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

Solicitation

NUMBER	PAGE
FAR140001	1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
GUY NISBET
304-558-2596

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DEPARTMENT OF ADMINISTRATION
FINANCIAL ACCOUNTING AND
REPORTING SECTION
2101 WASHINGTON ST E
CHARLESTON, WV
25305-1510 304-558-4083

DATE PRINTED
04/25/2014

BID OPENING DATE: 05/15/2014 BID OPENING TIME 1:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
	ADDENDUM NO.03 ADDENDUM ISSUED TO PUBLISH AND DISTRIBUTE THE ATTACHED INFORMATION TO THE VENDOR COMMUNITY.					
0001	1 AUDIT OF STATE CAFR	LS		946-20		
	****** THIS IS THE END OF RFQ FAR140001 ****** TOTAL:					

SIGNATURE

TELEPHONE

DATE

TITLE

FEIN

ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO SOLICITATION, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

SOLICITATION NUMBER: FAR140001
Addendum Number: No. 03

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

Description of Modification to Solicitation:

1. Addendum issued to distribute copies of the JP Morgan EBT Services & 2013 Molina Medicade SSAE-16 Report.

2. Vendor submitted questions and Agency responses

3. No other Changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

Vendor Submitted
FAR140001 Questions
April 22, 2014

Q.1. How many audit entries did the prior auditor propose? Any passed adjustments?

A.1. Four auditor proposed entries. There were no passed adjustments.

Q.2. When are books closed and ready for audit? Do you have a closing schedule?

A.2.

Items	*Closing Schedule*
WVFIMS	June 30
WVFIMS Opening Balance workpapers	Middle of July
WVFIMS Detail from Opening Balance Revenues/Expenditures	End of July
Unaudited Accrual workpapers (rec., payables, Medicaid, claims & judgements, unclaimed property…	Various times (July – November)
Audited Financial Statement workpapers	Various times (October – November)
Environmental Liabilities	End of September - October
CAFR Financial Statements	End of November – First of December

Q.3. Can you provide the Management Letter Comments and SAS 114 communication from the last audit?

A.3. No, this is only available for Management review.

Q.4. Who is assisting the State with the implementation of the ERP system? Do you have a separate vendor doing IV&V (independent verification and validation) of the implementation?

A.4. Information Services Group (ISG)

Q.5. Can you provide an organization chart of the finance function of the State?

A.5. Each State Agency process their own revenue and expenditures in WVFIMS (current State accounting system). Transactions are approved to the State Auditor's Office for review and approval as to accuracy of financial codes, an approved contract and/or vendor, and cash/budget availability. Transactions are then approved to the State Treasurer's Office where payments are processed once cash is determined to be available in the State's bank accounts with financial institutions.

Q.6. Do you outsource any major systems to a third party servicer?

A.6. Yes, Molina Medicaid Solutions, JPMorgan Chase SNAP/TANF/Child Support, etc.

Q.7. Any significant transactions we should be aware of that will impact the audit in 2014?

A.7. Not that I am aware of at this time.

Q.8. Who is on the selection committee for the auditor?

A.8. Five member committee representing several different areas of State Government.

Q.9. What were total fees and hours for the 2013 audit?

A.9. Total hours for CAFR, Single Audit, State Rail, and SOC 1 report is 15,000. Total fees were $1,620,000.

Q.10. Do you have a formal audit committee? If so, who is on the Committee and how often do they meet?

A.10. The State of West Virginia does not have a formal audit committee.

Q.11. Please describe the assistance that is available from internal audit historically used by the Statewide Auditor.

A.11. The previous external audit firm has used the reports from the Legislative Auditor, post audit division. Those reports are random agencies, approximately 15 each year. The Treasurer's Office internal auditor has provided assistance with internal procedures of cash handling of lockboxes.

Q.12. What are the most important attributes the State is looking for in your external auditor?

A.12 Independence, experience, and knowledge of GASB and GAAP pronouncements

Q.13 Page 35 of the RFP refers to the 4.5 of Section Four. We cannot locate 4.5 of Section Four, Please clarify.

A.13. Instead of 4.5 of Section Four it should be "all mandatory requirement of section 4 subsection 5".

Q.14. What were the audit fees for 2013 audit?

A.14. Base fee was $1,077,710 and out of scope was $543,267. The out of scope also includes the SOC 1 report for IS&C, this was not previously included in the original RFP and was requested later.

Q.15 What were the total hours incurred by the auditor for the 2013 audit?

A.15. 15,000

Q.16 How many programs were audited in 2013? Do you anticipate the same number of programs in 2014?

A.16. 28 major programs were audited in 2013. Yes, the State anticipates approximately the same number of programs in 2014.

Q.17. What is the Audit approach taken with the Student Financial Assistance cluster? Does the State have a rotational methodology that has been approved by the cognizant Federal agency? If a rotational methodology has not been approved, is the auditor required to obtain coverage (i.e. 95%) of the Federal expenditures by testing at multiple schools as required by OMB Circular A-133? If so, at how many colleges/universities is testing performed? Is any of the testing (control or compliance) centralized or is each college/university operating independently?

A.17. The State does not have an approved college/university rotation approach, so this approach is not permissible. The auditors performed testing at 15 schools for coverage needed in accordance with the compliance supplement. The colleges/universities are all decentralized.

Q.18. Can you estimate the remaining American Recovery and Reinvestment Act (ARRA) expenditures for fiscal years ending 2014, 2015, 2016 and 2017?

A.18. 2014 – approximately $60 million and 2015-2017 not sure but should be drastically reduced.

Q.19. With the pending ERP implementation (WVOASIS), should the proposed fees include the additional audit procedures to evaluate the system conversion? These additional audit procedures would be an evaluation of the systems development cycle methodology and processes including, but not limited to, system security set-up, data conversion / integrity, privileged access administration through hyper-care period, and incident and problem management processes related to the implementation. If so, which year do you want the estimated fees related to the system conversion included?

A.19. Yes. There will be some reliance on information in the wvOASIS system for the FY 2014 CAFR (i.e. accounts payable and subsequent receipts and disbursements).

Q.20. What is the scope of services covered within the West Virginia Office of Technology SOC 1 report? Is the scope broader than just WVFIMS / WVOASIS applications to expand and cover additional data center services?

A.20. The scope of the SOC 1 (Type 2) report is broader than the IT general controls procedures for the WVFIMS application. The report addresses WVOT data center services and support across the State of West Virginia which is over and above in-scope agencies and procedures for the CAFR and A-133 audits. The report consists of eight different control objectives; 1) application software development, 2) system software and network changes, 3) logical access, 4) system performance monitoring, 5) physical access and environmental controls, 6) automated job scheduling, 7) problem management and tracking, and 8) data backup and recovery. The application software development control objective is specific to the WVFIMS application; there are no other specific applications that are tested within the SOC 1 report. All remaining control objectives are inclusive of the WVFIMS application and supporting infrastructure; however, in addition supporting infrastructure (i.e. Windows, UNIX, LINUX-base operating system platforms) and data center services are included for the executive branch agencies of the State of West Virginia. The various supporting infrastructure is inclusive of Windows, UNIX, and LINUX-based operating system platforms, SQL, and Oracle database management systems.

Q.21. Should all the subcontractors be identified in the Proposal? If so, will the lead vendor be able to add or change subcontracts in the subsequent years?

A.21. Yes, all subcontractors should be identified in the proposal. Yes, the lead vendor would be able to add or change subcontractors in the subsequent years with prior notice to the State Comptroller.

Q.22. What were the fees associated with the prior year SSAE 16 report over WVFIMS?

A.22. $85,519

Q.23. What were the fees associated with the prior year State Rail separately issued audited financial statements?

A.23. $32,975

Q.24. What were the prior year base audit fees for the CAFR and Single Audit? Also, what was the total amount of the prior year additional billings related to the CAFR and Single Audit?

A.24. FY 2011 base $1,089,760 and total additional $305,385; FY 2012 base $1,045,710 and total additional $456,335; FY 2013 base $1,045,710 and total additional $457,748.

Q.25. What was the prior year EY fee schedule (rate per hour by level) for additional out-of-scope billings?

A.25. An average of $106 per hour.

Q.26. What were the total hours billed by EY for the fiscal year 2013 audit?

A.26. 15,000

Q.27. What new GASB standards do you plan on implementing in 2014?

A.27. GASB 67 and GASB 70

Q.28. What service organizations utilized by the State provided SSAE 16 Reports SOC1 Reports which were relied upon by the prior year auditors? Please provide copies of such reports.

A.28. Molina (Medicaid) and JPMorgan (EBT)

Q.29. Please provide the company names and areas where external specialist are relied on by the State to assist with estimated recorded balances (i.e. reserves, pension obligations).

A.29. CCRC for PEIA and Retiree Health Benefit Trust (RHBT); BuckConsultants for pension obligations

Q.30. For Single Audit purposes, should we assume the same number of major programs as in fiscal year 2013 when developing our 2014 fee estimate?

A.30. Yes

Q.31. What is the planned system conversion date to the new information system (ie OASIS)? Also, please describe what information will be generated from OASIS that will be used in the preparation of the fiscal year 2014 CAFR?

A.31. Planned system conversion date if July 1, 2014. For the FY 2014 audit information related to accounts payable and subsequent receipts and disbursements will be pulled from wvOASIS.

Q.32. What were the major contributing factors that caused the delay in issuing the financial statements subsequent to December 31st in the prior years? Do you expect these factors to be resolved for the current year engagement?

A.32. Did not receive Information Service and Communication (IS&C) financials, Higher Education Consolidated audit, and Prepaid Tuition/SMART 529 audit until late November. Cleanup of the WVFIMS Fixed Asset System was being completed from September – October, this caused changes in the already completed capital assets in November.

Q.33 Who will be on the selection committee for the making the auditor selection?

A.33. Five member committee representing several different areas of State Government.

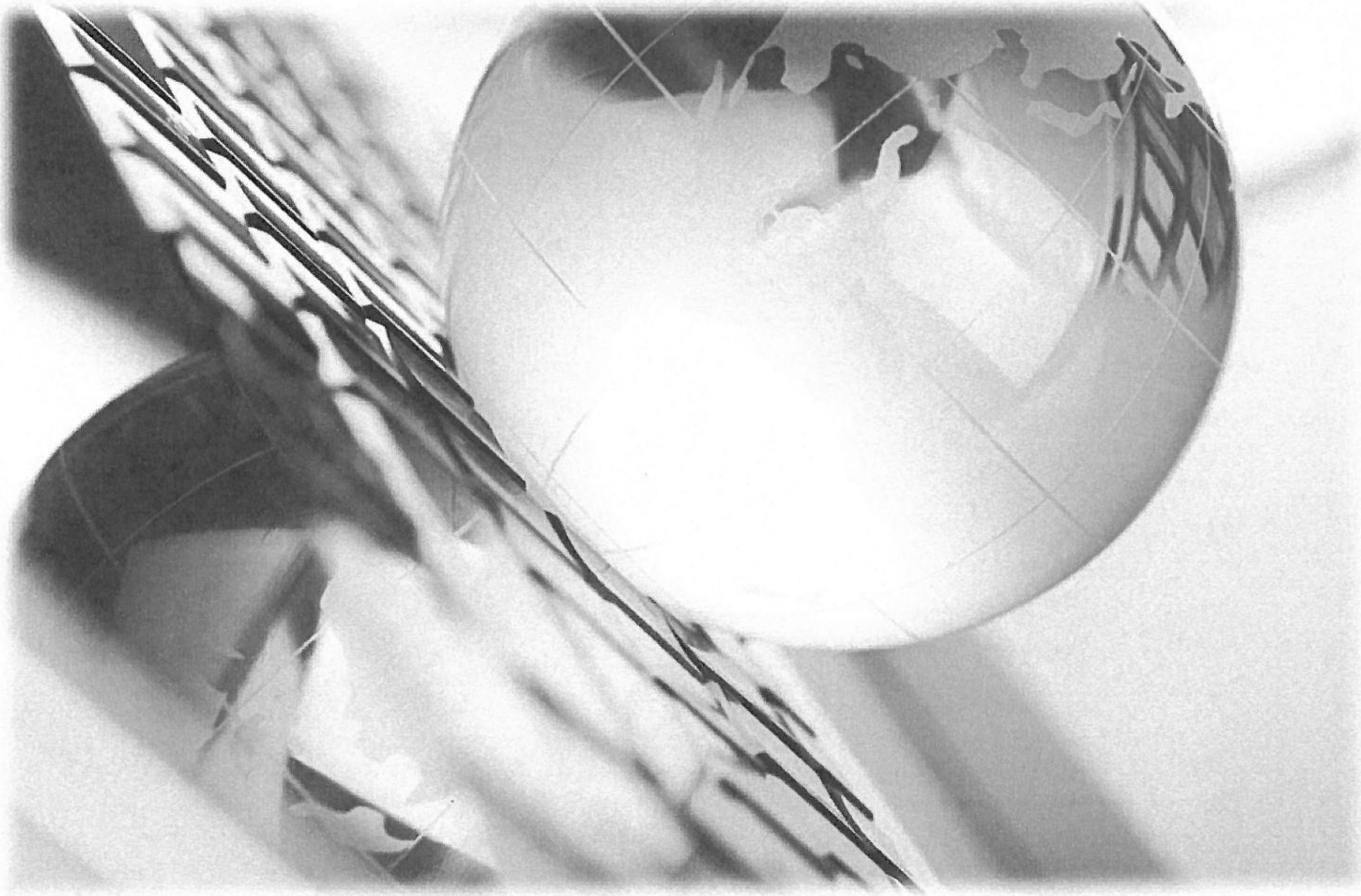
Q.34. How many State run hospitals are there in 2014? What are estimated total fiscal year 2014 revenues for these hospitals?

A.34. There are seven State hospitals. There estimated revenue for FY 2014 is $69 million.

J.P.Morgan

Electronic Benefits Transfer Services

Report on Treasury Services' Description of its Electronic Benefits Transfer Services System and on the Suitability of Design and Operating Effectiveness of its Controls



July 1, 2012 - June 30, 2013

Treasury Services

Contents

Introduction

This report is designed to provide information to be used for financial reporting purposes by clients of JPMorgan Chase Bank, N.A., Treasury Services (J.P. Morgan) and their independent auditors. It is intended to describe certain controls at J.P. Morgan related to its Electronic Benefit Transfer Services system for certain client accounts and supporting operations for clients of Treasury Services' business of J.P. Morgan. This report was prepared according to guidelines contained in the American Institute of Certified Public Accountants Statements on Standards for Attestation Engagements No. 16 “Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting.” The focus of this report is on the aspects of the internal controls of J.P. Morgan likely to be relevant to its clients, but does not encompass all aspects of the services provided or procedures followed by J.P. Morgan.

The Board of Directors and management of JPMorgan Chase & Co. are committed to having a strong control environment throughout the organization, including Treasury Services. Section IV provides an overview of J.P. Morgan and Treasury Services, outlining J.P. Morgan's approach to achieving a strong control environment. Section VI provides a summary of control objectives that J.P. Morgan believes are relevant to its clients, and Section VII provides details of the controls supporting each control objective, as well as related tests performed by PricewaterhouseCoopers LLP, the independent service auditor, and the results of that testing. Sections IV, VI, VII (excluding the Independent Service Auditors' tests of operating effectiveness and the results of those tests) and VIII form the "description" as referenced in the Report of Independent Service Auditors contained in Section II and the Assertion by the Management of JPMorgan Chase Bank, N.A., contained in Section III. Section VIII provides complementary user entity controls and Section IX contains information provided by the independent service auditors.

This report describes the control environment, control objectives and related controls pertaining to the processing of transactions for the Treasury Services Electronic Benefit Transfer (EBT) Services operations located in Tampa, Florida; Westerville, Ohio; and Elgin, Illinois; through its subsidiary, Electronic Financial Services, Inc. (EFS). This report applies to certain electronic benefit transaction processing services offered by J.P. Morgan to federal, state, county and territory agencies for the Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), and Women, Infants and Children (WIC). The description is as of June 30, 2013, and for the period July 1, 2012, to June 30, 2013.

This report applies to the Electronic Benefit Transfer Services system and includes only those internal controls that may be relevant to clients who utilize these services but does not encompass all aspects of the services provided or procedures followed. This report is not intended to describe controls relating to any specific client.

The information included in Section V describing Treasury Services' business resiliency, reports available to Benefit Issuers, EBT only POS terminals, Retail Management operations and Benefit Access Information System not tested in this report is presented by Treasury Services to provide additional information and is not part of Treasury Services' description of controls that may be relevant to clients' internal control as it relates to an audit of financial statements. Such information has not been subjected to the procedures applied in the examination of the description of Treasury Services, related to the Electronic Benefit Transfer Services system.

This report does not encompass the following services:

- Prepaid Card Services
- Global Payment Processor (GPP)
- Treasury Services Automated Clearing House (ACH), check processing and cash management services
- JPMorgan ACCESS ^{SM} Web-based System and client information and delivery system
- Other J.P. Morgan subservice organizations

pwc

Report of Independent Service Auditors

To the Management of JPMorgan Chase Bank, N.A.

Scope

We have examined JPMorgan Chase Bank, N.A. Treasury Services' ("Treasury Services") description of its Electronic Financial Services (EFS) Electronic Benefits Transfer (EBT) system for processing Benefit Issuer sponsored food stamp and cash benefits transfer transactions throughout the period July 1, 2012 to June 30, 2013 (the "description") and the suitability of the design and operating effectiveness of Treasury Services' controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Treasury Services' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Treasury Services uses a subservice organization for all of its transaction switching services. The description in Section IV includes only the control objectives and related controls of Treasury Services and excludes the control objectives and related controls of the subservice organization. Our examination did not extend to controls of the transaction switching services subservice organization.

Service organization's responsibilities

In Section III, Treasury Services has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Treasury Services is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the 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, 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. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require plan and perform our examination to obtain reasonable assurance about whether, in all material respects, 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 July 1, 2012 to June 30, 2013.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in the description in Section IV. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 inadequate or fail.

Other information provided by the service organization

The information included in Section V, "Other Information Provided by the Service Organization Not Tested in this Report", is presented by management of Treasury Services to provide additional information and is not a part of Treasury Services' description of its EFS EBT system made available to user entities during the period July 1, 2012 to June 30, 2013. Information about Treasury Services' business resiliency practices, Benefit Issuer reporting, EBT-Only POS terminals, Retail Management operations, and the Benefit Access Information System has not been subjected to the procedures applied in the examination of the description of the EFS EBT system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the EFS EBT system and accordingly, we express no opinion on it.

Emphasis of a Matter

As described on page 27 of JPMorgan Chase's description, the ITSM system is a workflow application utilized to track approvals, documentation and resources relating to system changes. As indicated on page 28 of JP Morgan Chase's description of its EFS EBT System, for the period September 17, 2012 to June 30, 2013, a processing error existed in the ITSM system, which allowed for application changes to be moved into production without final approvals. Our tests of operating effectiveness relating to this issue are associated with the control objective "Controls provide reasonable assurance that new system developments and changes to existing systems are documented, tested, approved and implemented by authorized personnel."

Opinion

In our opinion, except for the matters described in the preceding paragraph, and based on the criteria described in Treasury Services' assertion in Section III, in all material respects,

a. the description fairly presents the EFS EBT system that was designed and implemented throughout the period July 1, 2012 to June 30, 2013.

b. the controls related to the control objectives of Treasury Services 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 July 1, 2012 to June 30, 2013 and user entities applied the complementary user entity controls contemplated in the design of Treasury Services' controls throughout the period July 1, 2012 to June 30, 2013.

c. the controls of Treasury Services tested, which together with the complementary user entity controls referred to in the scope section of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2012 to June 30, 2013.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section VII.

Intended users and purpose

This report, including the description of tests of controls and results thereof in Section VII, is intended solely for the information and use of Treasury Services, user entities of Treasury Services' EFS EBT system during some or all of the period July 1, 2012 to June 30, 2013 and the independent auditors of such user entities, who 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 misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties. If report recipients are not user entities that have contracted for services with Treasury Services for the period specified above or their independent auditors (herein referred to as a "non-specified user") and have obtained this report, or have access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/ or has access to it.

PricewaterhouseCoopers LLP

October 4, 2013

Assertion by Management of JPMorgan Chase Bank, N.A.

