□ation □PII□□t□e UPS sta□□s□ould ta□e all reasonable ste□s to deter□ine t□e s□o□e o□t□e re□ords in□ol□ed and retrie□e t□at in□or□ation □□en □ossible□Re□ e□ber t□at t□e sa□ety o□sta□□□ e□bers is al□ays t□e □irst □riority□

8.7□Print Recovery

In t□e e□ent o□relo□atin□ □rodu□tion o□erations to anot□er □a□ility□s□aller □riority re□orts □ill be rerouted to anot□er □rinter at t□e re□o□ery lo□ation□

T□e AS□□□ □osted in Dallas□□ort □ ort□□Te□as □as a □rinter asso□iated □it□t□e □uin□y LPAR t□at is lo□ated in t□e □uin□y o□i□e□In t□e e□ent t□at o□erations are relo□ated□a se□arate □rinter □ill need to be □ro□ured and t□e out□ut re□routed so t□at it □rints at t□e alternate □rinter□□or se□urity □ur□oses□t□e alternate □rinter □ill be lo□ated □it□in a se□ured roo□ □

8.8□Financial Services Recovery

T□e site □a□ility does not □er□or□ any □inan□ial ser□i□es □or t□eir □lient□

9□Returning to Primary Site

T□e □ollo□in□ ste□s s□ould be □onsidered □□en returnin□ □rodu□tion to t□e □ri□ary site□Per□or□ only t□e tas□s or a□ti□ities t□at are re□uired and a□□ro□riate□

9.1□Facility Restoration

- □ or□ □it□ Cor□orate □a□ilities in deter□inin□ i□a ne□ □a□ility is re□uired or i□t□e □a□ility □ill be re□aired□
- C□e□□ □it□ lo□al □ode o□i□ials to identi□y buildin□ □ode re□uire□ents □or re□airs□ne□ □onstru□tion or de□olition□
- □eri□y t□e □ealt□□sa□ety and se□urity o□t□e □a□ility□
- □eri□y t□e o□erational state o□□ey su□□liers and sub□ontra□tors and de□elo□ □ro□edures □or □ui□□ly □ro□urin□ □riti□al □ard□are□so□t□are□and su□□lies□
- Deter□ine □□at e□ui□□ent □ so□t□are needs to be ordered□

- Ad□ise e□ □loyees o□any □ealt□, se□urity, and se□urity □on□erns □it□in t□e □a□ility. S□reen e□ □loyees □or ris□ □a□tors as □eart □onditions, ast□□a, □o□ □rised i□ □une syste□s and aller□ies to □old and dust.
- Pro□ide a□□ro□riate □rote□ti□e e□ui□□ent to □ersonnel (□lo□es, □disin□e□tant □i□es, & □as□s).
- Prior to resu□in□ □rodu□tion in t□e □a□ility, □ondu□t a t□orou□□ □a□ility assess□ent. Re□er to t□e A□eri□an So□iety o□Sa□ety En□ineer Ne□s (ASSE) business resu□ □tion sa□ety □□e□list in Section □ 14. 9.]

□

□

9.2□Travel Preparations

- Pro□ide t□e Lo□al Business Continuity Coordinator □it□ a list o□□ersonnel t□at relo□ated.
- Re□uest t□e Site O□i□e Ad□inistrator □a□e t□e a□□ro□riate tra□el arran□e□ents.
  - Ensure □eals and lod□in□ are □onsidered, ˙a□□ro□riate.
  - I□dri□in□ to t□e re□o□ery site is a□□ro□riate, tea□ □e□bers □ill be res□onsible □or □ro□idin□ t□eir o□n trans□ortation.
  - Monitor tea□ tra□el to ensure team's sa□e arri□al.

9.3□Preparing for System Cutover

- Prioriti□e t□e order o□resu□in□ o□erations and identi□yin□ any obsta□les or ris□s.
- Deter□ine □□et□er syste□ relo□ation □ill be a □□ased or □ut□o□er a□□roa□□.
- I□a □□ased a□□roa□□, deter□ine which □□ase e□ery re□o□ery tea□ □e□ber □ill be assi□ned.
- Ensure su□□ess□ul □ut□o□er o□re□routed tele□□one syste□s.
- Ensure su□□ess□ul □ut□o□er o□all net□or□□o□ □uni□ation syste□s.
- Ensure su□□ess□ul syste□ □database / □ile syn□□roni□ation and □ut□o□er o□□o□ □uter syste□s.
- Ensure su□□ess□ul user testin□ and □ut□o□er o□all □riti□al business □un□tion su□□ort a□□li□ations.

9.4□Preparing for Recovery Site Shutdown

- On□e □rodu□tion business □un□tions are □on□ir□ed o□erational at t□e □ri□ary site, ensure t□at all data is erased on the recovery site's system.
- Re□uest tra□el arran□e□ents □or re□ainin□ Re□o□ery Tea□ □e□bers.
- Ensure □ro□er stora□e or return o□Re□o□ery Site e□ui□□ent.
- In□entory and re□lenis□e□□ended site sto□□ed □aterial i□a□□li□able).
- Ensure utility s□utdo□n i□a□□li□able and as a□□ro□riate).
- Ensure all □eys i□any) are a□□ounted □or and returned to t□e a□□ro□riate indi□idual or lo□ation.
- Ensure site se□urity u□on de□arture.
- Monitor tea□ tra□el to ensure team's sa□e arri□al.

9.5 Emergency Material Replenishment

- Inventory purchase and restock all supplies and documentation used during relocation.
- Ensure the return of the replenished team boxes to offsite storage by the Business Continuity Coordinator.

9.6 Recovery Analysis and Final Documentation

- IMT will make a final meeting after full recovery and restoration of full service at primary 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

System 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.System 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.

System 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 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 sections of the Business Continuity Plan and redistribute it using the plan distribution guidelines.

Plan revisions resulting from changes to hardware configurations network or 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 EOM or environmental changes.
- Major changes in operating system or utility software programs
- Major changes in the design of a production database.
- Major changes in communication system s network or design code s adapters etc. The addition of a communications circuit to a new location an upgrade in network bandwidth etc.
- Changes in offsite storage facilities and methods of delivering backups to the offsite and/or backup facility.
- New application system s 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 lan audits ill be ondu ted to deter ine

- T e readiness o t e In ident Mana e ent Tea to res ond to an e er en y
- et er ba ed u data and do u entation stored o site are ade uate to su ort t e resu tion o business o erations
- et er t e in entories tas s and ro edures are ade uate to su ort t e resu tion o business o erations
- et er t e Business Continuity Plan as been ro erly aintained and u dated to re e t t e a tual resu tion re o ery and restoration needs

T e lan audits ill ta e la e as art o t e e aluation ro ess t rou annual stru tured al t rou A enu UPS or a tual disaster re o ery tests On e t e al t rou s and tests are o leted t e A enu Insi ts Analyti s LLC Ser i e Continuity Deli ery Tea in onsultation it t e Lo al Business Continuity Coordinator ill rodu e a lan audit re ort based on t e bulleted ite s abo e T e lan audit re ort ill do u ent o ell t e lan eets t e abo e re uire ents identi y any de i ien ies in t e lan and a e re o endations or i ro e ent T e A enu Insi ts Analyti s LLC Ser i e Continuity Deli ery Tea ill u date t e lan to address t e de i ien ies identi ied in t e lan audit re ort T e lan audit re ort and any ne essary updates to the Business Continuity Plan will be submitted to the site's In ident Mana e ent Tea and t e A enu Insi ts Analyti s LLC Ser i e Continuity Deli ery Tea or re ie

11.3 Plan Security

T e Business Continuity Plan is lassi ied on idential and ontains ro rietary in or ation to A enu Insi ts Analyti s LLC T ese lans are not to be s ared it anyone outside o A enu Insi ts Analyti s LLC it out t e a ro al o t e A enu Insi ts Analyti s LLC Ser i e Continuity Deli ery Tea Plans ust be s rubbed o all on idential and ro rietary in or ation en distributed outside o A enu Insi ts Analyti s LLC

11.4 Plan Distribution and Access

T e ollo in des ribes t e ro esses and uidelines or distributin o ies o t e Business Continuity Plan to ensure t at ey ersonnel a e a ess to re o ery ro edures in t e e ent o a disaster and to ensure t at o ies o t e lans are stored at a se ure o site lo ation