We have prepared the description of JPMorgan Chase Bank, N.A.'s Treasury Services' Electronic Financial Services Electronic Benefit Transfer system for processing Benefit Issuer sponsored food stamp and cash benefits (the "description") for user entities of the system during some or all of the period July 1, 2012, through June 30, 2013, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

a) the description fairly presents the transaction processing system made available to user entities of the system during some or all of the period July 1, 2012, through June 30, 2013, for processing their transactions. The service organization uses a subservice organization for transaction switching services. The description includes only those control objectives and related controls of the service organization, and excludes the control objectives and related controls of the transaction switching services subservice organization. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

      (1) the types of services provided, including, as appropriate, the classes of transactions processed;

      (2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system;

      (3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system;

      (4) how the system captures and addresses significant events and conditions, other than transactions;

      (5) the process used to prepare reports or other information provided to user entities of the system;

      (6) specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls contemplated in the design of the service organization's controls; and

      (7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

   ii. does not omit or distort information relevant to the scope of the transaction processing system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the transaction processing system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b) the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c) the controls related to the control objectives stated in the description, which together with complementary user entity controls were suitably designed and operated effectively throughout the period July 1, 2012, through June 30, 2013, to achieve those control objectives. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved and user entities applied complementary user entity controls contemplated in the design of the service organization's controls; and

   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Signed on behalf of the Management of JPMorgan Chase Bank, N.A.

Treasury Services

Overview

JPMorgan Chase & Co. (the firm) is a leading global financial services firm with operations worldwide. The firm is a leader in investment banking, financial services for consumers and small businesses, commercial banking, financial transaction processing, asset management and private equity. JPMorgan Chase Bank, N.A., is one of the firm's principal banking subsidiaries. See Attachment 1 in Section X for an organization chart of the firm as of June 30, 2013.

The Corporate & Investment Bank (CIB) offers a broad suite of investment banking, market-making, prime brokerage, and treasury and securities products and services to a global client base of corporations, investors, financial institutions, government and municipal entities. Markets & Investor Services includes the securities services business, a leading global custodian which holds, values, clears and services securities, cash and alternative investments for investors and broker-dealers, and manages depositary receipt programs globally. Within Banking, the CIB offers a full range of investment banking products and services in all major capital markets, including advising on corporate strategy and structure, capital-raising in equity and debt markets, as well as loan origination and syndication. Also included in Banking is Treasury Services.

Treasury Services (TS) is a full-service provider of cash management, trade, liquidity and escrow services to corporations, financial services institutions, middle market companies, small businesses, governments and municipalities worldwide.

Regulatory Environment

The firm is subject to regulation under state and federal laws in the United States, as well as the applicable laws of each of the various jurisdictions outside the United States in which the firm does business.

JPMorgan Chase Bank, N.A. (the Bank) is subject to regulation and supervision by the Office of the Comptroller of the Currency (OCC) and is a member of the Federal Reserve System. As a member of the Federal Reserve System, the Bank is subject to the Federal Reserve Act and the regulations of the Board of Governors of the Federal Reserve System. The Bank is required to file periodic reports with the OCC and the Federal Reserve Bank and is subject to periodic regulatory examinations by both agencies.

Control Environment

An integral part of the firm's approach to risk management is the control environment, which represents the collective effect of various factors on establishing, enhancing and maintaining the effectiveness of specific internal controls. The internal control environment reflects the overall attitude, awareness and actions of directors, management and employees concerning the importance of internal control and its emphasis in the firm. These factors are reflected in management's internal control structure, the internal audit function, and personnel policies and procedures that are described in detail in the following sections.

Corporate Values

The firm has established a firmwide code of ethics called the Code of Conduct. Within this document are specific guidelines for employee conduct; compliance with the law; reporting of violations of the Code of Conduct or of laws or regulations; employment and diversity; confidentiality of information; protection and proper use of company assets; conflicts of interest and personal securities and other financial transactions; or taking any action that would adversely affect clients or the reputation of the firm.

The Code of Conduct sets forth an employee's obligation to report violations of laws and regulations, fraudulent acts or dishonesty. Several avenues and contacts are identified to report any wrongdoing or violations of the Code, including direct contact with the Audit Committee. Retaliation is prohibited under the Code of Conduct.

The Code of Ethics for Finance Professionals (the Code of Ethics) is intended to supplement the Code of Conduct and applies to all professionals worldwide serving in a finance, accounting, treasury, and tax or investor relations role. The Code of Ethics is intended to promote honest and ethical conduct and compliance with the laws, rules and regulations of federal, state and local governments and other appropriate regulatory authorities.

Human Resources Policies and Procedures

Treasury Services has formal hiring practices designed to ensure new employees are qualified for their job responsibilities. Written job descriptions for employees are maintained by department management and the Human Resources department. The descriptions are reviewed and revised as necessary. References are sought, and background and security checks are conducted for all persons employed. The confidentiality of client information is stressed during the new employee orientation program and is emphasized in the Code of Conduct.

Officers of the firm generally have an undergraduate college degree, usually with a concentration in finance, accounting or business management. Other employees also have undergraduate degrees, and the firm strongly encourages employees to further their education.

Employees are recruited from a variety of sources, including many colleges and universities, through the firm national recruiting effort and midcareer hiring program, which recruits qualified senior and middle managers.

Staff Development

Firm training programs provide an array of courses and customized programs to meet the educational needs of staff. These programs help orient new staff to their job functions, develop core competencies and train supervisors and managers. The firm has a dedicated technical training function, and courses are continually updated to reflect market and/or industry changes.

At the time of hiring, each employee is required to affirm an understanding of the Code and to agree to comply with the Code. Periodically, all employees receive training and are asked to reaffirm their understanding and compliance with the Code of Conduct. In addition, subject matter expert contact lists are provided to answer specific questions or concerns.

In addition to multiple course offerings, delivery methods include an e-learning (Web-based and Webcast) capability. The following list identifies some of the course offerings:

- Legal, regulatory and risk training across multiple shareholder bases, fund types, markets and industries (e.g., Anti-Money Laundering/Know Your

Customer firmwide training or risk awareness training)

- Introduction to CIB Product Series
- Product seminars

In certain locations, employees are required to be certified (e.g., validate business/technical competency) or complete certain courses to comply with regulatory requirements. In addition to curriculum, staff may attend management development, product management, systems, banking and financial courses.

The firm believes the appraisal process is critical in maintaining an employee's high standard of performance. Each employee's performance is reviewed at least annually through a performance appraisal process. The process is designed to assess each employee's performance results and development activities in comparison to mutually agreed objectives and plans. Evaluations are documented and maintained.

In accordance with corporate policy, and in compliance with the Federal Reserve Bank regulations and OCC guidelines, employees in sensitive positions are required to take off consecutive days. Senior business unit managers are responsible for determining how to comply with regulatory guidance within their respective business units and inform affected staff of the consecutive-day absence policy.

During their absence, employees subject to these restrictions may not conduct business activities or instruct any other employee to take such actions on their behalf, either in person or by remote access. Employees may fulfill the consecutive-day absence policy through any combination of vacation (that must be taken in the calendar year in which it was earned), holidays, jury duty, offsite training or leave of absence.

Corporate Policies and Procedures

Policies and procedures are set at the corporate level by the Board of Directors, line-of-business management, and financial control, risk management, compliance and technology groups. Policies and procedures are updated regularly according to market, industry and government initiatives, business leadership or regulatory developments.

The Corporate Accounting Policies Manual forms the key repository for Board-level policy documents and various corporate accounting and control policies and procedures. Examples include policies for general ledger control, nostro control, expense approval, funds transfer and credit control. These policies incorporate the requirements of legislation, as well as standards set by management, on the control environment and customer service. The policies apply to all business units and all bank and nonbank subsidiaries of the firm. Credit policies and guidelines are specifically detailed in the Corporate Credit Manual, which is intended to provide a consistent methodology of credit origination, distribution and management. In turn, each line of business maintains individual policies and procedures at the lower level, and each production area maintains standard operating procedures that detail the manner in which procedures should be performed. Existence and compliance with these standard operating procedures is confirmed in the ongoing control self-assessments and may be checked by internal audit during audit reviews.

Segregation of Functions

Inherent to the firm's internal control is the principle of segregation of functions and duties, which is reflected in control policies and operating procedures. Treasury Services' global service delivery organization is structured to delineate responsibilities, through automated or non-automated means, in a manner that reinforces segregation of the following functions:

- Input and verification of transactions
- Processing of transactions
- Recording of transactions
- Custody of assets
- Reconcilement activities
- Compliance monitoring

Know Your Customer/Anti-Money Laundering

The firm is committed to knowing its customers, being aware of the services used by its customers, maintaining adequate account documentation, as well as properly identifying customers through credit review and other established policies and procedures to prevent the use of its operations for transactions that facilitate money laundering and terrorist financing. As such, policies and procedures and internal controls have been established to promote compliance with laws and regulations. Independent compliance reviews and internal audits are conducted to validate compliance.

Based on job responsibilities, Treasury Services employees are required to complete regular Anti-Money Laundering (AML) and Know Your Customer (KYC) training. Minimum training requirements have been established to not only include the appropriate policies and practices, but the implications of noncompliance. Training required by corporate policy is monitored and tracked.

The firm has established the Anti-Money Laundering Oversight Committee to lead the firm's fight against money laundering and terrorist financing. Experts from across the firm are brought together to define and promote communication, escalation and coordination of AML, KYC and Anti-Terrorist Financing policies, issues and initiatives; to promote awareness and training to ensure appropriate practices are incorporated into systems and processes; and to provide a global framework for the AML risk analysis of clients, products and countries. The firm maintains intranet sites dedicated to providing timely communication of Anti-Money Laundering and related information to employees throughout the firm who are responsible for overseeing compliance with AML and Anti-Terrorist Financing laws and regulations.

Internal Audit

The firm's internal audit function provides the Audit Committee, executive and senior business management, and regulators with an independent assessment of the firm's ability to manage and control its risks.

Treasury Services activities are subject to periodic examination by internal audit. Internal audit utilizes a risk-based program of audit coverage to provide an independent assessment of the design and effectiveness of controls over operations, regulatory compliance and reporting. Audit reviews may be undertaken by a combination of audits, change activity reviews and continuous auditing (review of management metrics). The audits evaluate compliance with the firm's policies and procedures and with laws and regulations to which the firm is subject, including regulations of the OCC and, the Federal Reserve Bank and the Department of Labor under ERISA, if appropriate. Examinations also address the soundness and adequacy of accounting, operating and administrative controls. In addition, controls surrounding information processing and data center operations are audited by internal audit employees specifically trained in information technology. Internal audit partners with business management and members of the control community, provides guidance on the operational risk framework, and reviews the effectiveness and accuracy of the business self-assessment process as part of its business unit audits.

Final reports of audit findings are submitted to management, and, when appropriate, summaries are presented to the Audit Committee of the Board of Directors. Management is required to respond formally to audit findings and include target dates when corrective action will be completed. Once corrective action is agreed, internal audit and Risk Management work together to follow up with management to ensure timely and effective implementation.

Risk Management

Risk is an inherent part of the firm's business activities. The firm's risk management framework and governance structure are intended to provide comprehensive controls and ongoing management of the major risks inherent in its business activities. The firm employs a holistic approach to risk management intended to ensure the broad spectrum of risk types are considered in managing its business activities. The firm's risk management framework is intended to create a culture of risk awareness and personal responsibility throughout the firm where collaboration, discussion, escalation and sharing of information are encouraged.

The firm's overall risk appetite is established in the context of the firm's capital, earnings power, and diversified business model. The firm employs a formalized risk appetite framework to integrate the firm's objectives with return targets, risk controls and capital management. The firm's Chief Executive Officer (CEO) is responsible for setting the overall firmwide risk appetite. The lines of business CEOs, Chief Risk Officers (CROs) and Corporate/Private Equity senior management are responsible for setting the risk appetite for their respective lines of business or risk limits, within the firm's limits, and these risk limits are subject to approval by the CEO and firmwide CRO or the Deputy CRO. The Risk Policy Committee of the firm's Board of Directors approves the risk appetite policy on behalf of the entire Board of Directors.

Risk Governance

The firm's risk governance structure starts with each line of business being responsible for managing risks inherent in its business, with the appropriate corporate oversight. Each line of business risk committee is responsible for decisions regarding the business' decisions relating to the business' risk strategy, policies and internal controls.

Overlaying the line of business risk management are corporate functions with risk management-related responsibilities: Risk Management, Treasury and Chief Investment Office, the Regulatory Capital Management Office (RCMO), the Oversight and Control group and the Governance Valuation Forum.

Risk Management reports independently of the lines of business to provide oversight of firmwide risk management and controls, and is viewed as a partner in achieving appropriate business objectives. Risk Management coordinates and communicates with each line of business through the line-of-business risk and line-of-business chief risk officers to manage risk. Risk Management is headed by the firm's Chief Risk Officer, a member of the firm's Operating Committee and who reports to the Chief Executive Officer and is accountable to the Board of Directors, primarily through the Board's Risk Policy Committee. The Chief Risk Officer is also a member of the line-of-business risk committees.

Risk Management is responsible for providing a firmwide function of risk management and controls. Within Risk Management are units responsible for credit risk, market risk, country risk, principal risk, model risk and development, reputational risk operational risk framework, as well as risk reporting and risk policy. Risk Management is supported by risk technology and operational functions responsible for building the information technology infrastructure used to monitor and manage risk.

The Risk Management organization maintains a Risk Operating Committee and Risk Management Business Control Committees. The Risk Operating Committee focuses on risk management, including setting risk management priorities, escalation of risk issues, talent and resourcing, and other issues brought to its attention by line-of-business CEOs, CROs and cross-line of business risk officers (e.g., Country Risk, Market Risk and Model Risk). This committee meets biweekly and is led by the CRO or deputy-CRO.

Legal and Compliance has oversight for legal risk. In January 2013, the Compliance function was moved to report to the firm's co-COOs to better align the function, which is a critical component of how the firm manages its risk, with the firm's Oversight and Control function. Compliance continues to work closely with Legal, given their complementary missions. The firm's Oversight and Control group is dedicated to enhancing the firm's control framework, and to looking within and across the lines of business and the corporate functions.

The Board of Directors exercises its oversight of risk management, principally through the Board's Risk Policy Committee and Audit Committee.

The Audit Committee is responsible for oversight of guidelines and policies governing the process by which risk assessment and management is undertaken. In addition, the Audit Committee reviews with management the system of internal controls relied upon to provide reasonable assurance of compliance with the firm's operational risk management processes.

Risk Identification and Measurement

Risk identification is the recognition of the operational risk events that management believes may give rise to operational losses. All businesses utilize the standard self-assessment process and supporting architecture as a dynamic risk management tool.

The goal of the self-assessment process is for each business to identify the key operational risks specific to its environment and assess the degree to which it maintains appropriate controls. Action plans are developed for identified control issues and businesses are held accountable for tracking and resolving the issues on a timely basis.

Risk Monitoring and Reporting

The firm's risk management policies and procedures incorporate risk mitigation strategies and include approval limits by customer, product, industry, country and business. These limits are monitored on a daily, weekly and monthly basis, as appropriate.

Risk reporting is executed on a line-of-business and consolidated basis. This information is reported to management on a daily, weekly and monthly basis, as appropriate. There are nine major risk types identified in the business activities of the firm: liquidity risk, credit risk, market risk, interest rate risk, country risk, private equity risk, operational risk, legal and fiduciary risk, and reputation risk.

Business Control Committees

J.P. Morgan's business executives are responsible for establishing and maintaining a sound control environment in compliance with all applicable laws, regulations and internal policies. To achieve this goal, operational risk must be identified, understood, and periodic evaluations of the adequacy and effectiveness of the control environment must be performed with actions to correct control gaps. Each line of business is required by corporate policy to have a business control committee to provide a forum to accomplish these objectives and facilitate effective communication around risk issues.

Operational Risk Management

Operational risk is the risk of loss resulting from inadequate or failed processes or systems, human factors or external events. Operational risk is inherent in each of the firm's businesses and support activities.

Operational risk can manifest itself in various ways, including errors, business interruptions, inappropriate behavior of employees and vendors not performing in accordance with outsourcing arrangements. These events can potentially result in financial losses and other damage to the firm, including reputational harm.

To monitor and control operational risk, the firm maintains an overall framework that includes strong oversight and governance, comprehensive policies, consistent practices across the lines of business, and enterprise risk management tools intended to provide a sound and well- controlled operational environment.

The framework clarifies:

- Ownership of the risk by the businesses and functional areas
- Monitoring and validation by business control officers
- Oversight by independent risk management
- Governance through business risk and control committees
- Independent review by Internal Audit

The goal is to manage operational risk at appropriate levels, in light of the firm's financial strength, the characteristics of its businesses, the markets in which it operates, and the competitive and regulatory environment to which it is subject.

In order to strengthen focus on the firm's control environment and drive consistent practices across businesses and functional areas, the firm established a new firmwide Oversight and Control group during 2012. This group is dedicated to enhancing the firm's control framework, and looking within and across the lines of business and corporate functions to identify and remediate control issues. The firmwide Oversight and Control group will work closely with all control disciplines - partnering with compliance, risk, audit and other functions - in order to provide a cohesive and centralized view of control functions and control issues. Among other things, Oversight and Control will enable the firm to detect problems and escalate issues quickly, engage the right people to understand common themes and interdependencies among various business and control issues, and effectively remediate issues across all affected areas of the firm. As a result, the group will facilitate an effective control framework and operational risk management across the firm.

The firm's approach to operational risk management is intended to mitigate losses by supplementing traditional control-based approaches to operational risk with risk measures, tools and disciplines that are risk-specific, consistently applied and utilized firmwide. Key themes are transparency of information, escalation of key issues and accountability for issue resolution.

Operational risk management reports provide timely and accurate information, including information about actual operational loss levels and self-assessment results, to the lines of business and senior management. The purpose of these reports is to enable management to maintain operational risk at appropriate levels within each line of business, to escalate issues and to provide consistent data aggregation across the firm's business and support areas.

Management and supervisors monitor the quality of internal control performance as a routine part of their activities. The monitoring process is accomplished through a variety of ongoing activities, including assessment of the results of internal audit, regulatory examinations, Board of Directors and senior management oversight, and management review of operating performance and self-assessments. Treasury Services business units produce monthly Key Risk Indicator reports that highlight key statistics on functions and processes performed within Treasury Services where key risks have been identified. These reports supplement the core operation management performance indicators.

The firm's operational risk framework is supported by Phoenix, an internally designed operational risk system, which integrates the individual components of the operational risk management framework into a unified, web-based tool. Phoenix enhances the capture, reporting and analysis of operational risk data by enabling risk identification, measurement, monitoring, reporting and analysis to be done in an integrated manner across the firm.

For purposes of identification, monitoring, reporting and analysis, the firm categorizes operational risk events as follows:

- Fraud risk
- Improper market practices
- Improper client management
- Processing error
- Financial reporting error
- Information risk
- Technology risk (including cybersecurity risk)
- Third-party risk
- Disruption and safety risk
- Employee risk
- Risk management error (including model risk)

All businesses are required to perform ongoing internal controls self-assessment. The self-assessment process allows each business to identify the key operational risks specific to its environment and assess the degree to which it maintains appropriate controls. The self-assessment process is used to assist business management in their responsibility for ongoing reevaluation of their control environment. The process aids in establishing a consistent and accurate set of global procedures and common practices as each business unit assesses itself against one set of global templates. Any issues identified are highlighted for management and tracked to ensure corrective action is completed. As self-assessment results are used as a key measure of operational control quality, the results are one factor in the calculation of the internal charge for economic capital. This provides incentive to managers to invest in sound control structures to result in reduced cost of operational risk capital and provide shareholder value at lower risk.

In addition, the Treasury Services New Business Initiative Approval process is utilized to ensure management's review and approval of new business and clients within Treasury Services. The New Business Initiative Approval process is utilized to ensure new and changing product risks are identified, analyzed, managed and approved by accountable business management and, as the case may be, the Treasury Services Risk Committee. This process requires review and approval by senior Treasury Services business, operations, technology, and risk management executives prior to the acceptance of new business.

Insurance

The Corporate Insurance Services department is responsible for the structure and administration of worldwide insurance programs for JPMorgan Chase & Co. to provide a level of balance sheet protection against significant fortuitous losses. Accidental losses arise from risks that are not deliberately assumed by the organization in the course of its business and provide only a chance of loss and not of gain.

Examples of such risks are fire, earthquakes, injuries, fidelity of employees, loss from safe deposit or vault, action of servicing contractors and fraudulent transactions. Coverage is provided by several independently-rated insurance companies that management believes are financially sound and at levels the firm considers appropriate given the size and scope of its operations. Examples of the types of coverage are: Master Financial Institution Bond & Computer Crime, and All Risk Securities coverage and Blanket Property Program.