T e Business Continuity Plan ill be reated and aintained in t e ollo in or ats

- r An ele troni o y o t e lan ill be stored on t e A enu UPS net or

T e Lo al Business Continuity Coordinator ill distribute ne o ies o t e lan to tea e bers and ensure t at all re ious ersions are destroyed T is ill ensure t at in t e e ent o a disaster e eryone is or in ro t e sa e ersion o t e lan T e Lo al Business Continuity Coordinator ill also ensure t at all a ro riate tea e bers are edu ated and trained on t e lan an es

12 Testing Procedures

This section contains an overview of the Business Continuity Testing Process. Business Continuity Testing will address elements of the production systems which may require recovery like 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 order of 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 walkthroughs 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 walkthrough 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 walkthrough 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

□□□□□□□□□□□ □□□□□

□□□□□□□D r□□□□r□□

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 @avenuingists.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 the Client 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 the following information:

- Your Name
- Incident location
- Physical Address (address of the facility where the disaster event is taking place)
- Telephone number where the person reporting the incident can be reached
- Nature of Disaster/Incident

The Avenu Leadership 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 or 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 □ress□□edia □onta□ts are to be re□erred to A□enu Insi□□ts □ Analyti□s□LLC Cor□orate □ead□uarters □or assistan□e or a□□ro□al□

14.2.3 Avenu Insights & Analytics, LLC' Corporate Press Contact

Press□□edia □onta□ts in□lude ne□s□a□ers□ tele□ision stations□ radio stations□ □a□a□ines□ ne□sletters□ □ournals□and trade □ubli□ations □or t□e □ealt□ □are industry□on□line ser□i□es□and ot□er or□ani□ations □at□erin□ and distributin□in□or□ation □or t□e □ubli□□ All res□onses to □ress□□edia re□uests are to be □ro□ided at A□enu Insi□□ts □ Analyti□s□LLC Cor□orate □ead□uarters□unless ot□er□ise a□□ro□ed□

14.2.4 Procedure

Any indi□idual re□resentin□a □ress□□edia or□ani□ation is to be i□□ediately re□erred to t□e lo□al Mana□er on site□T□e Mana□er □ill re□er t□e □ress□□edia re□resentati□e to t□e a□□ro□riate □or□orate □onta□t □or assistan□e□

14.2.5 Process

T□e e□□loyee re□ei□in□ t□e □ress□□edia □all or □onta□t □ill re□er t□e indi□idual to t□e A□enu UPS Mana□in□Dire□tor □□o □ill e□□lain to t□e □ress□□edia □onta□t t□at all □ress□□edia re□uests are addressed at Avenu Insights & Analytics, LLC' Corporate Headquarters and refer the individual to the appropriate corporate □onta□t□ T□e Mana□in□Dire□tor □ill t□en □ro□eed to in□or□ t□e □or□orate □onta□t t□at a □ress□□edia re□erral □as been □ade□

A□enu Insi□□ts □ Analyti□s□LLC □or□orate □onta□t □ill see□a□□ro□al to □ondu□t t□e □ress□□edia inter□ie□□ I□a□□ro□al is not □i□en□t□e □ress□□edia □onta□t □ill be noti□ied by A□enu Insi□□ts □ Analyti□s□LLC □or□orate □onta□t□

□ it□t□e a□□ro□al o□t□e State □lient and A□enu Insi□□ts □ Analyti□s□LLC □i□e President□□ey □essa□es and ans□ers to t□e □ress□□edia □uestions □ill be □o□□leted□a s□o□es□erson desi□nated□and an inter□ie□ □eetin□ s□□eduled□ T□e □ress□□edia inter□ie□ □ill be □ondu□ted□ A□enu Insi□□ts □ Analyti□s□LLC □or□orate □onta□t □ill □o□□lete any □ollo□□u□a□ti□ities□

14.2.6 Accountability

T□e A□enu Insi□□ts □ Analyti□s□LLC e□□loyee re□ei□in□t□e □ress□□edia □onta□t is a□□ountable □or ensurin□ t□at t□e indi□idual is i□□ediately trans□erred to t□e Mana□er on□site□ T□e Mana□er is t□en a□□ountable □or ensurin□t□at t□e □ress□□edia is i□□ediately re□erred to t□e a□□ro□riate □or□orate □onta□t□