Communication

The firm has various methods of communication to ensure all employees understand their individual roles and responsibilities over transaction processing and controls, and to ensure that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees, monthly communications that summarize significant events and changes occurring during the month, and the use of electronic mail messages to communicate time-sensitive messages and information.

Executive management and corporate leadership hold periodic meetings to provide insight into strategic direction, key decisions and earnings results. Managers also hold periodic staff meetings as appropriate. Every employee has a written position description and every position description includes the responsibility to communicate significant issues and exceptions to an appropriate higher level of authority within the organization in a timely manner.

Description of Services Offered

Program Overview

EBT offers Benefit Issuers an alternative to paper benefit disbursement for food and cash benefits. Recipients of SNAP, TANF and WIC benefits utilize a non-branded debit card to access funds at merchants and ATMs. The service allows agencies to issue benefits, maintain benefit recipient accounts, reconcile funding and transactions and obtain reporting.

Infrastructure

EBT functional teams supporting the delivery of services include:

Media Relations/Public Affairs serves as a liaison between the Benefit Issuer, technology and operations.

Public Sector manages relationships with Benefit Issuers and monitors adherence to service contracts.

Retail Management establishes and maintains relationships with EBT-only retailers, and manages third-party vendors providing point-of-sale (POS) equipment, installation, maintenance and training.

Operations supports the following key functions:

- Settlement and funds management functions between Benefit Issuers, J.P. Morgan and the transaction switch maintained by Fiserv, Inc. (Fiserv)
- Customer service assistance to benefit recipients
- Project management support including overall program tracking, implementations and related enhancements
- Management support in the development of new initiatives and escalation of operational or process-related issues
- Compliance and risk oversight for various functional areas and processes

Client Implementation

EBT client implementations can be large complex events with various activities including establishment of network connectivity, application integration, functionality customization and data conversion. J.P. Morgan recognizes the importance and complexities of such events and the benefit of a program management approach to onboarding new EBT clients. Implementations follow an established Software Development Life Cycle (SDLC) process used firmwide for governance of projects and programs. A cross-functional implementation team consists of representatives of EFS technology, product, operations and relationship management, along with representatives from the Benefit Issuer and the Benefit Issuer's current EBT provider.

Account Setup/Management

Account setup data is processed at the highest priority. Benefit Issuers provide account setup records authorizing the establishment of benefit recipient accounts in batch, online, host-to-host or any combination thereof. Benefit Issuers transmit benefit recipients' information including demographic, status and funding. Information is processed sequentially and validated by automated processes prior to update. In addition, account setup includes inactive and dormant account identification, reporting, benefit conversion and benefit expungement. Processed, rejected and pended information is available to Benefit Issuers online or through file transmission on a daily basis.

Data transmission problems are managed and resolved by appropriate personnel using documented procedures with escalation when appropriate.

Benefit Transaction Authorization

Automated Transaction Authorizations

Benefit recipient transactions including balance inquiries, cash withdrawals (cash account only) and purchases (SNAP, WIC and TANF) are processed through the J.P. Morgan transaction switch, maintained by Fiserv. The switch receives and passes authorization requests from participating networks, third-party processors (TPPs) and retailers to the EBT system. The system performs transaction verification and message generation activities described as follows:

- **Transaction Acquirer (Network/TPP Retailer) Verification** is performed by Fiserv to validate the transaction is received from an authorized source. For SNAP transactions, the retailer initiating the transaction is verified as a Food and Nutritional Services (FNS) authorized retailer.
- **Benefit Recipient Verification** confirms the card is valid and active, and the encrypted PIN is authenticated. The EBT system automatically deactivates a card after a designated number of invalid PIN attempts.
- **Benefit Verification** occurs by validating transaction type, amount of purchase or cash withdrawal and any applicable fees to the available benefit balance.
- **Message Generation** provides balance information and approval or denial notification to the switch.

Manual Food Stamp Authorizations

Manual authorization of SNAP transactions may be performed through the Interactive Voice Response (IVR) system in the event of POS terminal malfunction, network interruption or the retailer is not a qualified POS provider. The IVR requests various pieces of information from the retailer. Once validated, the system provides an authorization number for the manual voucher.

The EBT system posts the transaction to the benefit recipient account with a status of "hold," and the benefit amount is unavailable for the number of days defined by the Benefit Issuer. Retailers are responsible for clearing or forwarding the transaction for processing within the required timeframe; otherwise the "hold" is reversed and the retailer is not reimbursed for the purchase.

If the system is unavailable to process transactions, each Benefit Issuer authorizes a "stand in" transaction dollar amount for benefit recipients. Once the system is back online, a manual transaction is processed to "hold" the funds. The retailer forwards the transaction to be posted to the benefit recipient account. If a retailer allows a customer to make a purchase for more than the "stand in" amount, the retailer assumes the liability if the purchase exceeds the available benefit balance.

Settlement and Reconciliation

Automated Switch Settlement

Fiserv facilitates network settlement on behalf of J.P. Morgan to the ATM or merchant for processed transactions. Settlement with Fiserv occurs each business day at a designated time.

J.P. Morgan's settlement process conforms to the settlement timing guidelines specified in FNS regulations, the Quest® Operating Rules, as specified by the Electronic Benefits and Services Council, and commercial electronic funds transfer standards, however, retailers are advised the availability of funds is determined by individual retailers' contractual relationships with TPP and banks processing and application of Automated Clearing House (ACH) credit entries.

Transactions initiated at point-of-sale and ATMs are recorded on the transaction switch log prior to routing to J.P. Morgan host computers or a TPP. Routing is determined by the Benefit Issuer identification code embedded in the transaction for authorization. The transaction switch performs merchant/TPP settlement and reconciliation, and settles directly with merchants and TPPs. All transactions passing through each processor connected to the transaction switch are totaled and a single net debit or credit settlement entry is issued for SNAP, WIC and TANF transactions.

The transaction switch creates an ACH file with all merchant/TPP settlement totals. The ACH file is delivered through the transaction switch financial institution, which is an ACH originator, for posting to the appropriate settlement accounts for each merchant/TPP. The transaction includes American Banker Association (ABA) account numbers provided by TPPs, networks and other authorized agents. The offset for settlement is the J.P. Morgan settlement bank account maintained for each Benefit Issuer. The transaction is subsequently funded by the U.S. Department of Agriculture (USDA) for food stamp benefits and by each Benefit Issuer for cash benefits.

The debits and credits to J.P. Morgan are the total transactions documented in the transaction switch log for each settlement date.

Reconciliation with the Switch

Daily, transaction log files from Fiserv are compared to J.P. Morgan log files to identify any unmatched or mismatched items using an automated reconciliation tool. Matching criteria is maintained in tables within the reconciliation tool and includes the card number or PAN, date, time, terminal sequence, terminal ID, approval code and amount. J.P. Morgan validates the amount of funds debited from the switch to the aggregate of transactions posted to benefit recipients' accounts.

Unmatched transactions are recorded in a suspense file for utilization in the comparison during the next processing cycle. The file compares unmatched transactions caused by the difference in the daily time period covered by each log. The reconciliation tool maintains unmatched transactions in the suspense file for three cycle days. Unmatched transactions are transferred to the discrepancy file after the three-day cycle and flagged for investigation and further action. Mismatched transactions may also be transferred to the discrepancy file on the date the mismatched transaction is identified for investigation and resolution. Discrepancies are flagged for resolution. Items not successfully resolved are reviewed and periodically written off.

Benefits Recipient Settlement and Reconciliation

J.P. Morgan, in its capacity as financial agent, does not hold funds on behalf of recipients for SNAP, WIC or TANF benefit programs. Benefit recipient accounts reflect current available credit balances after settlement with the Benefit Issuer occurs.

The Discrepancy Records report is further utilized for possible adjustments to benefit recipient and/or retailer accounts. Manual adjustments are posted to the benefit recipient account where required.

Benefit Issuer Settlement

J.P. Morgan settles TANF, SNAP and WIC benefits daily with Benefit Issuers. Daily, operations monitors the automated Benefit Issuer redemption request and verifies requests reconcile to the sum of the day's benefit transactions authorized for payment to the transaction switch. The reviewed redemption request amounts are input in Automated Standard Application for Payments (ASAP) daily for drawdown. End-of-day reports are transmitted supplying detail on all transactions and adjustments for the current redemption request.

Weekly, reconciling transactions or discrepancies noted on an aging report are reviewed to confirm items not resolved within ten days are cleared timely and out-of-balance conditions are explained and investigated for resolution. Bimonthly, Settlement inspects the Net Retail Credit report in Account Management Agent (AMA) to confirm the Store Tracking and Redemption System (STARS) file and Benefit Draw-Down total balance. Any out-of-balance condition is investigated for resolution.

Claims and Adjustments

Benefit Recipient Claims

Benefit recipients may contact Customer Service to initiate a claim. Benefit recipients are authenticated prior to initiating a claim. Claims are tracked utilizing a unique case number automatically assigned in Case Tracking and monitored for resolution. Claims investigators perform a reasonable investigation including a review to determine the existence of another claim related to the specific transaction prior to processing any claim.

Adjustment limits are established for all Claims Investigators. Adjustments beyond established limits require system-enforced secondary review and approval. Customer Service representatives have the ability to initiate a claim in Client Service Platform (CSP) but are restricted from making any adjustments to a benefit recipient account.

Adjustments applied to benefit recipient accounts are reconciled to funds received from the switch. Claim dispositions are updated in Case Tracking and monitored to effect timely resolution.

Merchant Claims

Merchant adjustments are initiated directly with the transaction switch or through a TPP. Claims Investigators review adjustments prior to processing and send to the client for approval. If a claim is approved by the client, a Claims Investigator adjusts the benefit recipient's account.

Subservice Organizations

J.P. Morgan uses various subservice organizations which provide services that may be relevant to user organizations' internal controls over financial reporting. These include:

Transaction Switching Services

Fiserv, Inc. maintains the transaction switch supporting connections to various transaction acquirers (e.g., networks or third-party processors) and routes transactions initiated by benefit recipients at ATM or POS terminals to the EBT host system. Fiserv facilitates settlement with transaction acquirers on behalf of J.P. Morgan.

J.P. Morgan accesses the following Fiserv systems to facilitate reconciliation of transactions:

- *Client Workstation (CWS)* provides the ability to view details of Fiserv's transaction switch logs.
- *Single Point Corrections (SPC)* is accessed through Client Workstation for inquiries and claims processing.

J.P. Morgan follows internal policies and procedures and other applicable regulations in choosing subservice organizations. J.P. Morgan reviews the financial status, operating procedures and contingency plans of certain subservice organizations on an annual basis depending upon the nature of the service provided.

The Report on Treasury Services' Description of Its Electronic Benefit Transfer System and on the Suitability of the Design and Operating Effectiveness of Its Controls is confidential. The report is intended solely for use by the management of Treasury Services, its user entities and the independent auditors of its user entities.

Systems and Technology

J. P. Morgan global technology policies and procedures are implemented by each business for the technology platforms utilized to deliver services. Policies and procedures are developed and approved by relevant management teams. Each Treasury Services (TS) business unit is responsible for implementation and ongoing operation of specified controls.

Treasury Services is supported in the delivery of systems and technology services by the following information technology functions:

- Global Technology Infrastructure (GTI)
- Line-of-business technology support
- Information Technology Risk and Security Management (ITRSM)

Global Technology Infrastructure

Global Technology Infrastructure (GTI) is the technology infrastructure organization for the firm, delivering a wide range of software and hardware products, and other services, and partnering with all lines of business to provide high-quality service delivery.

The technology infrastructure includes data centers, service desk, operations, computing environments (distributed, web hosting, desktop, mainframe, and midrange), data networks and voice networks. Products and services delivered by GTI include:

- Establish firmwide technology architecture and standards
- Build/support services (24 hours/7 days a week) for infrastructure
- Engineering and deployment of networks, voice technologies, desktop products, and data center technologies
- Infrastructure project management and project resources
- Infrastructure service-level management
- Infrastructure monitoring and technical support
- Incident and problem management
- Business management of the technology infrastructure function
- Vulnerability management, including intrusion detection services and incident management

GTI operates a global framework to suit the nature of the firm's businesses, with a regional operations model to meet specific business requirements including: business proximity, location-based technology differences or country-specific regulations. GTI addresses the unique infrastructure needs of specific lines of business and corresponding demand to leverage economies of scale across the firm. GTI's global framework and management are critical to establishing core technology infrastructure direction, standards and policies. GTI's regional construct and management are critical to providing input to the direction of technology infrastructure for the regions and ensuring appropriate execution and implementation.

GTI's services are delivered by the following groups:

Enterprise Computing Services (ECS) manages installation, maintenance, and issue resolution for server operating system and database systems layer services in mainframe, midrange and distributed environments for both primary processing (production) and disaster recovery environments. In this capacity, incident monitoring and resolution services meet availability requirements through support of resiliency and disaster recovery processes. Additional responsibilities include data backup operations for mainframe environments.

Global Service Operations (GSO) perform job scheduling, maintenance and issue resolution for systems in midrange and distributed environments, as well as data backup operations for midrange and distributed environments.

Core Infrastructure Services (CIS) supports all physical controls related to operation of the data centers where technology servers and various network infrastructure components are housed.

Responsibilities include physical access security and environmental and failover controls.

Line of Business Technology Support

TS Application Technology provides implementation and development for internal applications as well as, customization/configuration of vendor-provided applications. In addition, technology teams monitor the operation of individual applications in their respective production environments and manage application-specific issues. In this capacity, the team provides incident monitoring and resolution to meet the availability requirements at the application layer.

EFS Technology systems are developed internally or licensed for use from external vendors. Support for these systems is provided through a combination of the Technology Support team which exists within EFS and various groups within the GTI organization.

Support services include application development, infrastructure support, production support and access administration. These groups maintain technology controls, ensuring compliance with corporate policies and guidelines. EFS utilizes a suite of standard J.P. Morgan tools for technology support. Incident and problem management is handled through the Peregrine Enterprise Incident Management System which manages proper categorization of incident severity and prioritizes incidents for resolution. Additional functionality of the tool includes tracking of issues to completion, documentation of root cause analyses and management reporting of incidents.

Changes to EFS technology systems follow a stringent change promotion standard. This standard addresses the promotion of both scheduled and emergency changes to controlled-processing environments (e.g., segregated production, testing, and contingency environments), for projects of all sizes, and for routine changes to the technology environment. All changes are controlled through a documented system development lifecycle or project methodology, including scheduled projects, infrastructure rollouts, maintenance releases and break-fix activities. The Enterprise Change Management System (ECMS) and Information Technology Service Management (ITSM) are utilized as a central repository to document these changes.

Cardholder AutoRecon (CAR) supports reconciliation of transactions between Fiserv, the transaction switch log and EBT activity log (ALOG).

Case Tracking records and tracks transaction disputes and adjustments.

Electronic Benefits Transfer System is the transaction processing system and database of record for the benefit recipients' accounts. The system consists of multiple modules and services to perform the following:

- Database of record for all benefit recipient cardholder account maintenance and benefit updates received from various interfaces/methods
- Automatic transaction routing and authorization of benefits
- All financial logging and tracking to support state and federal grant program requirements for settlement and reconciliation with the switch

EBT Browser Admin provides Benefit Issuers administrative functionality to manage their programs. Capabilities include viewing and updating account information for benefit recipients and general program data.

EFS Block-mode Operating System Services (BOSS) is a Pathway software product that is a secured common front end that grants audited access to any other NonStop pathway and to other networked NonStop nodes. Access is defined by what applications appear on the users' screens and the allowed conversational interpreter commands.

Front End Balancing (FEB) provides settlement functionality to calculate daily settlement due from various government agencies; track funds received; reconcile payments received; and generate general ledger entries.

Security Gateway (SG) provides a single-point of user authentication to FEB, AutoRecon, Case Tracking, Client Service Platform and EBT Browser Admin.

The following applications are utilized in the delivery of services, but not included in the scope of this review:

Client Service Platform (CSP) supports Benefit Recipient Customer Service agents giving them the ability to research and maintain benefit recipient data and initiate claims on behalf of the benefit recipients. CSP interfaces with the EBT system for all benefit recipient updates; therefore all relevant controls in this report are tested in the underlying EBT system.

EBT Account provides benefit recipients with access to their account information, and the ability to exchange secure emails with Customer Service. EBT Account is a front-end application to the EBT system; therefore all relevant controls in this report are tested in the underlying EBT system.

Implementation and Development

Software Development

Development and implementation of new applications and systems is performed according to J.P. Morgan System Development Life Cycle (SDLC) guidelines and the Product Delivery Framework:

- Project Initiation – Prior to the commencement of a development project, business management meets with technology to determine the business priority and viability of the proposed implementation, scope, cost and level of effort required. Project scope notification to management and the starting point for discussions with related parties
- Approvals –Business management and technology approvals are required prior to the commencement of technology development activities
- Definition – A detailed understanding of the business requirements are translated into functional specifications or a statement of work
- Design – A statement of work is translated into a technical solution to develop a system design document for the construction phase
- Construction –Development of software source code and reconciliation of source code functionality to the requirements of the system design document
- Validation – Various types of testing are performed, including unit testing, quality assurance testing, user acceptance testing, parallel operation, security architecture testing, failover testing, etc. Test execution results are documented and approved at completion
- Implementation – Migration of the software solution to the production environment. In addition to the movement of software, the business is required to perform procedures to ensure users are ready to use the system effectively. Prior to migration to production, documented approvals are obtained from required business and/or technology management. Software development migrations are performed using an emergency user ID or individual user ID belonging to a user who does not have access to develop, as described in further detail under "Change Management," below.

Change Management

Scheduled Changes

During the audit period, the Information Technology Service Management (ITSM) tool replaced the global Enterprise Change Management System (ECMS) as the firm's change management tool. Both ECMS and ITSM initiate internal program changes to track approvals, documentation and resources in a managed workflow. Program changes are subject to the following lifecycle:

- Initiation – A request is assigned a tracking number and entered in ECMS or ITSM.
- Review and approval of requirements – Business and/or technology teams review the project plan and requirements document(s), as appropriate, and evaluate the impact of the change. Impacted teams compile cost estimates and submit the change

request for final approval by technology, operations and business leadership.

- Design/Development — Utilizing the business requirements document(s), a detailed design is created and entered in ECMS or ITSM. The technology team schedules resources and completes development of the change, communicating with the business periodically on issues and adjustments.
- Testing — Various types of testing are performed depending on the nature of the change, including unit testing and user acceptance testing (UAT). In all cases, UAT testing teams are segregated from development staff. Members of the testing team are required to approve test execution and results at completion. Testing results and evidence of the approval are retained in ECMS, ITSM or alternate repositories.
- Implementation — Migration of changes to the production environment are performed utilizing an ID belonging to a user not having development access or an emergency (privileged) ID, which are established to manage changes to the production environment. Emergency IDs remain inactive and require activation through a "break-glass" event. Users must be preauthorized by Management in order to use privileged IDs and access to the IDs is granted for a limited time period. Access to system resources using privileged break-glass IDs is documented and available for review. Management is notified by regular, break-glass event reports or real-time email alerts. Prior to migration to production, documented approvals are obtained from required business and/or technology management. Post-implementation testing may occur on large changes. Once complete, the change request is subsequently closed.

For operating system and software changes, infrastructure technology support staff (either members of GTI ECS or GTI GSO team or a member of a specific business technology support group, depending on the technology platform in question) are responsible for maintaining operating system installations, authentication/security infrastructure and software development lifecycle control packages. Changes made to system software follow notifications from system vendors of updates or notification of infrastructure layer issues from various sources. The infrastructure technology support team notifies the impacted business of scheduled downtimes for upgrades. Testing and installation of updates to these technology components is supported by the same team. Management approves changes to be released in the production environment at the infrastructure layer based on security and functionality considerations dictated by J.P. Morgan infrastructure policies and procedures. Changes are scheduled to occur during specific off-hours time frames. Users cannot access the systems in question during these scheduled events.

For the period September 17, 2012, to June 30, 2013, a processing error existed in the ITSM system, which allowed for changes to be moved into a production-ready status without the appropriate approvals. Such application changes were previously approved and tested but were not yet approved for migration to the production system. Upon the discovery of the system error, the ITSM code was corrected. All changes to relevant EBT systems which would have been affected by the processing error were retrospectively reviewed and approved subsequent to the period covered by this report.

Emergency Changes

In emergency situations, the process for internal program change is identical to the requirements for scheduled changes, with the following exceptions:

Emergency changes may be promoted to the production environment prior to creation of the ECMS/ITSM record or obtaining all required approvals, subject to retroactive approval in a timely manner. Testing of required changes may be limited only to the functionality impacted by the production issue in question.

When emergency changes are required, either a member of the GTI ECS group or a member of a specific business technology support group will obtain access to the production environment through the use of temporary privileged user IDs (described above). Access is monitored by management within the technology group of the party initiating the action. Emergency requests are also tracked through the ECMS/ITSM process and identified as emergency changes. Such changes require timely retroactive approval by a technology and/or a business representative depending on the nature of the change.

Computer Operations

Batch Scheduling and Processing

Automated batch job scheduling is performed either through a centrally managed job scheduler or through an application internal job scheduler. Jobs executed through centrally-managed job schedulers have dedicated support representatives in GTI responsible for the jobs on individual schedulers. Jobs pertaining to an application are maintained within the job scheduler's central registry and segregation is enforced through requirement that only the appropriate GTI support teams are able to affect the application's scheduled jobs. Access changes to modify who may affect the jobs of a particular application are managed through a standard J.P. Morgan request process.

Applications utilizing their own internal scheduler have automated jobs supported by the production support team for the application (e.g., in the technology team of the business supporting the application). An access change, modifying who can affect the jobs of these applications, is handled through a standard J.P. Morgan request process (previously described).

Requests for changes to job processing schedules (both centrally-managed job schedulers and application-specific schedulers) are documented and approved in ECMS or ITSM prior to the change being made. Requests for changes to batch schedules are completed by the technology team supporting the job scheduler in question and the production support team validates the change made to the job schedule is appropriate.

Unscheduled jobs are initiated by the respective scheduler's support team and require a ticket in Peregrine, a problem resolution system, to document the event. Business operations and technology management periodically review Peregrine ticket reports. Escalation procedures, identifying key contact names and emergency notification information for each application, are utilized during problem investigation and resolution.

Job processing is monitored through automated alert mechanisms and job execution outcomes are logged in either an application or a job scheduler log. In the event of a job failure or unexpected result, automated alerts are raised with the appropriate application's production support team. The responsible team is required to respond, investigate, determine an appropriate response, and implement the response. Team responses are documented through Peregrine tickets and manual interventions in job processing resulting from these events are documented either through a break-glass event and/or through an application or scheduler log indicating the ad-hoc actions.

Backup Processing and Disaster Recovery

J.P. Morgan utilizes a comprehensive backup process to minimize occurrence of loss of processing services through:

- Backup data centers, geographically remote from primary data centers
- Disaster recovery hot data center sites configured to replicate both the processing environment and production data in a window of time determined critical (and documented) by each business
- Uninterruptible power supplies, diesel generators, fire detection and suppression systems and water detection systems
- Redundant communication links between business sites and data centers

Computing environments using automated replication to a remote site rely on replication software to produce activity reports and identify the location and state of backup copies. Backup files are available for delivery upon request through a request management system.

GTI CIS is responsible for computing environments' onsite and remote storage and rotation of backup media. Computing environments utilize either a tape backup system with remote storage or an automated network data transfer to a remote location (referred to as "core-bunker" backup systems). Computing environments relying on tape backup systems use a tape management system to produce maintenance reports, documenting the production of tape files and movement to and from onsite and remote storage facilities. Backup media are delivered on a scheduled basis to remote storage facilities. Transmittal forms are prepared and countersigned for movement of backup media between sites.

Computing environments relying on core-bunker backup systems use an automated data feed to periodically copy data to a physically remote data center. The size and outcome of each transfer operation is tracked in an internal infrastructure log.

Businesses are required to periodically verify the recoverability of each application and its associated data. The interval at which this testing is required is determined based on the criticality of the application to the business. This testing may either occur through a scheduled restore of backup copies of data volumes with associated coherency tests, or through an exercise in which the application state and its associated data are tested in a functioning disaster recovery environment. In both cases, the procedures executed for each application and the results of those procedures are documented and reviewed by the business to determine its success or failure. In the event of a failure, the business is required to modify the environment and re-execute the exercise until a successful outcome is obtained.

Physical and Environmental Controls

All Production computing environments are required by J.P. Morgan policy to maintain adequate physical and environmental controls. Physical control requirements include physical locking mechanisms at all external and internal access points to computing facilities, and controls governing how authorized visitors are permitted physical access to these facilities. Visitors must be issued identification badges, must be accompanied by authorized personnel while on the premises of the computing environments and their arrivals and departures must be recorded. A process is in place to periodically recertify that physical access remains commensurate with job responsibilities, or to periodically revoke all users requiring reapproval of their access.

Environmental control requirements include the presence and periodic testing of backup sources of electrical power and switchover mechanisms to allow use of these sources in the event of the failure of municipal power facilities.

Environmental control requirements also include the presence of fire suppression systems, temperature and humidity control systems, and automated monitoring of smoke, temperature and humidity conditions within the computing environments.

Access Administration

Security policies and standards are established to address security entitlement processing, resource access processing, and emergency user ID release. Access administration includes the following control processes:

- Provisioning (creating/removing/changing)
- Recertification completeness of technology access to applications for users, databases and operating systems for technology support staff (either periodically or upon transfer events), and removal of users (in the event of transfer or termination events)

- Management of password requirements (length, expiration intervals and lockout policies) and password resets
- Segregation of security administrators from application developers

Access Provisioning

J.P. Morgan employs a methodology for assigning access to sensitive resources, including system software, production and development application software, and data files based on responsibilities. Two levels of control limit access to applications. The first level is the assignment of a user ID at the infrastructure level; the second level is association of the user ID with applications or specific menu functions within an application.

In mainframe and midrange environments, the infrastructure level control involves the creation of a user ID at the Logical Partition (LPAR) or operating system layer, while the application level control associates the user ID with menus within the applications available in these environments. Access controls surrounding user IDs existing in the environments are built directly into the operating systems and enforced at this layer.

In distributed environments, the infrastructure level control involves the creation of a user ID at the Novell or Active Directory layer (referred to as the 'server domain' level). In these environments, the application level control involves either the registration of access permissions to specific applications within the server domain level user ID profile or the creation of a separate user ID within an application.

Some applications within the distributed environment enforce a third layer of access controls at the workstation's desktop layer. These applications require specific client software be distributed to the local desktop of the authorized user in order for the user to connect to the application. Determination of local desktops to distribute an application's client software to is managed through the Implementation Manager infrastructure, supported by the GTI GSO group.

Users requiring technology access at any control layer must complete an access request form and obtain documented approval from the line manager. Access privileges are assigned based on job responsibilities. Once approved, the request is forwarded to a segregated team responsible for provisioning user IDs for the application. If the request is complete and authorized, the team provisions the requested access. The team then communicates the user ID and a temporary password to the user through a communications channel approved by J.P. Morgan policies.

For certain distributed environment applications requiring user access provisioning at the server domain level, the provisioning team forwards the request to the appropriate team within Global Identity & Access Management to complete the remaining elements of the provisioning process. For distributed environment applications utilizing a third access-control level requiring distribution of client software to the user's desktop, the provisioning team also forwards the request to the GTI GSO team to schedule distribution of the client software to user's desktop.

Global Identity & Access Management (GIAM) administers authorized access to certain J.P. Morgan technology applications. I&AM oversees the creation, deletion and maintenance of access IDs for most applications through request processing, workflow and approval mechanisms. I&AM also manages the recertification process at the application and database layers and ensures appropriate review of personnel terminations and transfers occurs.

Access Maintenance

Security policies and standards govern application recertification, transfers and terminations. At a minimum, on an annual basis, user IDs are forwarded to the respective users' line managers, with the permissions those users retain to the application, database and/or operating system layer. According to the user's current job responsibilities, the manager is asked to identify the access permissions each user should retain as of the date the review is performed.

If a manager denies access permission for a user, the access is removed. Removal of the user may occur either through an automated removal request or through a manual process. In addition, human resource transfer events are periodically compared to access retained by users on the list. The new manager certifies the user's current access. If a manager denies access permission for a user, the access is removed.

For application and database access managed by ITRSM, recertification and review for employee transfer and termination events is managed through either an automated workflow tool or a manual process. For remaining applications and systems, the responsible security administration function executes the recertification process and the application information owner reviews for transferred or terminated employees through alternate means.

Human Resources' termination events are compared to network ID lists and to other access which users retain. Network access is automatically removed for users who experience these events. Removal of application access, in these cases, occurs either through an automated process or a manual request submissions process.

Password Management

Security policies and standards govern J.P. Morgan user password configurations. To access an application, users are required to enter a login ID and a password. Passwords must be masked during on-screen entry and have a required minimum length.

Information Technology Risk and Security Management

Information Technology Risk and Security Management (ITRSM) provides a centralized leadership role in driving execution of firmwide risk management initiatives. In this role, ITRSM is responsible for:

- Representing the firm's information technology risk approach
- Applying a consistent set of information technology risk controls, identity and access and security solutions
- Ensuring a prioritized risk management approach is applied to interpreting regulatory requirements, as well as conforming to internal policies and standards
- Improving firmwide information technology risk governance and linkage to each line of business through the Information Technology Risk Leadership Board (ITRL)

ITRSM fulfills its responsibilities through its own implementation capabilities and drives execution through firmwide governance processes. In addition, ITRM operates under a global framework to satisfy the global nature of the firm's businesses but has regional constructs to address location-specific business and regional requirements.

Separate ITRSM functions also exist in Treasury Services and GTI. Each team ensures risk management goals meet the core services provided by the respective portions of the organizations covered.

Products and services delivered by ITRSM include:

- Information technology policy and standards development, maintenance and compliance strategy
- Periodic assessments of operation of standard technology controls
- Application security product selection, engineering, risk assessment and selected solutions
- Resiliency management, including policy, standards, corporate crisis management and critical multiple line-of-business site tests
- Identity and access management (GIAM) for most infrastructure platforms and selected applications and databases
- Third-party organization technology risk management

Figure 1:
Application Platforms

Application	Platform	Development	Access Point*	Users
Cardholder AutoRecon **	UNIX	Internal	Internal	Internal Settlement
Case Tracking **	UNIX	Internal	Internal / External	Internal and Vendor-Supplemented Customer Service and Claims
EBT System	HP NonStop	Internal and Vendor Licensed	Internal / External	Internal, FNS, Benefit Issuers, Fiserv and Vendor-Supplemented Customer Service
EBT Browser Admin**	UNIX	Internal	External	Benefit Issuers
Front End Balancing **	UNIX	Internal	Internal	Internal Settlement and Claims
EFS BOSS	HP NonStop	Vendor	Internal/ External	Internal, FNS, Benefit Issuers, Fiserv and Vendor-Supplemented Customer Service
Security Gateway	UNIX	Internal	Internal / External	Internal and Benefit Issuers Access Administration

* External connectivity is provided through the J.P. Morgan Business Partner Network and is limited to only those applications and services requested and approved.

** User access authentication is performed by Security Gateway

Other Information Provided by the Service Organization

Other Information Provided by the Service Organization Not Tested in this Report

Business Resiliency

J. P. Morgan's integrated business resiliency strategy, addresses both disaster recovery and business continuity planning required to resume operations from a disruption and provide for continuing operations over the course of a business interruption.

As an integral part of normal business operations, every manager in J. P. Morgan is responsible for developing and maintaining resiliency plans as part of the firm-wide Resiliency Management program. TS business continuity managers and coordinators are responsible for executing the business impact analysis, developing a recovery strategy with management, documenting the strategy in the form of a business continuity plan and testing the plan.

Resiliency plans address the business, operations and technology components of a business process, including those critical processes and functions provided by outside service providers and industry utilities. Contingency locations are an integral part of resiliency planning. In combination with the firm's testing program, the locations ensure business resiliency plans remain accurate, relevant and operable to minimize disruption to clients.

Requirements are defined for each critical business process to provide essential business and technology service levels and comply with resiliency requirements of the Office of the Comptroller of the Currency, the Federal Financial Institutions Examination Council and regulatory agencies in the different geographic regions.

J. P. Morgan's extensive global footprint provides built-in redundancy for many core processing, operations and service delivery functions. J. P. Morgan has strategically located data centers and operation centers throughout the world. This geographic distribution helps reduce the impact of a local disruption on business. Each location has at least one defined and tested recovery site with connectivity to applications and a tested plan for relocating to the alternate site and resuming business.

Critical resiliency plans are tested regularly to verify the effectiveness of alternate locations and to demonstrate the plans remain accurate and executable. A representative number of TS employees participate in tests to validate service provisions remain adequate in the event of a contingency. The results of tests are documented and analyzed to correct potential weaknesses.

Reports Available to Benefit Issuers

J.P. Morgan provides Benefit Issuers with standard reports for monitoring transaction processing, reconciliation, settlement and system performance. Reports are prepared in accordance with each Benefit Issuer's requirements. J.P. Morgan provides two types of reports:

Draw-Down Reports contain financial details for Benefit Issuer totals for all transactions processed the same day, based on a payment cycle.

Benefit Issuer Reports contain opening balance, accumulated financial transactions and current balance for Benefit Issuer totals for transactions processed the same day.

Examples of additional reports and files available include:

- Financial audit reports
- Account Activity file
- Account reconciliation, maintenance, status and audit reports
- Benefit Posting report
- Expungement report
- Manual Transaction report
- Food Stamp Coupon Conversion
- Adjustment Audit report
- Food Stamp Activity report
- Food Stamp Transaction Profile report
- Monthly Issuance report

- Transactions Attempted on Invalid Cards
- Exceeded PIN Attempts report
- Food Stamps Even Dollar Transaction report
- Lost/Damaged/Stolen Card report — Card Status Log
- Administrative Transaction report
- Monthly Downtime report
- Host CPU Transaction Response Time
- Device Type Usage report

Benefit Issuers have the option of receiving a hard copy or electronic copy of a report through online administrative terminals. Transaction data files may also be prepared and distributed to Benefit Issuers for additional local processing, trend analysis and fraud investigation.

EBT-Only POS Terminals

Federal regulations provided FNS-authorized retailers a choice to participate in the new EBT program through the use of EBT-only POS equipment. Many of these retailers are small, independent store owners whose business has been built on the flow of paper food stamp coupons.

J.P. Morgan manages the deployment and installation of EBT-only POS terminals for Benefit Issuers contracting with J.P. Morgan. The Retail and Field Support team (RFS), located in Tampa, is responsible for accurately updating and maintaining the Benefit Access Information System (BAIS). In addition, an onsite Retail Manager is assigned for each Benefit Issuer.

J.P. Morgan uses subservice organizations for POS equipment deployment, installation and configuration of terminals and retailer training. These subservice providers are not included in the scope of this report.

Retail Management Operations

The Retail Management Office recruits new FNS approved retailers and RFS coordinates the completion of agreement packets and enrollment for EBT-only and non-electronic merchants. The packets consist of forms detailing the types of changes to be made, as follows:

- Retailer Agreement Form to record EBT-only or non-electronic retailers
- Retailer Site Survey form to record retailer demographic information
- Retailer Settlement Authorization form to document/change the retailer's ABA and/or checking account

Completed forms are reviewed by RFS to ensure accuracy and completeness. Incomplete forms are returned to the retailer. Once the agreements are completed, BAIS is updated and RFS coordinates with subservice organizations for deployment, installation and configuration of terminals and retailer training.

Benefit Access Information System

The BAIS application supports retailer management including, but not limited to:

- Identify and evaluate terminal coverage for access to food stamps and cash benefits
- Manage retailer training
- Support POS deployment and installation
- Store information on equipment currently in use for inventory and asset-tracking purposes.
- Provide tracking, reporting and reconciliation functions for applicable retailers and retailer updates.

Summary of Control Objectives

Summary of Control Objectives

Settlement to State/Federal Agencies — Benefit Account Settlement

1. Controls provide reasonable assurance that benefit accounts are updated, based on benefits received from federal/state (or county) agencies, completely, accurately, and timely.

Account Management

2. Controls provide reasonable assurance that benefit recipient account standing data is updated completely and accurately.

Benefit Transaction Authorization

3. Controls provide reasonable assurance that benefit recipient transactions are authorized.

Merchant/TPP Settlement

4. Controls provide reasonable assurance that merchant/TPP transactions are recorded completely, accurately, and timely.

5. Controls provide reasonable assurance that merchant/TPP settlement with Fiserv is complete, accurate, and timely.

Settlement to State/Federal Agencies — Cash Settlement

6. Controls provide reasonable assurance that benefit issuer settlement is performed completely, accurately, and timely.

Claims and Adjustments

7. Controls provide reasonable assurance that claims and associated adjustments are authorized and processed completely and accurately.

Information Processing

8. Controls provide reasonable assurance that new system developments and changes to existing systems are documented, tested, approved and implemented by authorized personnel.

9. Controls provide reasonable assurance that access to systems is limited to authorized individuals.

10. Controls provide reasonable assurance that physical access to the computing environment is limited to authorized individuals.

11. Controls provide reasonable assurance that processing is appropriately authorized and scheduled (including backup and mirroring of relevant data and programs) and that deviations from the schedule are identified and resolved.

Control Objectives, Related Controls and Independent Service Auditors' Tests of Operating Effectiveness

In this section, TS has specified the control objectives that it believes are relevant to its clients and their independent auditors and has identified the related controls in place to achieve those objectives. Those objectives have been determined by J.P. Morgan management by reference to, among other things, the American Institute of Certified Public Accountants' Audit and Accounting Guides specifically, "Service Organizations: Applying SSAE No. 16." For each control objective, there is (i) a description of the controls designed to achieve the stated control objective; (ii) an indication of the nature, timing and extent of tests of operating effectiveness of such controls performed by PricewaterhouseCoopers LLP; and (iii) the results of such tests. For further information on testing performed by PricewaterhouseCoopers LLP, see Section IX.

Control Objective 1

Controls provide reasonable assurance that benefit accounts are updated, based on benefits received from federal/state (or county) agencies, completely, accurately, and timely.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Federal food stamp and state cash benefits are received from Benefit Issuers multiple times a day and processed, posted or pended to the system. Summaries of benefits rejected, posted and pended for each settlement date are generated by the system and available to states online or through file transmission on a daily basis.	**Inspection** Inspected transaction screens within the EBT production application to determine information received from client systems is processed, posted or pended to the system. Inspected transaction screens within the EBT production application to determine summaries of benefits rejected, posted and pended are produced and made available.
Benefits are processed sequentially and automatically validated prior to benefit account update.	**Reperformance** Reperformed the processing of benefit files to determine files are processed sequentially and subject to benefit file header and trailer edit checks prior to benefit accounts being updated. Reperformed the processing of benefits through Host-to-Host to determine updates are validated by an automated process prior to benefit accounts being updated.
FEDERAL FOOD STAMP: Settlement performs a proof to ensure the issuance file received is posted to the State LOC for FNS completely and accurately. Reconciling items are researched and resolved.	**Reperformance** Reperformed Settlement proofs for a sample of dates to determine the benefits issuance file received was posted completely and accurately and that reconciling items were investigated for resolution.
Data transmission issues are managed and resolved by appropriate operations personnel using documented procedures with escalation, when appropriate.	**Inspection** Inspected data transmission procedures for evidence of existence. Inspected a sample of help desk tickets to determine data transmission issues are managed and resolved by operations utilizing documented procedures, and escalated when appropriate.

Control Objective 2

Controls provide reasonable assurance that benefit recipient account standing data is updated completely and accurately.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Account demographic information received from Benefit Issuers is processed sequentially and validated by an automated process prior to update of changes to benefit recipient accounts.	**Inspection** Inspected transaction screens within the EBT production application to determine information received from client systems is processed and posted to the system. **Reperformance** Reperformed the processing of demographic information to determine updates are processed sequentially and validated by an automated process prior to update of changes to benefit recipient accounts.
Return demographic responses are transmitted to the Benefit Issuers containing processed data.	**Inspection** Inspected system documentation to determine return file transmissions are provided to the client with the processed information confirming the processed transactions from the client's file.
Data transmission issues are managed and resolved utilizing documented procedures and escalated, when appropriate.	**Inspection** Inspected data transmission procedures for evidence of existence. Inspected a sample of help desk tickets to determine data transmission issues are managed and resolved by operations utilizing documented procedures, and escalated when appropriate.