14.3 Incident and Crisis Response Center

In t□e e□ent o□an e□er□en□y situation at UPS □a□ility□ensure all e□□loyees are a□are o□t□e □ollo□in□ □ro□edure□

14.3.1 Incident and Crisis Response

In t□e e□ent o□a situation □□ere an e□ □loyee is unable to □onta□t t□eir su□er□isor or □ana□er □it□ t□eir i□ □ediate status and lo□ation, t□e e□ □loyee s□ould □onta□t t□e A□enu Insi□□ts & Analyti□s, LLC □u□an Resour□es tea□. T□e A□enu Insi□□ts & Analyti□s, LLC □u□an Resour□es tea□ □ill be used as a ba□□u□ □or e□ □loyees to re□ort t□eir status and lo□ation.

T□e e□ □loyee s□ould tell t□e re□resentati□e t□e □ollo□in□ in□or□ation:

- T□at t□ey □a□e not been able to □onta□t t□eir i□ □ediate su□er□isor/□ana□er (□i□e t□e re□resentati□e t□e na□e o□t□eir i□ □ediate su□er□isor/□ana□er)
- T□at t□ey □and t□eir □a□ily) are sa□e
- I□t□ere are any □ersonal or □a□ily in□uries
- I□t□ey □a□e e□□erien□ed any □ersonal □ro□erty da□a□e □residen□e or □ar)
- T□eir ability to □et to □or□
- T□eir lo□ation and □onta□t in□or□ation □es□e□ially i□t□ey e□a□uated t□eir □o□e area).

14.4 Temporary Staffing

In t□e e□ent t□e A□enu UPS sta□□ is unable to □er□or□ t□eir nor□al daily o□erational duties be□ause o□an e□er□en□y situation or disaster, A□enu Senior Mana□e□ent □ill □a□e t□e deter□ination to □ire □leri□al and □ro□ra□ □in□ □ersonnel □ro□ a te□ □orary sta□in□ and□or te□□ni□al ser□i□es a□en□y.

Table 15-1 Co□n □ract Labo r Prog ram Contact □

Avenu Insights □□ Analytics, LLC Position	Name □
C□O	□a□es Bar□□an

14.5 AVENU Unclaimed Property Solutions Office

AVENU UPS □
100 □an□o□□Street
10□□ □loor
□uin□y, MA 02171
617-722-9600

14.5.1 Directions to AVENU UPS Office from Logan Int'l Airport

Driving time: approximately minutes Distance: miles

Leave airport terminal and proceed onto Logan West Mass Pike via Ted Williams Tunnel Take the Logan exit exit toward South Boston
Take exit on the left toward Logan

Merge onto Logan US SR RT S via the exit on the LEFT Take exit toward RT A
S Newport Quincy
Turn slight right onto Dalligan Blvd Rt E Turn slight right onto Dalligan Blvd
Turn slight right onto RT A S Newport Ave

RT A S Newport Ave becomes Newport Bridge Newport Bridge becomes Hancock St
Hancock St is on the left

14.5.2 Best Western Adams Inn Crisis Command Center

Command Center
Hancock Street
Quincy MA

14.5.3 Directions to Best Western Adams Inn from UPS Office

Start out going northwest on Hancock St Rt A N toward Newport Ave Exit Continue to follow
Hancock St The Best Western Adams Inn is on the Right

14.5.4 Holiday Inn Command Center

Command Center Primary Driver

Massachusetts Ave
Dorchester MA

14.5.5 Directions to Holiday Inn from UPS Office

Start out going northwest on Hancock St Rt T A N toward Newport Ave
Exit Continue to follow Hancock St Turn slight left onto Newport Bridge
Newport Bridge becomes Rt A N Morrissey Blvd illiam T Morrissey
Blvd Merge onto I N US N RT N Southeast Expy toward Boston
Take the Columbia Rd exit Exit toward Edward Everett
Sq Turn right onto Columbia Rd Pass through
roundabout Turn slight right onto Massachusetts Ave