Control Objective 3

Controls provide reasonable assurance that benefit recipient transactions are authorized.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Benefit recipient transactions are transmitted through Fiserv and authorized by J.P. Morgan following validation of appropriate recipient account status, PIN information and availability of benefit balances to satisfy transactions.	**Reperformance** Reperformed transaction processing to determine transactions are authorized by J.P. Morgan upon validation of appropriate recipient account status, PIN information, and availability of benefits to satisfy the transaction.
Benefit recipient PINs transmitted between Fiserv and J.P. Morgan are encrypted.	**Inspection** Inspected system documentation to determine PINs transmitted between Fiserv and J.P. Morgan are encrypted.
When a hold is placed on a benefit recipient's account, held benefits are no longer available.	**Reperformance** Reperformed transaction processing to determine, when a hold is placed on a benefit recipient's account, the held benefits are no longer available.
A temporary hold is placed on cardholder benefits when a merchant is unable to process transactions due to a nonfunctioning terminal, not having a terminal or an unavailable host computer. Benefits are subsequently released once the merchant terminal is properly functioning and able to process the transaction on receipt of documentation from the retailer or expiration of the systematic hold.	**Inspection** Inspected procedural documentation to determine benefits are held when merchants are unable to process transactions and that on receipt of documentation from the retailer, benefits are subsequently released. **Reperformance** Reperformed transaction processing to determine benefits held are properly released based on expiration or subsequent processing of the transaction.

Control Objective 4

Controls provide reasonable assurance that merchant/TPP transactions are recorded completely, accurately, and timely.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Fiserv and J.P. Morgan logs of authorized benefit recipient transactions are automatically reconciled each day in the CAR module of the FEB system. Results of the automated reconciliation are detailed in a report reviewed by J.P. Morgan to ensure discrepancies are identified and resolved.	**Reperformance** Reperformed the automated reconciliation between Fiserv logs and J.P. Morgan logs for a sample date to determine the automated reconciliation process was performed accurately. **Inspection** Inspected a sample of weekly FEB Aging Reports to determine that management performed a review to confirm reconciling items were being cleared and/or out-of-balance conditions were explained.
Weekly, reconciling transactions or discrepancies noted on an aging report are reviewed to confirm items not resolved within corporate clearing standards are cleared timely and out-of-balance conditions are explained and investigated for resolution.	**Inspection** Inspected a sample of weekly FEB aging reports to determine management performed a review to confirm reconciling items were being cleared and/or out-of-balance conditions were explained.

Control Objective 5

Controls provide reasonable assurance that merchant/TPP settlement with Fiserv is complete, accurate, and timely.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
FEB reconciles funds debited by Fiserv for a given settlement date to J.P. Morgan records to ensure the settlement amount paid is complete and accurate. Actual fund movements are reviewed to validate occurrence.	**Reperformance** Reperformed the automated reconciliation for a sample date to determine the automated reconciliation process was performed completely and accurately. Reperformed review of actual fund movements to validate occurrence.
Weekly, reconciling transactions or discrepancies noted on an aging report are reviewed to confirm items not resolved within corporate clearing standards are cleared timely and out-of-balance conditions are explained and investigated for resolution.	**Inspection** Inspected a sample of weekly FEB aging reports to determine management performed a review to confirm reconciling items were being cleared and/or out-of-balance conditions were explained.

Control Objective 6

Controls provide reasonable assurance that benefit issuer settlement is performed completely, accurately, and timely.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
State Cash/Federal Food Stamp Programs (Post Fund on Spend): Daily, Settlement actively monitors the system automated Benefit Issuer redemption requests and verifies requests reconcile to the sum of the day's benefit transactions authorized for payment to the transaction switch (Fiserv). An out-of-balance condition is researched and resolved.	**Inspection** Inspected FEB balancing report (DIFF01) for a sample of dates to determine management reviewed the reports and, in instances where an out-of-balance condition existed, determined the reason for the condition was investigated, addressed and resolved. **Reperformance** Reperformed the automated reconciliation for a sample date to determine the automated reconciliation process was performed accurately.
Federal Food Stamp: FRB Redemption request amounts automatically calculated by FEB and input in ASAP daily for drawdown are reviewed to ensure the amounts are complete and accurate.	**Reperformance** Reperformed the ASAP quality review for a sample of drawdown occurrences to determine the FEB drawdown amount agreed to the amount entered in ASAP.gov.
Weekly, reconciling transactions or discrepancies noted on an Aging report are reviewed to confirm items not resolved within corporate clearing standards are cleared timely and out-of-balance conditions are explained and investigated for resolution.	**Inspection** Inspected a sample of weekly FEB aging reports to determine management performed a review to confirm reconciling items were being cleared and/or out-of-balance conditions were explained.
A Store Tracking and Redemption System (STARS) file, providing a summary of federal food stamp transactions occurring on the settlement date, is transmitted to FNS. Bimonthly, Settlement inspects the Net Retail Credit report in AMA to confirm the STARS file and Benefit Draw-Down total balance. Any out-of-balance condition is investigated for resolution.	**Inquiry** Inquired with appropriate personnel to determine management reviews the settlement drawdown amount balance to the STARS file transmitted to FNS and out-of-balance items are investigated, addressed, and resolved.

Control Objective 7

Controls provide reasonable assurance that claims and adjustments are authorized and processed completely and accurately.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Benefit recipients are authenticated prior to initiating a claim by telephone.	**Observation** Observed the benefit recipient authentication process to determine benefit recipients are authenticated prior to initiating a claim by telephone. **Reperformance** Reperformed the automated authentication processes to determine benefit recipients are authenticated prior to initiating a claim by telephone.
Case Tracking automatically assigns a unique case number to each claim entered in the system. Claims are systematically prevented from exceeding the original benefit or transaction plus any applicable surcharge fees.	**Observation** Observed a unique case number automatically assigned to a claim entered into Case Tracking. **Reperformance** Reperformed transaction processing to determine claims exceeding the original transaction amount are not processed within Case Tracking.

Control Objective 7

Controls provide reasonable assurance that claims and adjustments are authorized and processed completely and accurately.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Case Tracking automatically populates a timeframe to specify claim resolution and completion dates based on claim type. The claims team monitors reports daily to confirm outstanding claims are researched and closed.	**Inspection** Inspected a Case Tracking report to determine, for each case type, a timeframe has been defined specifying when a claim needs to be completed. **Observation** Observed Claims enter a claim in Case Tracking and noted a completion date was automatically populated based on claim type. Observed management's review of Case Tracking reports and queues for evidence claims are monitored to confirm outstanding claims are researched and closed.
Adjustment limits are established for all claims investigators. Adjustments exceeding established limits require system-enforced secondary review and approval.	**Inspection** Inspected Case Tracking system parameters to determine adjustment limits are established for all investigators. **Reperformance** Reperformed transaction processing to determine an adjustment beyond an investigator's established limit required secondary review and approval.

Control Objective 8

Controls provide reasonable assurance that new system developments and changes to existing systems are documented, tested, approved and implemented by authorized personnel.

J.P. Morgan Controls	PwC Tests and Relevant Exceptions, If Any
Functionality and systems acceptance tests are performed for new developments and changes to existing systems. Testing is approved by the party requesting the change or a designee.	**Inspection** Inspected a sample of changes made to the production environment to determine that acceptance tests had been approved by the party requesting the change or a designee. **Exception Noted** For the period September 17, 2012, to June 30, 2013, five out of the total population of 121 ITSM change tickets pertaining to in-scope EBT applications did not contain evidence of approval prior to implementation to production. A processing error in the ITSM system allowed for certain tickets to be moved into a production-ready status without the appropriate approvals. Management subsequently reviewed the five changes and obtained the required business and/or technology approvals. Management also corrected the processing error in the ITSM system.
New system development and changes to existing systems are approved by the required business and/or technology management prior to the implementation of the change.	**Inspection** Inspected a sample of changes made to the production environment to determine that approval was obtained from required management or a designee prior to the implementation of the change. **Exception Noted** For the period September 17, 2012 to June 30, 2013, five out of the total population of 121 ITSM change tickets pertaining to in-scope EBT applications did not contain evidence of approval prior to implementation to production. A processing error in the ITSM system allowed for certain tickets to be moved into a production-ready status without the appropriate approvals. Management subsequently reviewed the five changes and obtained the required business and/or technology approvals. Management also corrected the processing error in the ITSM system.

Control Objective 8

Controls provide reasonable assurance that new system developments and changes to existing systems are documented, tested, approved and implemented by authorized personnel.

J.P. Morgan Controls	PwC Tests and Relevant Exceptions, If Any
Unplanned or emergency changes to the production environment are logged and subject to retroactive review and approval by the required business and/or technology management.	**Inspection** Inspected a sample of changes made to the production environment to determine that approval was obtained from required management or a designee. **Exception Noted** For the period September 17, 2012 to June 30, 2013, five out of the total population of 121 ITSM change tickets pertaining to in-scope EBT applications did not contain evidence of approval prior to implementation to production. A processing error in the ITSM system allowed for certain tickets to be moved into a production-ready status without the appropriate approvals. Management subsequently reviewed the five changes and obtained the required business and/or technology approvals. Management also corrected the processing error in the ITSM system. **Reperformance** Reperformed the automated process over the successful checkout of a breakglass account using an Alacrity, ITSM and Peregrine ticket to determine that checkout of accounts are appropriately logged and owner of the ID is informed of account usage. Reperformed the automated process over the unsuccessful checkout of an breakglass account using an Alacrity, ITSM and Peregrine ticket to determine that accounts cannot be used inappropriately if prerequisite criteria are not met. Reperformed the automatic reset of breakglass account password upon expiration of account usage for managed and unmanaged accounts.

Control Objective 8

Controls provide reasonable assurance that new system developments and changes to existing systems are documented, tested, approved and implemented by authorized personnel.

J.P. Morgan Controls	PwC Tests and Relevant Exceptions, If Any
Personnel with access to develop application changes do not have access to migrate changes to production without the use of a breakglass or monitored account.	**Inspection** Inspected access review reports for the population of applications to determine that a review was performed to ensure that personnel with access to develop application changes do not have access to migrate changes to production without the use of a break-glass procedure, or any changes are performed through a monitored account where all activity is logged and reviewed. **Reperformance** Reperformed the access review to determine that personnel with access to develop application changes do not have access to migrate changes to production without the use of a breakglass or monitored account.

Control Objective 9

Controls provide reasonable assurance that access to systems is limited to authorized individuals.

J.P. Morgan Controls	PwC Tests and Exceptions
Access to systems is granted only upon approval by authorized management or a designee. The approver confirms access is commensurate with the users' job responsibilities.	**Inspection** Inspected a sample of new user entitlements to determine that access had been approved by authorized management or designee and granted in accordance with the request.
Access to systems is recertified by appropriate management at regular intervals as defined by policy guidelines. The approver confirms access remains commensurate with the individual's job responsibilities or requests changes/revocation to access.	**Inspection** For a sample of application and database accounts, inspected recertification reports to determine access was recertified by management at regular intervals as defined by policy guidelines. For a sample of recertified accounts and transferred users, inspected that any changes or revocation required as a result of the recertification were processed. Inspected a sample of recertified operating system users and determined that requested changes were auctioned by the security administration function (manually or through use of automated administration tools) and any revocations had been completed on the relevant system. **Reperformance** For a sample of recertified application and database accounts including those with access administration capabilities, reperformed the access review to determine that access is commensurate with job responsibilities. Reperformed a sample of recertified operating system users, including those with user administration and job scheduler capabilities, to determine that access is commensurate with job responsibilities.

Control Objective 9

Controls provide reasonable assurance that access to systems is limited to authorized individuals.

J.P. Morgan Controls	PwC Tests and Exceptions, If Any
Access to systems is recertified after internal transfer and is amended or revoked when appropriate based on defined criteria and notifications.	**Inspection** Inspected transfer reports to identify a sample of transferred employees to determine that requested changes were auctioned by the security administration function (manually or through use of automated administration tools) and any revocations had been completed on the relevant system. **Exception Noted** For the period of January 4, 2013, to May 1, 2013, for one of a sample of 25 users whose operating system access was requested to be removed as a result of a transfer, one entitlement was not removed. A typographical error in the file used to remove access resulted in the user retaining one entitlement. As a result, PwC selected an additional sample of 25 users and noted no further exceptions.
Access to the network is automatically revoked following a Human Resources termination event.	**Inspection** Inspected network logs to determine access to the network was revoked for a sampled user following a Human Resources termination event. Inspected network logs to determine remote access through tokens was revoked for a sampled user following a human resource termination event.

Control Objective 9

Controls provide reasonable assurance that access to systems is limited to authorized individuals.

J.P. Morgan Controls

Logical access to systems is controlled through an appropriate authentication mechanism as defined by policies.

PwC Tests and Exceptions

Inspection
Inspected policies to determine that standards exist defining appropriate authentication mechanisms.

Inspection
Inspected systems settings to determine logical access to systems is controlled through an appropriate authentication mechanism as defined by policies.

Exceptions Noted.
On November 7, 2012, J.P. Morgan Corporate Policy for password minimum length was updated from six to eight characters. For the period November 7, 2012, to June 23, 2013, Unix platforms did not meet minimum requirements for password length. PwC noted that on June 24, 2013, the UNIX password settings had been remediated and the character length had been updated to eight characters.

On November 7, 2012, J.P. Morgan Corporate Policy for password minimum length was updated from six to eight characters. For the period November 7, 2012, to June 28, 2013, BOSS and Security Gateway did not meet minimum requirements for length. PwC noted on June 29, 2013, J.P. Morgan updated the password length requirements within the BOSS and Security Gateway applications in both test and production to require a password of eight characters in length.

Control Objective 10

Controls provide reasonable assurance that physical access to the computing environment is limited to authorized individuals.

J.P. Morgan Controls	PwC Tests and Relevant Exceptions, If Any
Entrances to computer data centers are restricted through physical access controls. A process is in place to periodically recertify that physical access remains commensurate with job responsibilities, or to periodically revoke all users requiring re-approval of their access.	**Observation** Observed that access to computer data centers requires a personalized means of identification (e.g., badge, authorized key card or biometrics) and entrances are secured (e.g., access controlled door and 24-hour closed-circuit television monitors). **Inspection** Inspected that computer data center access had been subject to periodic management review or periodic revocation of all users requiring reapproval of their access. For a sample of recertified users, inspected that any changes or revocation required as a result of the recertification were processed.
Visitors (excluding authorized contractors) entering data centers must be monitored by an authorized individual.	**Observation** Observed that visitors entering the critical data centers were monitored by an authorized individual.
Data centers are equipped with alternative power supplies (e.g. uninterruptible power supplies and generators).	**Observation** Observed that uninterruptible power supplies and diesel-powered generators were installed at computer data centers.
Environmental controls are in place at critical data centers including: • Fire protection systems (alarms and sprinklers) • Smoke, heat and moisture detection • Temperature control/air-conditioning units •Raised flooring	**Observation** Observed that environmental monitoring and detection mechanisms are installed in the critical data centers including: • Fire protection systems (alarms and sprinklers) • Smoke, heat and moisture detection • Temperature control/air-conditioning units • Raised flooring

Control Objective 11

Controls provide reasonable assurance that processing is appropriately authorized and scheduled (including backup and mirroring of relevant data and programs) and that deviations from the schedule are identified and resolved.

J.P. Morgan Controls	PwC Tests and Relevant Exceptions, If Any
A schedule is used to ensure the correct processing sequence is observed for production tasks. Changes to the production schedule follow the standard Change Management procedures.	**Observation** Observed on-screen the production task scheduling tools to determine they are used for the in-scope systems to ensure the correct processing sequence is followed for production tasks. Observed on-screen the automatic generation of problem tickets upon a job scheduling failure. **Inspection** Inspected a sample of job scheduler changes made to the production environment to determine that they have been approved by the appropriate party or designee.
Access to the job scheduler is restricted to authorized personnel who do not have processing responsibilities within the business.	**Reperformance** For a sample of recertified operating system users, including those with access administration capabilities, reperform the access review to determine that access is commensurate with job responsibilities **Inspection** Inspected a sample of job scheduler changes made to the production environment to determine that they have been approved by the appropriate party or designee.
Production incidents impacting systems are logged, reviewed and tracked for follow-up and resolution.	**Inspection** Inspected a sample of production incidents (including job scheduler and data backup incidents) to determine that the incidents were logged, reviewed and tracked to resolution.

Control Objective 11

Controls provide reasonable assurance that processing is appropriately authorized and scheduled (including backup and mirroring of relevant data and programs) and that deviations from the schedule are identified and resolved.

J.P. Morgan Controls	PwC Tests and Relevant Exceptions, If Any
Systems are backed up or mirrored to an alternate site on a periodic basis as defined by business requirements.	**Observation** Observed on-screen the relevant software tools and production schedules to determine successful backup/replication to an alternate site. **Inspection** Inspected a sample of production incidents (including job scheduler and data backup incidents) to determine that the incidents were logged, reviewed and tracked to resolution.
The recoverability of backed up or mirrored data is periodically tested according to frequencies defined in the relevant policies and standards.	**Inquiry** Inquired with appropriate personnel to determine restoration tests were completed according to the frequency defined in the relevant J.P. Morgan policy.

Complementary User Entity Controls

Introduction

The controls described in this document cover only a portion of the overall internal controls for each client. The user of this document should consider the client's internal control elements in conjunction with J.P. Morgan's overall control environment and with the specific controls in place in Treasury Services

In addition, there are certain features of the controls that J.P. Morgan believes to be the responsibility of the client. J.P. Morgan expects that these controls are in place for each client and has considered them to be so in developing its own controls. Each client must evaluate its internal controls to determine if appropriate procedures are in place. Furthermore, J.P. Morgan's list of control activities is intended to address only those controls surrounding the communication between the client's staff assigned to service accounts and J.P. Morgan. Accordingly, this list should not be viewed as a complete listing of the control activities that provide a basis for the assertions underlying the financial statements of clients.

The list of complementary user entity controls presented here does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required.

The following are client controls that the user auditor should consider in reviewing the client's financial statements and control environment.

Each complementary user entity control applies to all control objectives unless specifically noted.

Client Controls

- Instructions and information provided to J.P. Morgan from its clients or their agents are accurate, complete and in accordance with the provisions of the servicing agreements or other applicable governing agreements or documents between J.P. Morgan and the client.
- Timely notification of changes to client data is adequately communicated to J.P. Morgan. (Control Objective 1 and 2)
- Clients are responsible for validating the accuracy of any client-specific edit and validation checks. (Control Objective 2)
- Timely notification of changes in the designation of individuals authorized to act on behalf of the client is provided to J.P. Morgan.
- Physical and logical access to J.P. Morgan systems through terminals at client locations is restricted to authorized personnel. (Control Objective 9 and 10)
- Clients are required to periodically evaluate users' access and communicate necessary updates to J.P. Morgan. (Control Objective 9)
- Timely review of reports provided by J.P. Morgan of account balances and related activity by appropriate users for completeness and accuracy. If discrepancies exist, the client should provide written notice to J.P. Morgan detailing the outstanding discrepancies.
- Transactions entered by employees are appropriately authorized, complete and accurate. (Control Objective 3)
- Balancing of transmissions is the joint responsibility of J.P. Morgan and the Benefit Issuers. Controls should be established to schedule all transmissions and to help ensure positive acknowledgment of record counts between J.P. Morgan and all Benefit Issuers.
- Benefit Issuers are responsible for reviewing the reports provided by EBT to ensure all transmissions were received completely and posted accurately.

- Local security administrators are responsible for assigning EBT user IDs and passwords, maintaining the EBT user IDs and access privileges, and coordinating system access with EBT Security. Local security officers are also responsible for requesting and reviewing user access reports. (Control Objective 9)

- Controls should be established to help ensure that requests for changes to EBT, initiated by the Benefit Issuer, are appropriately authorized, tested and approved prior to implementation. (Control Objective 8)

Information Provided by the Independent Service Auditors

Introduction

This "Report on Treasury Services' Description of its Electronic Benefits Transfer Services System and on the Suitability of the Design and Operating Effectiveness of its Controls" is intended to provide interested parties with information sufficient to understand the flow of transactions within J.P. Morgan Treasury Services related to Treasury Services Electronic Benefit Transfer (EBT) Services operations located in Tampa, Florida; Westerville, Ohio; and Elgin, Illinois; through its subsidiary, Electronic Financial Services, Inc. (EFS) and the operating effectiveness of the controls tested that may affect the administration and processing of transactions.

This report, when combined with an understanding of the internal controls in place at client locations and at its subservice organizations, is intended to assist user auditors in planning their audit and in assessing control risk for assertions of the financial statements of EBT user organizations and in planning the audit of TS user entities. This report was prepared according to guidelines contained in the American Institute of Certified Public Accountants Statements on Standards for Attestation Engagements No. 16 "Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting"

Testing of the controls was restricted to the control objectives and the related control activities outlined by J.P. Morgan management in Section VII of this report, which management believes to be the relevant key controls for the objectives stated. The description is for the period July 1, 2012, through June 30, 2013, and applies to EBT clients and was not extended to controls in effect at client or other service or subservice organizations. The tests of operating effectiveness performed were based on the scope described in Section I of this report.

It is each interested party's responsibility to evaluate this information in relation to internal controls in place for each client. If effective client internal controls are not in place or operating with sufficient effectiveness, J.P. Morgan controls may not compensate for such weaknesses.

As part of the examination of J.P. Morgan controls, a variety of tests was performed, each of which provided different levels of attest comfort. The combined results of these tests provided the basis for understanding the framework for control and whether the controls surrounding the operations that J.P. Morgan represented were suitably designed and implemented and were operating effectively throughout the period from July 1, 2012, through June 30, 2013.

Control Environment

Tests of the control environment, risk assessment, monitoring and information and communication included inquiry of appropriate management, supervisory and staff personnel, observation of J.P. Morgan Treasury Services activities and operations, and inspection of J.P. Morgan Treasury Services documents and records. The results of these tests were considered in planning the nature, timing and extent of our testing of the controls designed to achieve the control objectives described on the following pages. Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

Controls

Tests of the operating effectiveness of the controls included such tests as were considered necessary in the circumstances to evaluate whether the controls and the extent of compliance with them were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from July 1, 2012, through June 30, 2013. Unless otherwise indicated, tests of the operating effectiveness of the controls were designed to cover a sample number of transactions and procedures, throughout the period July 1, 2012, through June 30, 2013, for the controls listed in Section VII, which are designed to achieve the specified control objectives. In selecting particular tests of the operating effectiveness of the controls, the following were considered: (a) the nature of the controls being tested; (b) the types and competence of available evidential matter; (c) the nature of the control objectives to be achieved; (d) the assessed level of control risk; (e) the expected efficiency and effectiveness of the test; and (f) the testing of other controls relevant to the stated control objective. Where applicable, testing performed was accomplished through one or more methods including but not limited to:

- Observing actual production transactions processed through the system (e.g., transactions failing edit/validation checks)
- Recalculating system-calculated balances manually or using computer-assisted audit techniques
- Using computer-assisted audit techniques to validate the accuracy and completeness of systems output and/or systems reports
- Tracing transactions through the live production or test systems (which we validated to be the same environment as production) to appropriate reports
- Reviewing client testing results of systems changes prior to their migration to the production environment

Test Descriptions

The types of tests performed of the operational effectiveness of Treasury Services controls detailed in Section VII are briefly described below:

Test — **Description**

Inquiry

Inquired of appropriate J.P. Morgan personnel. Inquiries seeking relevant information or representation from J.P. Morgan personnel were performed to obtain, among other factors:

- Knowledge and additional information regarding the control
- Corroborating evidence of the control

As inquiries were performed for substantially all J.P. Morgan controls, this test was not listed individually for every control listed in the tables in Section VII.

Observation

Observed the application or existence of specific controls as represented.

Inspection

Inspected documents and records indicating performance of the control. This includes, among other things:

- Inspection of reconciliations and management reports that age or quantify reconciling items to assess whether balances and reconciling items are properly monitored, controlled and resolved on a timely basis as required by the related controls
- Examination of source documentation and authorizations to test propriety of transactions processed
- Examining documents or records for evidence of performance, such as the existence of initials or signatures
- Inspection of J.P. Morgan systems documentation, such as operations manuals, organization charts and job descriptions

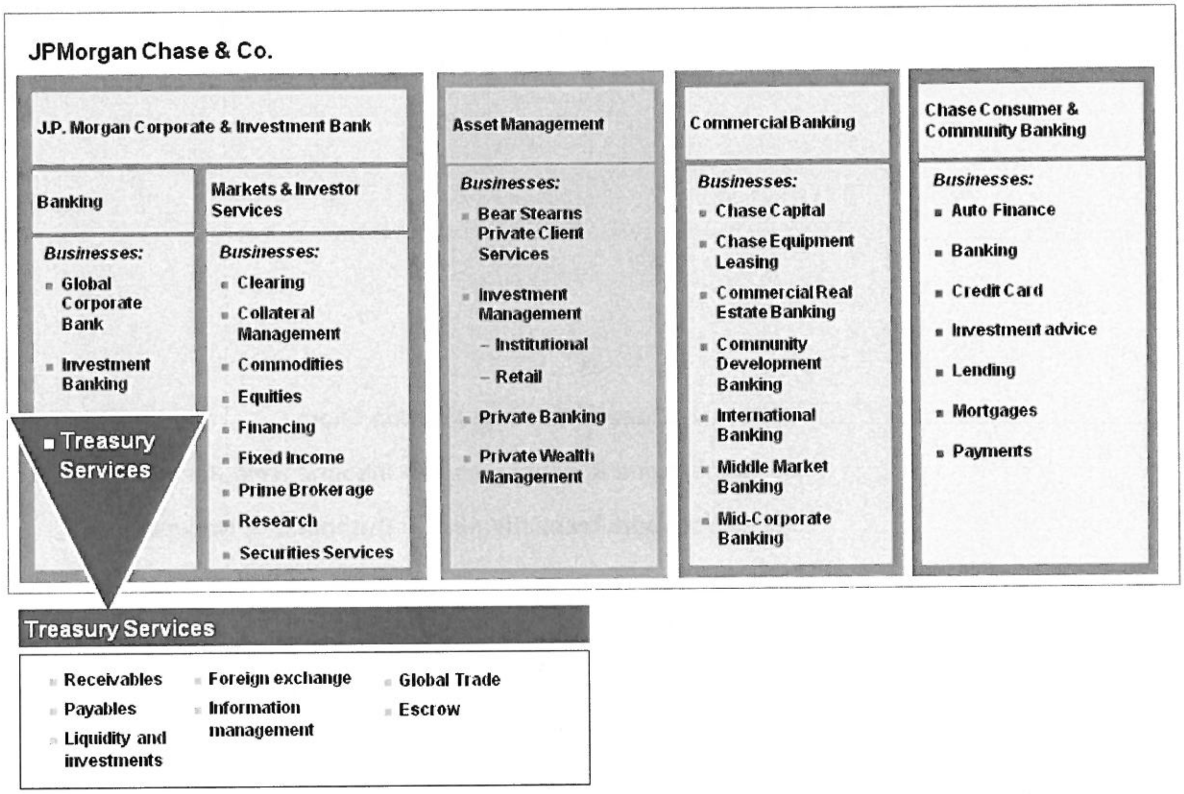
Reperformance

Reperformed the control or processing application to test the accuracy of its operation. This includes, among other things:

- Obtaining evidence of the arithmetical accuracy and correct processing of transactions by either recomputing the J.P. Morgan computation or performing independent calculations
- Performance of systems testing

Attachments

Attachment 1: JPMorgan Chase & Co. Organization Chart



JPMorgan Chase & Co.

J.P. Morgan Corporate & Investment Bank

Banking

Businesses:

- Global Corporate Bank
- Investment Banking
- Treasury Services

Markets & Investor Services

Businesses:

- Clearing
- Collateral Management
- Commodities
- Equities
- Financing
- Fixed Income
- Prime Brokerage
- Research
- Securities Services

Asset Management

Businesses:

- Bear Stearns Private Client Services
- Investment Management
  - Institutional
  - Retail
- Private Banking
- Private Wealth Management

Commercial Banking

Businesses:

- Chase Capital
- Chase Equipment Leasing
- Commercial Real Estate Banking
- Community Development Banking
- International Banking
- Middle Market Banking
- Mid-Corporate Banking

Chase Consumer & Community Banking

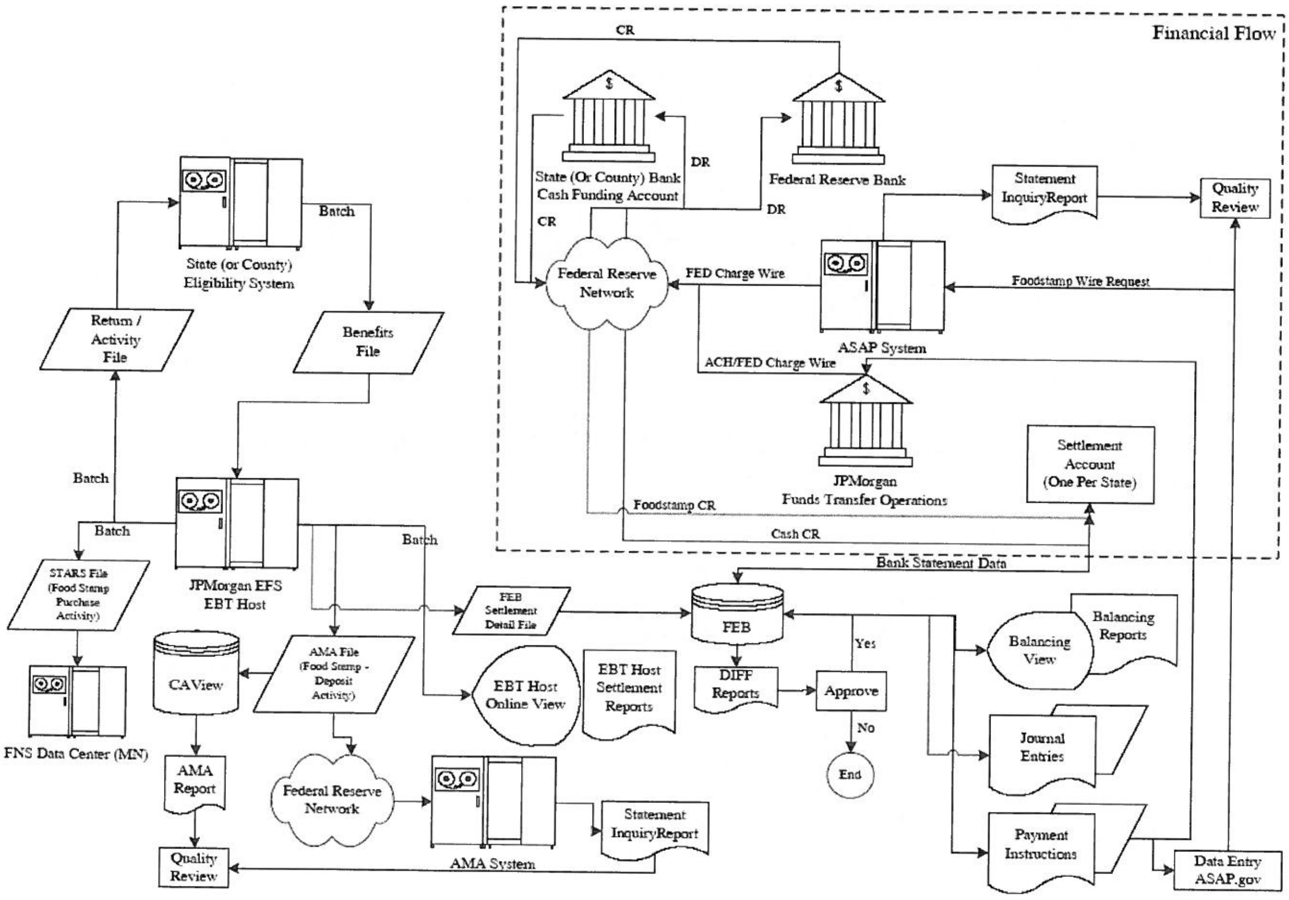
Businesses:

- Auto Finance
- Banking
- Credit Card
- Investment advice
- Lending
- Mortgages
- Payments

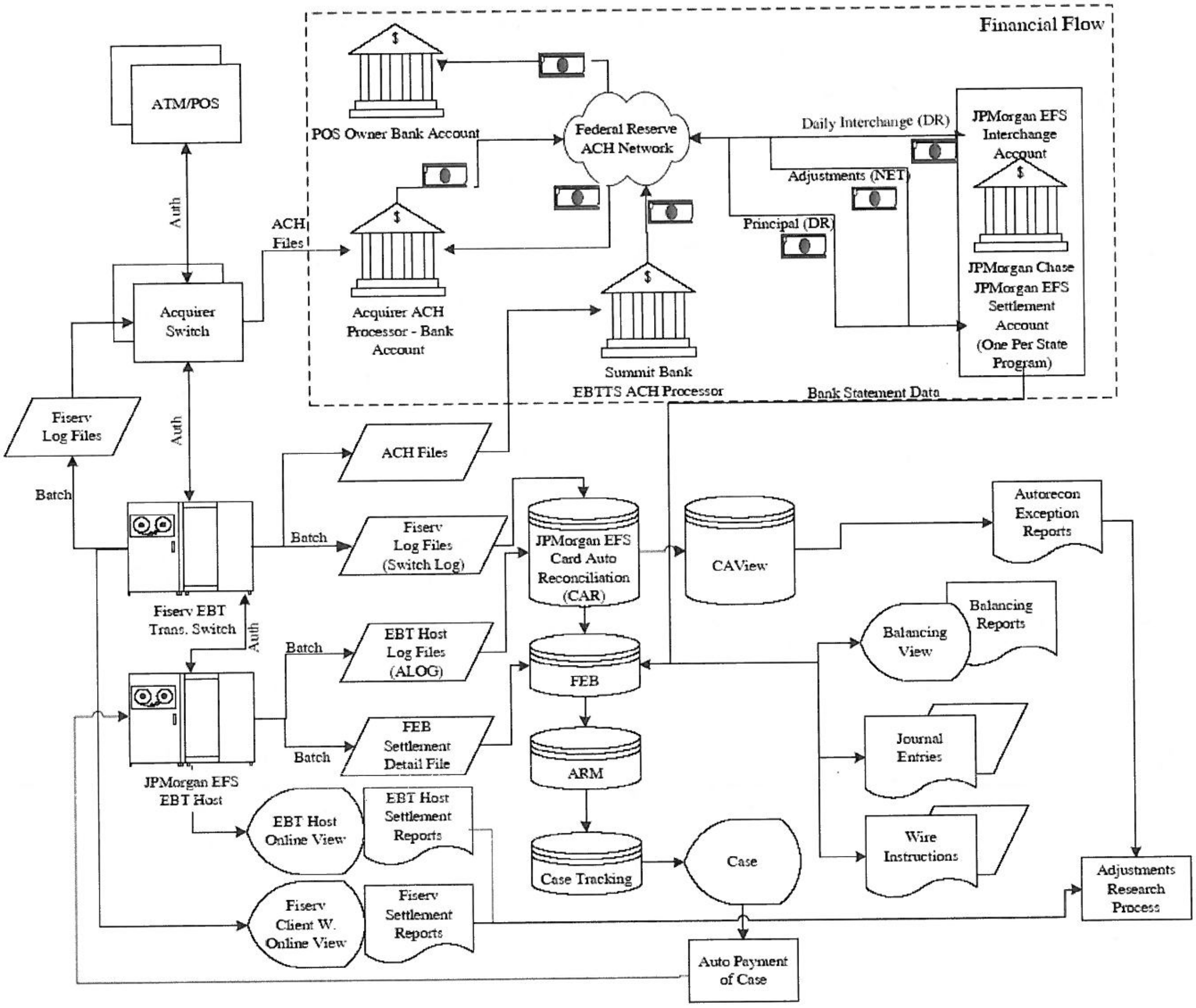
Treasury Services

- Receivables
- Payables
- Liquidity and investments
- Foreign exchange
- Information management
- Global Trade
- Escrow

Attachment 2: Settlement and Reconcilement — Inbound from Benefit Issuer



Attachment 3: Settlement and Reconcilement — Outbound to Network


Financial Flow
ATM/POS
Auth
Acquirer Switch
ACH Files
POS Owner Bank Account
Acquirer ACH Processor - Bank Account
Federal Reserve ACH Network
Summit Bank EBTTS ACH Processor
Daily Interchange (DR)
Adjustments (NET)
Principal (DR)
JPMorgan EFS Interchange Account
JPMorgan Chase JPMorgan EFS Settlement Account (One Per State Program)
Bank Statement Data
Fiserv Log Files
Batch
Auth
ACH Files
Batch
Fiserv Log Files (Switch Log)
Fiserv EBT Trans. Switch
Auth
Batch
EBT Host Log Files (ALOG)
Batch
FEB Settlement Detail File
JPMorgan EFS EBT Host
JPMorgan EFS Card Auto Reconciliation (CAR)
FEB
ARM
Case Tracking
CAView
Autorecon Exception Reports
Balancing View
Balancing Reports
Journal Entries
Wire Instructions
Case
EBT Host Online View
EBT Host Settlement Reports
Fiserv Client W. Online View
Fiserv Settlement Reports
Auto Payment of Case
Adjustments Research Process

This Report on Treasury Services' Description of its Electronic Benefits Transfer Services System and on the Suitability of the Design and Operating Effectiveness of its Controls is strictly confidential. It is intended only for use by JPMorgan Chase Bank, N.A., and its affiliates, clients whose services are covered by this report and their independent auditors. Unauthorized use of this report in whole or in part is strictly prohibited.

J.P. Morgan Treasury Services
jpmorgan.com/ts

MOLINA®
Medicaid Solutions

August 30, 2013

Emily McCoy, RN, BSN
Director, MMIS Operations
Division of Operations Management
Bureau for Medical Services
350 Capitol Street, Room 251
Charleston, WV 25301-3709

TRACKING NUMBER: WV13242-C

SUBJECT: 2013 Molina Medicaid Solutions SSAE-16 Report

Dear Ms. McCoy,

Please find attached the 2013 Ernst & Young LLP, SSAE-16 Report for the period of July 1, 2012 through June 30, 2013.

If you have any questions, please contact me at 304-348-3322.

Sincerely,

Barbara Holmes for

Tony Kazan
WV Deputy Account Manager

Document Acceptance Signature Form

MOLINA
Medicaid Solutions

Emily McCoy, RN, BSN
Director, MMIS Operations
Division of Operations Management
Bureau for Medical Services
350 Capitol Street, Room 251
Charleston, WV 25301-3709

Date: 8/30/2013

Subject: 2013 Ernst & Young, Molina Medicaid Solutions SSAE-16 Report

Tracking #: WV13242-C

Submitting Molina Employee: Stephen Secrist

Signed for and on behalf of **Bureau for Medical Services (BMS)**	Signed for and on behalf of **Bureau for Medical Services (BMS)**
Name:	Name:
Title:	Title:
Date:	Date:

MOLINA
Medicaid Solutions

Service Organization Controls 1 Report

Description of Molina's West Virginia Medicaid Management Information System

For the period July 1, 2012 through June 30, 2013

With Independent Service Auditor's Report Including
Tests Performed and Results Thereof

Molina Medicaid Solutions

Service Organization Controls 1 Report

Description of Molina's West Virginia Medicaid Management Information System

For the Period July 1, 2012 through June 30, 2013

With Independent Service Auditor's Report
Including Tests Performed and Results Thereof

Table of Contents

MOLINA
Medicaid Solutions

Molina Medicaid Solutions' Management Assertion

August 29, 2013

We have prepared the accompanying Description of Molina's West Virginia Medicaid Management Information System (WV MMIS) (Description) for the period July 1, 2012 through June 30, 2013 for the State of West Virginia ("State") who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. The management of Molina confirms, to the best of its knowledge and belief, that:

a. The Description fairly presents the Molina's West Virginia Medicaid Management Information System (System) made available to the State during the period July 1, 2012 through June 30, 2013 for processing their transactions. The Company uses its New Mexico Data Center Operations organization to host the system hardware required to support the West Virginia MMIS operations. The Description includes only the controls and related control objectives of the Company and excludes the control objectives, and related controls of the Molina New Mexico Data Center Operations organization. The criteria we used in making this assertion were that the description:

(1) presents how the System made available to user entities was designed and implemented, including

- the types of services provided, including, the classes of transactions processed.

- the procedures, within both automated and manual systems, by which those services are provided, including by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities.

- the related accounting records supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports provided to the State.

- how the System captures and addresses significant events and conditions other than transactions.

- the process used to prepare reports or other information provided to user entities.

- specified control objectives and controls designed to achieve those objectives.

- controls that, in designing the System, we contemplated would be implemented by user entities in order to achieve the specified control objectives (Complementary User Entity Controls).

- other aspects of the Company's control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided, including processing and reporting transactions of user entities.

(2) does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of the State of West Virginia and its independent auditors, and may not, therefore, include every aspect of the System that the State of West Virginia and its auditor may consider important in its own particular environment.

b. the Description includes relevant details of changes to the System during the period from July 1, 2012 through June 30, 2013.

c. the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period July 1, 2012 through June 30, 2013 to achieve those control objectives if user entities implemented the Complementary User Entity Controls and subservice organizations applied the controls contemplated in the design of the Company's controls. 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.