Massachusetts Ave is on the left

14.6 Disaster Assessment Checklist

[illegible] Disaster [illegible]

[illegible] d [illegible]	Yes No	Notes
E loyee Sa ety		
Any or er in uries		
o serious		
Anyone os itali ed		
Buildin Condition		
Are streets a essible		
Is buildin a essible		
All entran es a essible		
Any sa ety on erns		
Is buildin abitable		
Utilities		
Is o er on in t e buildin		
Is o er on in t e site		
I not is t ere artial o er ere		
Any e osed ele tri al lines		
Are t ere ele tri li ts on		
Is t ere ater in t e buildin		
Is AC syste on in buildin		
AC on in site		
AC on in Ser er Roo		
Is t ere se er ser i e		
Are restroo s a ailable		

□ P□ysi□al Site		
□ Is site a□□essible□		
□ Bot□ entran□es□		
□ Do ele□ators □or□□		

Detail e□a□tly □□at areas are a□e□ted □□ysi□ally□ Ta□e □□otos and□or □oi□e re□ordin□s durin□ a □al□t□ru□ Note su□□ite□s as □ater□s□ o□e□ire da□a□e□lte□s su□□as □an□in□ □ires□□eilin□tiles□□all □roble□s□bro□en □lass □ro□ terra□e □indo□s□dri□□in□ □ater□e□□osed stru□ture□unsa□e door□ays□u□ended or turned o□er □rniture□ initial indi□ation o□e□ui□□ent status□ Be □ery dili□ent to □at□er as □u□□ in□or□ation on □roble□s□□otential

	Yes□No	Notes
Base□ent stora□e roo□		
Is it a□□essible□		
Is □rei□□t ele□ator □or□in□□		
Any in□entory da□a□e□		
I□yes□is in□entory sal□a□eable□		
Ser□er Roo□		
Are ser□ers u□ and runnin□□		
I□not all□□ □i□□ ones are on□		
Any UPS □o□er units runnin□□		
Are t□e routers □or□in□□ Do t□e li□□ts indi□ate any a□ti□ity□		
Is Ser□er Roo□ usable□		
Tele□o□ □uni□ations		
Are ACD lines u□ and runnin□□		
Is net□or□ useable□		
Bot□ inbound□outbound lines on□		
Are e□er□en□y □□ones □or□in□□		
Site □a□ility □loor		
Are □ubi□les□des□s usable□		

Any □ater□s□ o□e□ire da□ a□e□l□ so□□ □ere□		
Are □ile □abinets da□ a□ed□		
Are any □a□er □iles da□ a□ed or destroyed□		
Mailroo□		
Is □ailroo□ inta□t□ Usable□		
Any□all□so□ e □ui□□ ent usable□		
□as any □ail□□ase □iles□□ anual re□ords been da□ a□ed□destroyed□		
□ile Roo□		
Note i□any da□ a□e to re□ords		
Mana□ers O□i□es		
List □□i□□ are usable		
Brea□□ Con□eren□e Roo□		
Is □it□□en usable□		
Anne□Con□eren□e Roo□ usable□		

14.7 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	
o **If NO:**	o **If YES:**
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 o Notify Communications & Public Relations and Human Resources for assistance	IMT activated based on incident
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.	

14.9 Business Resumption Safety Checklist

T□e A□eri□an So□iety o□Sa□ety En□ineers□□□ □□asse□or□□disaster sa□ety □□e□□list assists in □ro□idin□ ite□s t□at need to be □onsidered be□ore□durin□ and a□ter a disaster□