(2) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent those control objectives stated in the Description from being achieved if user entities implemented the Complementary User Entity Controls and subservice organizations applied the controls contemplated in the design of the Company's controls.

(3) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Molina Medicaid Solutions
August 29, 2013

ERNST & YOUNG

Ernst & Young LLP
One Commerce Square
Suite 700
2005 Market Street
Philadelphia, PA 19103

Tel: +1 215 448 5000
Fax: +1 215 448 4069
www.ey.com

Independent Service Auditor's Report

Management
Molina Medicaid Solutions

Scope

We have examined Molina Medicaid Solutions' ("Molina") accompanying Description of Molina's West Virginia Medicaid Management Information System (WV MMIS) for the State of West Virginia ("State") transaction processing and administration throughout the period July 1, 2012 through June 30, 2013 (Description), and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Molina's controls are suitably designed and operating effectively, along with the related controls at Molina. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Molina uses the Albuquerque, New Mexico data center, operated by Molina New Mexico, for the hosting of its MMS Health PAS systems, and for physical security, environmental safeguards, backup and recovery, and hardware maintenance. The Description includes only the control objectives and related controls of Molina and excludes control objectives and related controls of the New Mexico data center. Our examination did not extend to controls of the Molina New Mexico data center.

Molina's responsibilities

Molina has provided the accompanying assertion titled *Molina Medicaid Solutions' Management Assertion* ("Assertion") about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description. Molina is responsible for preparing the Description and the Assertion, including the completeness, accuracy and method of presentation of the Description and the Assertion, providing the services covered by the Description, specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion and designing, implementing and documenting controls 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 described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination 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 fairly presented and the controls described therein are suitably designed and operating effectively to achieve the related control objectives stated in the Description, throughout the period July 1, 2012 through June 30, 2013.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls described therein to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives, and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Molina's Assertion:

a. the Description fairly presents the WV MMIS that was designed and implemented throughout the period July 1, 2012 through June 30, 2013.

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 July 1, 2012 through June 30, 2013 and, if the State applied the complementary user entity controls contemplated in the design of Molina's controls throughout the period July 1, 2012 through June 30, 2013.

c. the controls tested, which, together with the complementary State controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period July 1, 2012 through June 30, 2013.

Description of tests of controls

The specific controls tested, and the nature, timing, and results of those tests, are listed in the accompanying *Description of Control Objectives, Controls, Tests and Results of Tests.*

Restricted use

This report, including the description of tests of controls and results thereof in the *Description of Tests and Results* is intended solely for the information and use of Molina, the State of West Virginia, and the independent auditors of the State, who have a sufficient understanding to consider it, along with other information including information about controls implemented by the State, when assessing the risks of material misstatements of the State's financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst + Young LLP

August 29, 2013

Section III. Description of Molina's West Virginia Medicaid Management Information System

Scope of Report

This section of the Statement on Standards for Attestation Engagements 16 report has been prepared by Molina Medicaid Solutions ("MMS"), a wholly owned subsidiary of Molina Healthcare, to provide information about controls of MMS that may be relevant in assessing the internal controls of the WV MMIS for the State Department of Health and Human Resources and the Bureau for Medical Services ("BMS"). This report does not encompass all aspects of the services provided or procedures followed in conjunction with the WV MMIS system.

Overview of Operations

The MMS West Virginia ("WV") facility is managed and operated by Molina Healthcare. Headquartered in Long Beach, California, MMS manages Medicaid information processing facilities and fiscal agent services for multiple states throughout the United States. The Charleston, West Virginia facility is dedicated exclusively to supporting Medicaid processing for the State. MMS utilizes a data center in Albuquerque, New Mexico, operated by Molina Healthcare. The Description excludes control objectives and controls of Molina related to controls at the New Mexico Data Center.

Control Environment

The WV MMIS operation is designed to provide service to the State. As of June 30, 2013, there were 109 employees at the MMS WV MMIS site to meet customer requirements. There are approximately 50 additional staff, residing across the United States, which also provide support to the WV MMIS.

Section III. Description of Molina's West Virginia Medicaid Management Information System

The Account Director of the Charleston facility provides the overall management of the WV MMIS operations. Several functional groups report to the Account Director; the groups that are within the scope of this report are described below:

- Systems – Provides application development, maintenance, and configuration support to meet the State's information systems and reporting requirements, daily operational and technical support of claims processing, and local area network administrative services for users of the Charleston facility.

- Quality Control – Provides reviews and audits of the quality control procedures in operational and technical areas; identifies areas for improvement and makes recommendations for improvements.

- Claims Processing – Provides data collection and entry support for Medicaid claims. Once entered into the claims processing module, claims are adjudicated to a pay, pend, or deny status, using the Provider, Member, and Reference files. Those claims in a pend status are then resolved through an online review of these claims.

- Provider Relations and Enrollment – Provides assistance to Medicaid providers with billing and tracking claims; informs providers of billing updates and changes as well as communicates billing information. Provider Relations and Enrollment performs the enrollment of Providers into the West Virginia Medicaid Program. In addition, Provider Relations and Enrollment also performs input or change of provider information upon BMS approval. Housed within provider relations is the member services call center where assistance is given to Medicaid recipients, or members, who have questions regarding claims payments, coverage, and other general questions.

- Flexi or Finance Support – Provides the support required for the weekly claims payment run. Also responsible to establish provider requests for electronic funds transfers; reviews and reconciles provider 1099 data; and provides data to the BMS regarding claim financial information.

- Finance and Human Resources – Provides internal financial and personnel management services for MMS WV MMIS and its employees.

- Computer Operations – Provides operations support to MMS facilities and customers.

- Network Operating Center Support Center – Takes responsibility/ownership for management of the MMS WV MMIS production environments. The Network Operating Center group provides centralized coordination, management, and scheduling of production system activities.

- Security Management – The On-Site Technical Support Supervisor functions as the owner of security controls and processes for the MMS WV site. In addition, there are support personnel in the New Mexico Data Center in Albuquerque, New Mexico, and the corporate security department located in Long Beach, California also supports Medicaid processing for the State MMS.

In addition, there are support personnel in the MMS Development Centers in Herndon, Virginia that also support Medicaid processing for the State.

Risk Assessment

MMS WV MMIS Operations has implemented a risk assessment process to identify and manage risks that could affect its ability to provide reliable transaction processing of Medicaid transactions for the State. This process requires management to identify significant risks inherent in the operational and technical processing of the various types of Medicaid transactions and operational procedures being conducted for compliance with the State, federal, and Centers for Medicare and Medicaid Services (CMS) guidelines. This process has identified risks resulting from the nature of the services MMS WV MMIS Operations provides. In response, MMS management has implemented various measures to manage those risks.

Monitoring

MMS WV MMIS Operations management and supervisory personnel monitor the quality of their Medicaid control performance as a routine part of their activities. To assist them in this monitoring, MMS WV MMIS Operations staff has implemented a series of daily, weekly, monthly, quarterly, and annual reports that measure the results of various operational processes involved in processing transactions for the State. These processes allow WV MMIS Operations management to constantly review and attend to any issues regarding the quality of system and operational performance in a timely fashion.

On a monthly basis, operating quality performance reports, or report cards, are provided to MMS management and the State that summarize the performance statistics of the WV MMIS, including, but not limited to, system and online transaction processing, transaction and batch throughput, and numerous operational metrics. Production service managers review various other reports on a daily basis to monitor the status of application and transaction processing. Daily operating reports are provided to the State to assist them in monitoring their business.

On a monthly basis, MMS Corporate also reviews internal operating results.

Information and Communication

To help align MMS' business strategies and goals with operating performance, management is committed to maintaining effective communication with its personnel. Management across the organization participates in weekly meetings to discuss the status of current client processing, organizational structure, and other matters of interest and concern. Personnel are encouraged to bring issues or suggestions to the attention of management to be addressed and resolved. In addition, MMS personnel are required to attend monthly company meetings for updates on recent business performance and other matters.

Information System Control Environment

Application Development and Maintenance

The State has the primary responsibility for submitting change requests to business and/or technical processing in the form of formal Change Requests (CRs). In addition, MMS WV MMIS staff can also author CRs, but these CRs must be submitted to State Medicaid management for approval. A CR may pertain to a system or operational modification or enhancement, maintenance, or other change, or the creation, modification or production of a report.

Regardless of the origin or type of request, the first step is to enter the request into the Rational Clear Quest tracking system. The system automatically assigns a CR number to each request. MMS analytical staff then determines the nature of the request and assigns it to the appropriate resource. MMS analytical staff then decides if a CR is requested to create a new process or to modify an existing process. After the State approves the CR, testing will begin. The results are reviewed with the State before the CR is implemented into production. After the State approves the test results, a Production CR (RQMS) is submitted, and is presented to the Change Control Board, which will approve or deny the software change. If approved, the code is then created for the CR.

Promotion of changes is controlled by the WV MMIS Change Control Board and the CR process. The CR and Emergency Change Request (ECR) process are used to approve, promote, and schedule normal and emergency changes. CRs generally require a minimum of 24 hours advance notice before they are applied to the production system. The approved changes are scheduled by the Network Operating Center staff.

System Software Development and Maintenance

System software changes, changes to the operating system, supporting software packages, and scripts or base application code packages that are unrelated to business processing are requested by either a system programmer, network engineer or the operation supervisor (for hardware issues) at the NMDC. The initial request is documented by completing a RQMS, which is another installation of the Rational Clear Quest tool. Only authorized users have access to this electronic form and users must authenticate to the database with an ID and password before access to the electronic form is granted. With the creation of the request form, the system will automatically assign a tracking number to the request.

Changes are then reviewed and approved by the requestor's immediate manager. The system is designed to send an e-mail for an electronic approval once the request is completed. Daily conference calls and/or meetings are held with the system programmers, networking engineers, and other individuals who have submitted system requests, to discuss the recent and upcoming changes.

Scheduled changes are tested in a logical partition of the Health PAS Test Environment. Emergency changes are defined as changes that need to be implemented within 24 hours. Testing, where appropriate, is completed for all emergency change requests. In instances where testing has not been completed, a written justification must be submitted to management explaining why testing is not required given the specific circumstances and the type of change and management approval obtained before the change is implemented. Scheduled changes cannot proceed to the production environment without proper testing. Each day, a schedule is produced listing the changes planned for that day and is distributed to the system's software change team, as well as affected customers. Daily, a Change Control Board reviews the planned changes and advises if the technical staff has the approval to proceed with their change implementation.

For emergency changes that are made, the programmer will complete the HIMProdCR screen in the RQMS system and obtain the necessary approval from the Change Control Board prior to change being implemented. The HIMProdCR requests are stored indefinitely within the RQMS system.

Logical Access Controls

All employees and contractors of MMS are required to have a logon identification assigned to them by the Network Administrator to utilize an MMS computer system. The use of this logon identification and password provides users with access to the information and data within the MMS computers to which they have been authorized access. Users that allow others to utilize their access privileges are in violation of security and will be processed as a security violation when discovered.

Users are responsible and accountable for the control and use of the assigned logon identifications and passwords assigned to them.

Overview of User Security Controls

The following lists the basic security policies which MMS WV MMIS users must follow:

- Users shall log out and shut down their workstations at the end of each day, unless it is required for the workstation to be left on for processing or security update.
- If a user notices or becomes aware of any unusual login activity on their account, the user will report it immediately to the Network Administrator.
- Users are required to lock (Ctrl, Alt, Delete) their workstations while unattended, unless their workstation is physically secured. This prevents other users from accessing the user's workstation while they are not present at their desk.
- Users are not permitted to script their user IDs and passwords for logon access.

- Users are not permitted to allow another person to log on to any computer utilizing their account information, nor are they permitted to utilize someone else's account information to log on to a computer.

Security administration over the System is a two-tiered system. The first level of security over the system is the Active Directory Domain Policy, without which a user cannot access Health PAS. A description of security administration within Health PAS-Administrator™ is outlined below.

Physical Security Controls

Charleston

During the normal business hours of 8:00 a.m. and 5:00 p.m., a receptionist is responsible for monitoring access through the front entrance of the Charleston facility. Doors permitting access to the interior of the building are locked and controlled by a badge access system. Employees have a key card badge and a badge with their photograph. There are seven doors in total that are controlled by the key card system at MMS WV MMIS, which requires an active card to enter the building from the receptionist area.

Special badges with limited access are provided for temporary employees, visiting employees from other facilities, and for visitors. Visitors are required to have an MMS WV MMIS escort for access to the facility. There is a log kept at the receptionist's desk that visitors are required to sign. Once a visitor is signed in, they are given a visitor key card to display while in the building. Temporary and visitor badges allow access to the front door, lobby entrances, and side door only.

The badge reader system controls physical access to the computer room. There are two doors that allow access to the server room. Access to these two doors is limited to authorized individuals through the key card system. Access authority granted through badge readers is based on an employee's job responsibilities. Any employee who forgets a badge will be issued a temporary key badge which will allow access to the facility.

When an employee terminates, the employee's security access badge is retrieved and deactivated from the security system. When a person changes job responsibilities through a transfer, the manager/supervisor is responsible for providing notification to grant or revoke access to the necessary badge readers. Also, if an employee loses his/her badge, the individual is required to inform the local WV MMIS Facilities Manager to place the card into "lost" status, and make arrangements to obtain a replacement badge. The lost badge is then deactivated from the security system.

The badge log is reviewed to assure that all temporary and visitor badges have been returned to the receptionist. If a badge is unaccounted for, the receptionist notifies the appropriate area to deactivate the badge.

Environmental Protection Safeguards

Charleston

The building contains a water sprinkler system that is activated by heat sensors. The water sprinkler heads activate/discharge independently of one another. The facility is also protected by a fire alarm system and hand-held fire extinguishers. The computer room itself is located on a raised floor inside the MMS WV MMIS building. It is protected by a halon gas fire suppression system. The climate within the data center is controlled by both the building air conditioning and a separate air conditioning unit within the data center.

In the event of a power failure, there is an emergency power system ("EPS") installed in the Charleston facility that consists of an inline uninterruptible power supply ("UPS"). The MMS Charleston facility is periodically inspected by the local fire department.

Production Scheduling

The Network Operating Center (NOC) is handled by Molina support located in the Herndon, Virginia and Long Beach, California offices. There are daily Network Operating Center conference calls with the Charleston office.

Each production cycle is scheduled by the Network Operating Center staff and reviewed by the Charleston management team. The previous day's activity is reviewed each morning by the Network Operating Center team and the Charleston management team. Network Operating Center personnel in the Herndon office have access to make changes to the daily job schedule.

Application Environment Overview

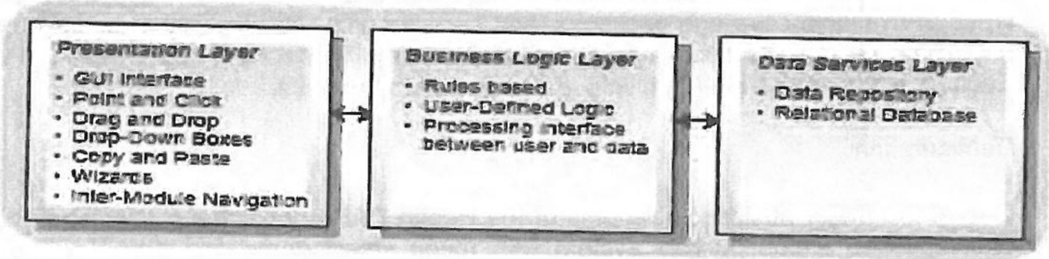
The WV MMIS for the State is the Health PAS Solution, which is a collection of Commercial-Off-The-Shelf (COTS) systems. The Health PAS-Administrator™ utilizes the QNXT system by TriZetto for claims processing, member enrollment, provider enrollment, and authorizations. Below is a brief description of some of the main Health PAS-Administrator systems, its key modular components, and an overview of the other Health PAS Solution components.

The Health PAS Solution

Health PAS consists of eight major components, integrated to create a flexible, adaptable structure that delivers a suite of tools, loosely coupled in a flexible framework to meet current and future business requirements. Health PAS is an end-to-end solution of integrated applications.

The open architecture of Health PAS applications enables standard interface capability throughout the system in a flexible infrastructure. This feature supports future incorporation of new functionalities within the components and integration of other applications and products as program priorities change and new business needs arise.

This solution provides the ability to use specific software/tools in a flexible framework. Health PAS is built on Microsoft technology, maximizing usability with extensive mouse functionality, point-and-click, drag-and-drop, drill-down menu selection, drop-down menu picks, and copy-and-paste functionality. The resulting user interfaces are easy to navigate and intuitive, and the population of data in each module is step-driven through wizards. The Health PAS architecture follows the industry-recommended approach of separating system services into three logical layers – presentation services, business logic and data services. This structure is illustrated below:



Health PAS-Administrator Overview

Health PAS-Administrator furnishes the core MMIS functionality to support a state's Medicaid program, including maintaining provider, member and reference data, as well as processing and adjudication rules for claims, encounters and prior authorizations. Health PAS-Administrator also provides configuration and system management tools to govern access to data, user security, and communications. Health PAS-Administrator is an object-oriented, rules-based software application that is designed to manage multiple lines of healthcare business. The system employs a unified relational database that enables efficient use of data and consistent information throughout all Health PAS applications.

Health PAS-Administrator includes functionality for claims processing and adjudication, provider administration, benefit plan and policy administration, member administration and medical service authorization management.

Key Features and Functions

- Multi-Payer Features

  The MMS solution provides multiprogram capability. Designed to address the needs of Medicaid payers, Health PAS offers processing capabilities for the definition and management of alternative programs and capitation/risk-sharing administration. These capabilities can be customized through configurable, user-definable parameters and business rules without the need for software modifications. These features enable WV MMIS to quickly make changes and implement new programs, policies and procedures. Some instances where this flexibility would expedite change are in the addition of waiver programs, the modification of benefits for members, or even processing claims for other agencies.

- Policy Administrator

The health insurance benefits an eligibility organization offers its members are defined in its policies. A policy describes the benefits organizational members may receive under the various benefit plans, riders and rate codes (aid categories or program/status codes) available under the policy.

The Policy Administrator module allows WV MMIS to define many of the components that may be included in a policy, such as the types of copayment services, the different types of available coverage packages, and benefit riders. An eligibility organization can have multiple policies and each policy can have multiple benefit plans attached to it. Each benefit plan can have multiple rate codes/aid categories.

- Configuration

One of the major business strengths of the Health PAS-Administrator solution is that it encompasses a configurable system with menu select items and drop-down boxes rather than a traditional hard-coded MMIS. The MMS solution is designed to leverage the capabilities of modern, commercially available products and a unified relational database structure to allow analysts with Medicaid knowledge to configure a system that supports business requirements and policies both efficiently and cost effectively.

The configuration feature of Health PAS-Administrator affords WV the opportunity to manage Medicaid processing at the source. Transparent to most users, the Configuration module functions in the background as a centralized store of information. Within its relational database structure and rules-based architecture, the Configuration module contains data elements that support most Health PAS-Administrator processing modules, including Member, Provider, Claim, Credentialing, and Call Tracking. The information can be updated online, in real-time and is consistent throughout.

The modules that are considered to be Configuration-related modules are as follows:

Configuration Module

The Configuration module contains system parameters that control how the system operates. A few examples are actions, alert codes, attributes, call resolutions, call types, rule reasons and specialties. These values are used throughout the QNXT environment.

Medical Codes Module

This module is used to store and maintain the library of medical-related codes to be used for Medical Management: ICD-9 and diagnosis groups; Case Management criteria, including Early Periodic Screening Diagnosis and Treatment ("EPSDT") code setup; Authorization Reason Codes, etc. These codes are referenced throughout Claim, Benefit Plan, Policy, Authorization and Contracts and must be populated prior to proceeding with configuration of the other modules.

Claim Finance Codes Module

This module is used to store and define claim-related codes other than diagnosis codes. Claims are edited against codes contained in these tables: CPTs, Revenue, HCPCS/Rev combinations, Condition Codes, Occurrences Codes, Type of Bill, Modifiers, etc. In addition to setting up a full set of valid codes, the administrator can begin to organize these codes into meaningful groups that will be used later.