- STRUCTURAL SECURITY□□a□e t□e stru□tural inte□rity o□t□e buildin□or □a□ility □alidated by □uali□ied □ro□essionals be□ore anyone enters t□e □a□ility□
- SA□E ENTRY□Conta□t t□e □ro□er □o□ern□ent a□en□ies to □et a□□ro□al to resu□e o□□u□an□y o□ t□e buildin□□Do not enter a □a□ility or buildin□unless t□e □ro□er □learan□es □a□e been attained□
- CLEAN□UP SA□ETY□I□ □le□ent □lean□u□ and business resu□□tion □ro□esses in a sa□e and □ealt□ul □anner□ Not□in□ □ill be a□□o□□lis□ed i□e□□loyees are in□ured or □illed durin□ t□e □ost□disaster □□ase□in □eriod□Pro□ide trainin□in □ro□er sele□tion and use o□Personal Prote□ti□e E□ui□□ent □PPE□ □or e□□loyees su□□ as eye□ear□ □lo□es□and dust □as□s□res□irators □or □leanin□□ and □□ere a□□ro□riate in ot□er o□erations□
- AIR □UALITY ASSESSMENT□Ma□e sure t□e at□os□□ere in t□e □or□□la□e en□iron□ent is tested □or asbestos and ot□er □□e□i□al□to□i□a□ents□Air □uality is an issue businesses □ay □is□to □ay □are□ul attention to □□en restartin□business o□erations□
- □ENTILATION□□a□e □ents □□e□□ed to assure t□at □ater □eaters and □as □urna□es are □lear and o□erable□Dust and debris □an sto□ or i□□ede air□o□ de□reasin□ its □uality and □ealt□□ulness□ Sa□ely start□u□ □eatin□□ □entilation and air □onditionin□ □□□AC□ syste□s□ □□i□□ in□ludes □rior ins□e□tion o□lines be□ore ener□i□in□ and □ressuri□in□ o□t□e syste□s□Test □entilation syste□s no□ a□ter ins□e□tion or □a□e a □uali□ied s□e□ialist do so□Blo□ □old air t□rou□□ □□AC syste□s □irst□as o□□osed to □ar□ air□as it □ill □el□ □re□ent t□e □ro□t□o□□old in du□t syste□s□
- INTERIOR□E□TERIOR E□POSURES□□or interior s□a□es□ensure no □all or □eilin□ □aterials are in dan□er o□□allin□□I□su□□ e□□osures do e□ist□t□e □or□ en□iron□ent is not ready □or o□□u□an□y□ C□e□□ □or □ra□□ed □indo□s and outside buildin□□aterials□as t□ese □ould □all onto □edestrians at any ti□e □□no□ and in t□e □uture□
- PROTECTION E□UIPMENT□□or □re and s□o□e alar□s it is i□□ortant to assure t□at t□ese □a□e been □leaned and tested be□ore allo□in□ o□□u□an□y o□t□e buildin□□I□su□□ syste□s are □ired into ot□er syste□s ensure t□at t□ey are still □o□□atible and □or□in an e□□i□ient and e□□e□ti□e □anner□T□orou□□ ins□e□tion o□□re□i□□tin□ syste□s su□□ as s□rin□ler and □□e□i□al e□ui□□ent □un□tions is a □ust do ite□□
- ELECTRICAL SA□ETY□ □a□e □□e□s □ade o□ ele□tri□al syste□s□ □o□□uter □ables and tele□o□□uni□ations□e□ui□□ent to ensure t□at t□ey are still sa□e and t□ere is no dan□er o□ e□□osure to ele□tri□ity□□irin□ ins□e□tions s□ould be □ondu□ted □ro□ t□e outside in to ensure all □irin□ and □onne□tions are not in dan□er o□s□ortin□ out due to □ater da□a□e □ro□ rain or □re□ □□□tin□e□orts□

- USE E□ISTIN□ □EDERAL □UIDELINES: Utili□e e□istin□ startu□ □uidan□e □aterials □ro□ided by □o□ern□ent a□en□ies su□□ as t□e □ederal E□er□en□y Mana□e□ent A□en□y (□EMA), □tt□://□□□.e□a.□o□ and t□e National Institute □or O□□u□ational Sa□ety and □ealt□ (NIOS□), http://www.c□dc.g□v/niosh.

- □EALT□ SANITATION ISSUES: T□e □eneral □ility sanitation syste□s □it□ t□e □ility s□ould be ins□e□ted and tested to □uard a□ainst □otential e□ □loyee e□□osure to to□i□a□ents. □ood sanitation s□ould also be an issue. Any unused □oodstu□s s□ould be dis□arded. I□ t□e □or□s□a□e □as a □it□□en, ins□e□t o□en □oods and ot□er □entilation de□i□es to ensure t□ey are not □lo□□ed and are □or□in□ e□□i□iently.

- O□□ICE □URNITURE: Ins□e□t t□e □urniture to ensure it □an □it□stand e□□e□ted loads and usa□es. Ensure t□at binder bins □stora□e de□i□es s□re□ed or bolted to railin□ syste□s on □alls and □anels) □a□e not be□o□e unstable due to □ater da□a□e or s□a□in□ due to e□□losions. Ins□e□t o□□i□e e□ui□□ent to ensure it is le□el, stable, and □annot ti□o□er.

- LI□□TIN□: Ma□e sure t□ere are ade□uate illu□ination le□els □or e□ □loyees. E□er□en□y li□□tin□ s□ould be □□e□□ed to ensure it o□erates and □un□tions in t□e □orre□t □anner.

- EMER□ENCY PLANNIN□: Ensure t□at t□ere is a □lear □at□ o□ e□ress □or t□e e□er□en□y e□a□uation o□e□ □loyees t□at t□e □ire e□tin□uis□ers are still o□erable and t□at □□e□ks □or da□a□e and ser□i□eability are □ade to see i□ any □ire e□tin□uis□ers' □a□ilities □ere used durin□ t□e disaster. I□ da□a□e is □ound, t□ey s□ould be re□la□ed i□ □ediately.

- SOLID/□A□ARDOUS □ ASTE REMO□AL: Bro□en □lass, □debris, □or ot□er □aterials □it□ □uttin□ ed□es s□ould be sa□ely □at□ered and dis□osed o□ □ediately. Ensure t□at su□□ □aterials □an be dis□osed o□be□ore □olle□tion to a□oid □reatin□ e□en bi□□er □a□ards □or bot□ e□ □loyees and t□e □ubli□. Solid □aste dis□osal □ill be an issue, es□e□ially i□□a□ardous □aste is in□ol□ed. E□aluate □aste dis□osal issues □rior to be□innin□ □lean□u□ o□erations to ensure it □an be □ro□erly dis□osed o□. ASSE's □ree '□a□ardous Materials Sa□ety In□or□ation □uide' □as □ey in□or□ation and is a□ailable by □onta□tin□ □usto□erser□i□e@asse□or□.

- PO□ ER C□EC□S: I□ t□ere is no a□□ess to ele□tri□ity on t□e site, do not use □ueled □enerators or □eaters indoors. Ensure t□at t□ere are no □as and se□er lea□s in t□e □ility. C□e□k □it□ lo□al utilities □or in□or□ation re□ardin□ □o□er, □as, □ater, and se□er usa□e.

- C□EC□ MAIN□RAMES: □t□e □ility □as □ain□ra□e □o□ □uter a□□li□ations □see t□at lines and □ablin□ □or □iller syste□s are □□e□□ed to a□oid □□e□i□al lea□out.

- EMER□ENCY PROCEDURES: Create a ne□ e□er□en□y □lan and distribute it to e□ □loyees as soon as t□ey return to □or□. In □ase o□ e□er□en□y, desi□nate a □la□e □or e□ □loyees to □at□er on□e out o□ t□e buildin□ or a □□one nu□ber t□ey s□ould □all □allo□in□ t□e e□er□en□y so t□at all □an be a□□ounted □or. □re□uently u□date t□e e□er□en□y □onta□t list o□na□es and □□one nu□bers.

- MAC□INE INSPECTIONS: Ins□e□t t□e □ondition o□ drain, □ill, □lu□bin□, and □ydrauli□ lines on □ro□esses and □a□□ines. I□ □ould be □rudent to □a□e □lu□bin□ lines e□aluated and tested in order to dete□t any □a□ardous □ases.

- SUR□ACES: Ma□e sure □loorin□ sur□a□es are a□□e□table and □ree □ro□ □ossible sli□s, tri□s and □alls - t□e se□ond leadin□ □ause o□ on t□e-□ob deat□s in t□e U□S. ANSI standard A1264- □rote□tion o□ □loor and □all o□enin□s is a □ood startin□ □oint.

Disaster Recovery Plan

CONFIDENTIAL AND PROPRIETARY

NOT FOR PUBLIC DISCLOSURE

DISASTER RECOVERY OVERVIEW

BNY MELLON

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.

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.