Fee Tables Module

This module is used to create and maintain all current and historical rates at the code level. These are used in the configuration of the Program and Contract modules. Before a Program can be saved, there must be a default fee schedule selected for the Program. The fee schedule that is used as a base usual and customary fee schedule should be loaded and named prior to creating a Program. Fees (or prices) are set on a code-by-code basis, and can be detailed by code and modifier.

Rules Module

This module is used to initially set the system options. Pre-configuration options consist of choices that activate or disable table-driven functionality within the overall system. These options are generally set immediately following system installation; however, they can be updated, as needed, as requirements further define the necessary system functionality up to the point of actual system implementation. Pre-configuration options are grouped according to the module that provides the functionality option.

Application object actions (triggers) are also configured and set up here, as are user interface activities options, electronic data interchange ("EDI") data import and export rules, and claims edit processing rules.

Restriction Groups (Benefit Plans and Contracts Modules)

The system administrator can apply restriction groups in configuration of Benefit Plans and Benefit Terms and Contract Plans and Contract Terms. Restrictions can be defined by including or excluding diagnosis codes, location codes, cpt/hcpcs, revenue codes, service groups, place of service codes, occurrence codes, condition codes or value codes or any combination of these code types.

Key Health PAS-Administrator Module Functionality

Utilization Management

The Authorization module of QNXT handles the prior authorization of services. This includes the minimum data set authorizations for Long Term Care claims. Electronic authorizations are also received from the West Virginia Medical Institute ("WVMI") and American Psychiatric Services, who provide authorizations on behalf of the State.

Authorization allows an authorized system analyst or user to create and modify prior authorizations, view a member's referral history and manage the overall authorization process. Templates based on authorization type are pre-defined and guide the prior authorization user through the steps needed to complete all required data elements for the authorization. Authorizations can be validated and priced in real-time to determine that an authorization is for an eligible member and/or provider and is for a valid service.

The Authorization module is also a work flow management tool. All authorizations that need review are displayed. Authorizations can be assigned to the medical staff by dragging and dropping the authorization to the folder name of the assigned employee. Clinical notes can be shielded from general system users through user security.

Benefit Plan

A Benefit Plan details the agreement between the State and the individuals and/or groups contracted to provide services to eligible members. In some states it is referred to as a Benefits Matrix or an "Evidence of Coverage."

There is no limit to the number of Benefit Plans that can be created for a Carrier. However, a Benefit Plan may belong to only one Program. Each Benefit Plan contains header information and detail information. The header information applies to the entire Benefit Plan. The detail information comprises the specific benefit terms (allowable services) that make up the Benefit Plan.

The Benefit module of QNXT controls all of the benefit details. The WV MMIS has 11 unique benefit programs:

- Behavioral Health and Health Facilities
- Bureau for Medical Services State Programs ("BMS")
- Children's Specialty Care
- Eligibility Exams
- Emergency Medical
- Juvenile Service
- Limited Pharmacy Services
- Medicaid
- Pre-Admission Screening and Resident Review ("PASRR")
- Special Medical Services
- Tiger Morton – Catastrophic Illness

Each state program has configured Benefit Plans. The plans contain the specific services that each plan allows and does not allow and the business processing rules regarding how these services can and cannot be utilized.

Carrier

A Carrier is defined as an entity that owns or manages one or more insurance programs and is the highest level of the summarization for reporting purposes (e.g. Bureau for Medicaid Services). In other words, a Carrier is one owning health care organization within the system. A Carrier is an organization that is responsible for claims processing and policy decisions concerning its members and providers.

Health PAS-Administrator can accommodate more than one owning organization's claims processing within the same system. For example, Bureau for Medicaid Services could be one Carrier, Department of Mental Health another, and Blue Cross Blue Shield, a Coordination of Benefits (COB) Carrier.

Programs, Benefit Plans, and policies that drive the processing and administration logic of the system are each affiliated to a specific Carrier and require the Carrier relationship in order to process claims within the system.

This module supports three distinct types of Carriers:

- **Health Plans** – an internal entity such as the Bureau for Medicaid Services. An administrator would input the Health Plan for the governing body paying claims and making policy decisions as a Carrier. Any Health Plan (such as a Medicaid Agency) for whom the system would be paying claims would be configured as a Health Plan Carrier.

- **COB Carriers** – An administrator would set up, within the system, any commercial or self-funded plan that would be the primary insurance plan for a member, and for which the main health plan is set up NOT to be responsible for claims payment. The setup of this module is to accommodate calculations for secondary claims payment. Medicare Carrier and Programs, such as Parts A, B, D, and AB would be configured here.

- **TPL Carriers (Third-Party Liability)** – This type of carrier is designed when an accident is potentially involved and liability for claims payment shifts from the insured's health plan to the TPL carrier.

A Carrier establishes the entities that are ultimately responsible for the claims processed by the system that are incurred by the eligible members. For example, a State Medicaid office or department is generally considered to be the Carrier when Health PAS-Administrator is set up to be an MMIS system.

Additionally, the Carrier module enables the user to efficiently manage different lines of business (i.e., Commercial, Medicaid, Self-funded, Medicare) within the same system if they so choose. A Carrier must be set up before any Programs can be associated with that Carrier. Under each Carrier, there are one or more Programs. Program logic defines how the member's benefits and provider's reimbursement are to be managed within the system and how it relates to the entity responsible for fiscal oversight (Carrier). Benefit Plans are connected to Programs and represent all the services a member can receive.

Claims

The Claims module is where the claim inquiry and claim correction functions are accessed. The Claims module allows the user to record, process and pay for services members receive from providers and other organizations.

The Claims module has two major functions:

- Logging a claim based on entering claim header information only; and
- Processing which includes the header information plus the detail information (line detail) on the claim. Claims are interactively adjudicated in real-time and submitted for payment. Large sets of claims can automatically be adjudicated using the mass adjudication module.

Claims can be searched for by claim number, provider number, member number, dates of service, dates of adjudication, clean claim dates and paid date. Memos can be added to claims for future reference. The Claims module also contains a field that indicates the processing steps that the claim went through.

This module automates the payment process and allows the adjudication of the majority of the claims inventory with minimal decision-making.

Additional Claims Module Features:

- If edits post during the adjudication process, all the edits will be displayed for the processor to research in order to determine the final disposition of the claim.
- Duplicate claim edits will fire even if the duplicate claim is in the same batch. The first claim through will process; the second and subsequent claims will stop for duplication.
- Each claim maintains an audit trail detailing the person who entered the claim, the person who submitted the claim for payment and the person who made any adjustments to the claim.
- Claims can be voided, reversed, or adjusted (reversed and replaced).
- Claims can be queried by provider, member, date of service, authorization number, claim number, adjudicate date, clean claim date and paid date.
- Within the Claims module, a member's entire or partial claims and/or authorization history can be accessed.
- Within the Claims module, a provider or member module can be accessed and opened for review and/or research during the processing of claims (based on configured role).
- Within the Claims module, the required documents may be accessed and opened for review during the processing of claims.
- The Claims module displays every processing step each claim went through during adjudication. This feature is extremely useful for research and for auditing.
- Any and all service limits are immediately updated as claims are processed. The limits may be viewed from either the Member module or the Claims module.
- Memos can be attached to claims.
- Health PAS-Administrator contains a Claim Work Flow module. This module allows the user the ability to review any of the claims that have not been processed. Claims can be selected on a variety of criteria, including:
  - Type of claim
  - Type of edits involved in processing the claim
  - Date the claim was originally logged
  - Review the entire results of mass adjudication

Contract

The Contract module contains the specific services that providers can perform as well as payment methodologies. The contracts can be either generic or specific. Each contract contains header and detail information. A generic contract would apply to a similar group of providers performing similar services. Some providers such as hospitals are given their own contracts that are custom tailored to the services they perform and the payment schedule that the State has agreed to reimburse the facility. The contracts are added to the individual provider numbers at the time of enrollment and can be modified at any time.

The Contract module is where provider pricing methodologies are configured for individuals and/or provider types. Contracts can use usual and customary rate or custom fee schedules and may contain many options. A provider's claim selects one contract during claim adjudication. A provider has one active contract per program, per affiliation.

Capitation tables are also built within the Contract module. During a capitation cycle, a single payment (not a claim) is calculated based on the capitation table and member assignment to that Provider. The Contracts module of Health PAS-Administrator is one of the more comprehensive parts of the Health PAS solution because it incorporates so many aspects of the provider, member and claim criteria into an array of reimbursement methodologies. A single contract may have an unlimited number of contract terms, each of which can be restricted by member age and/or gender, and by provider criteria: provider type, specialty, servicing location and primary care physician ("PCP") status. Each term may also be tailored to support the following claim criteria: service codes, modifier codes, diagnosis codes, groups, places of service, bill types and PA or attachment requirements. Once the claim adjudication process selects the appropriate contract and term for payment, any of the methodologies listed above may be used for calculating payment.

If certain services are covered under capitation, Health PAS can configure contract terms that are associated with capitation factors (variable by client gender, age and condition) or a capitation rate table (variable by client gender, age and grouping code). Health PAS users may also enter individual capitation adjustments per provider, per assigned client, as needed.

Pricing rules are governed by contract terms in the Contract module; these contract terms can be varied by provider type and/or specialty to cover more provider entities with a single contract to lessen complexity and maintenance.

Medical Codes

This module is used to store and maintain the library of medical-related codes to be used for Medical Management: International Classification Diseases – Version 9 (ICD-9) and diagnosis groups; Case Management criteria including EPSDT code setup; Authorization Reason Codes, etc. These codes are referenced throughout Claim, Benefit Plan, Policy, Authorization and Contracts and must be populated prior to proceeding with configuration of the other modules. The module also controls the authorization templates.

Medical Policy

Medical Policy represents the high-level global business rules for processing, denying or pending claims for the entire system. For example, an organization would generally set up medical policy rules and criteria for its lifetime processing rules, such as one hysterectomy per woman per lifetime, within a claims processing organization.

The Medical Policy module is comprised of two main areas of functionality: Medical Policy Criteria and Medical Policy Rules. The Medical Policy module allows the configuration of global medical and processing criteria and rules.

Medical Policy Criteria are requirements that validate if a claim is appropriate for a particular Health Plan. Medical Policy Criteria consist of service codes, diagnosis codes or procedure codes that make up a particular business rule that can apply to the entire Health Plan.

Medical Policy Rules contain specific requirements for validating claims when a medical policy rule is selected at the program, benefit plan or organization policy level. Medical Policy Rules also consist of service code groups and associated claims processing rules. Whenever a claim meets the criteria within the rule, the system posts the appropriate claims message and pends, denies or pays the claim based on the rule contained within the Medical Policy Rule. Any Medical Policy Rule actions that are set will override the rules set for a particular Program where the Medical Policy Rule set is selected (e.g., Benefit Plan and eligibility organization) to override.

Medical Policy Criteria apply to all Health PAS-Administrator Programs and are triggered at the service or procedure-code level. Medical Policy Rules are set at the Program, Benefit Plan, or organization policy. If a claim that belongs to a program, benefit plan or organization policy is using a specified Medical Policy Rule or Criteria that does not meet that criteria, the claim will deny or pend and the appropriate edit will be posted.

Both Medical Policy Rules and Criteria, if selected, will be applied to a claim before the more specific edits/rules configured in Benefits and Contracts. MMS uses Medical Policy Criteria to set "lifetime" service limits on selected service codes. When this is done, there is no need to configure those limits for different Benefit Plans. A Policy can be maintained centrally for certain services, reducing the need for applying certain system-wide changes throughout the separate Benefit Plans within the system.

Member

The Member module stores a unique number for each member. Health PAS is a real-time system that allows for instant viewing and updates. The member population is identified via Program, Policy, and Rate code. Members are associated with their Benefit Plans within their member record.

Benefit Plans associated with a member's record enable the member to be eligible for their specified services. These items are stored in the member record. Health PAS maintains pertinent data to the member's record. This data includes, but is not limited to: demographic information, eligibility effective and termination dates, Medicaid ID number(s), and PCP assignment.

Eligibility information is forwarded to MMS WV from a State-maintained system. Currently, this system includes eligibility information from Recipient Automated Payment and Information Data System (RAPIDS), and Families and Children Tracking System (FACTS), third-party systems/sources. In addition, eligibility information is maintained by several agencies including BMS and by other vendors (the Enrollment Broker adds and updates HMO and Position Assured Access System eligibility). The vendor will provide software for a common working file for maintenance and updating of eligibility information.

In Health PAS, the Member module links and has interdependencies with:

- Carrier
- Program
- Employer – Eligibility organizations
- Benefits
- Contracts
- Provider
- Configuration
- Claim Finance Codes
- Medical Codes
- Authorization
- Policy Administrator
- Claims

The Member and Claims modules are integrated to prevent the incorrect payment of claims. A claim will not adjudicate without a member record. During the claims adjudication process, Health PAS verifies the eligibility record of each member through the Member module and processes that member's claim in accordance with their related Benefit Plan and Terms and the Contract for which the provider rendering the service is attached.

Provider

This module houses provider demographics, program relationship, paid-to, 1099 information, group and other provider relationships.

Provider information is maintained in a single set of tables within the system. Because the system is a relational database, the provider's multiple relationships and their relationships or assignment to payment contracts are created and maintained within the affiliations tab of the module.

Provider demographic information is also stored in the details tab within the module. The demographic information includes:

- Mailing and physical addresses with foreign address capability
- Multiple languages
- Ethnicity, gender and date of birth
- NPI – National Provider Identifier

- UPIN – Universal Provider Identification Number
- E-mail, emergency phone, mobile and secondary phones

The Provider module also tracks address changes with an effective date. If an address change is made, the effective date, date of change and who made the change is recorded.

The Affiliations tab allows the client to maintain multiple professional relationships a provider may have.

For example, a provider can have a relationship with the following:

- Himself/herself (direct)
- Clinic or service location (service)
- Group of providers (group)
- Network, IPA, PPO or PHO (network)
- Group, network, IPA, PPO, or PHO (1099)
- To another physician (coverage)
- Hospital where physician is hospital staff with admit or consulting privileges (hospital staff)

Affiliations are also defined as:

- PCP – where members can be assigned and membership rosters are sent.
- Pay-To – where contracts are attached and checks and remits are sent.
- Miscellaneous – where all other relationships are defined.

Additional features available within the Provider module are:

- APS (Approved Provider Services) tab allows West Virginia to restrict the services a provider is licensed and credentialed to perform. This can ensure that a podiatrist isn't reimbursed for open-heart surgery, for example.
- The Specialty tab defines all of the specialties for the provider.
- Notes, memos, and alerts can be applied to a provider record. Alerts are uniquely defined and memos are free-form text.
- The Finance tab displays financial history specific to the provider. This includes payment history and advance information.
- The Recipient Counts tab allows West Virginia to view the total members assigned to the provider for each program.
- Calls, correspondence, notices, complaints, hearing and appeal dates, and grievances can be maintained and monitored from the provider module using the calls tab.
- Provider can be queried by full name, partial name, federal tax id, health plan identification number and by universal provider number.

User Security

User Security is the module where Health PAS-Administrator security and user permissions are managed. Users are given roles that grant access to the areas needed to complete their assigned task. Certain functions within QNXT will not be visible to users if they do not have the required permissions. Security can be restricted by:

- **Environments** – Represents a unique configuration of Health PAS-Administrator and a specific database. There can be multiple environments for a single health plan, for example, a test environment would point to a different database and may have different configuration options. Users are given access to one of three environments depending on their job responsibilities: medical, dental and pharmacy.
- **Users** – Defines individuals that can access Health PAS-Administrator, the environments that can be accessed, and their specific role within that environment.
- **Roles** – Defines the job description for a plan, and consists of activities within the application that make up the job description; a group of activities with a name that signifies a job description and grants that role all of the options within the application. The Claims staff is assigned a role that allows them to work pended claims but not update the provider file or change rule settings. The Provider relations staff is given inquiry-only access to claims and provider information. The Department Manager fills out a security request form which identifies the specific role required for that user. The security request must then be approved by account management.
- **Activities** – Functions within the application activities are objects and contain code that interacts with the application. Although a user cannot create an activity, attributes can be assigned to the activity. Activities can also be associated to roles. Department managers may use the security request form to add specific activities to specific user accounts. The Security Administrator will evaluate the request to see if a predefined role already exists. The security forms must be approved by account management.
- **Activity Group** – Enables the Security Administrator to organize activities into logical groupings. By creating groups and assigning activities to the group, a user can more effectively manage roles within the application.

Through the use of these security levels, users are given permission to modules and activities needed to perform their jobs without compromising data integrity and security.

Member Interface Analysis (MIA)

Another additional code module that was created to work with Health PAS modules is the MIA solution. This code imports demographic and eligibility data and offers an alternate data source to validate production processed data and to repair demographic details and eligibility segments. MIA datasets include historical, daily, and monthly member and eligibility files. MIA applies business rules and provides a method to compare production QNXT member eligibility data to MIA data. Extensive processing is performed to determine missing eligibility segments for existing members in the system.

Health PAS-InterComm

Health PAS-InterComm provides a collaborative intranet web-enabled portal as a convenient and automated means of sharing information and communicating with the fiscal agent through a Microsoft SharePoint Portal application. Through Health PAS-InterComm, the State may access project artifacts, including documentation, program reference information, project data, work plans, news, reports, and work flow. Health PAS-InterComm allows State personnel an easily accessible view into the fiscal agent's operation to monitor and review project progress, access contract management information such as the Report Card, and interact electronically with MMS project staff. Through the Health PAS-InterComm component, users are able to increase productivity by improved information access and integrated collaboration and by using a personalized portal view of data from various applications and sources. Health PAS-InterComm users can search for information stored in a variety of content sources, including other Health PAS components, databases, file systems, network file systems, and intranet or internet sites. Retrieved information/content is presented through a single point-of-access.

Health PAS-OnLine

Health PAS-OnLine permits providers and members to view State-approved information by means of an internet web-enabled portal. Providers may access reference materials, provider bulletins and manuals, remittance advices, eligibility information for members, web-based training, and many other documents or processes. Health PAS-OnLine enables the submission of claims on a web form and uploading of claims. Remittance advice is returned to providers through the portal as well.

With these features, providers save time and effort in claims submission/processing, access to information (for example, manuals), and availability of extensive online assistance (for example, training).

Health PAS-Document Manager

Health PAS-Document Manager provides image capture, letter generation, report output management, storage management, and retrieval capabilities throughout the system. It affords users the ability to view and print standard predefined and ad hoc reports, and to generate standard letters to providers, automatically incorporating member or provider information and optional standard paragraphs. Electronic copies of reports and outgoing correspondence are stored on disk for retrieval and print on demand.

Health PAS-Document Manager consists of six integrated core modules:

- **Capture Manager** – Provides input and processing services for documents received from an external source; these documents can be received in hard copy or by facsimile, e-mail, or other electronic means.

- **Letter Manager** – Provides for the creation and output of standard and user-customized letter-based communication to providers and members.
- **Report Manager** – Provides for the definition, formatting and manipulation of reports.
- **Storage Manager** – Provides secure storage and management of electronic documents and their associated index information (metadata).
- **Output Manager** – Provides for the distribution of documents to a variety of channels including printers, facsimile devices, file output devices, electronic in-boxes and web portals.
- **Document Explorer** – Provides Health PAS users a common interface from which to search, retrieve, view and output documents. Each module consists of one or more software products that, when combined, provide Health PAS core capabilities.

Health PAS-Process Manager

Health PAS-Process Manager provides the capability to move electronic work items through a predefined process according to the applicable business rules or ad hoc routing, enabling users such as claims resolution specialists, provider enrollment specialists and provider service representatives to direct work items to their correct destination. Document security for each type of work item is defined for the user's group. Health PAS-Process Manager provides the control metrics to locate work items, monitor work progress and generate workload reports.

Health PAS-Process Manager provides the enabling work flow technology for the Medicaid business processes to route work between participants. Health PAS-Process Manager provides event tracking, metrics reporting and documentation of individual work object histories. Work flow is the tool that provides the transportation mechanism for work objects, issues, and assignments. This component of the MMS solution forms the foundation for business processes such as administrative case management, provider enrollment/reenrollment, provider appeals, and prior authorization, to name only a few.

The work flow application routes work for these processes through either a predefined sequence of events based on business rules applied to the type of work, or information associated with the work object indexed metadata. Additionally, users have the ability to route work items based on their knowledge of the requirements. In addition to providing predefined paths, work flow can be configured interactively, allowing ad hoc routing of work objects to others at the discretion of the user.

Payment Process Module

Claim adjudication cycles (mass adjudication) are processed on weekends and Monday, Tuesday, and Wednesday nights. The preliminary payment process occurs on Thursday nights. The final payment process occurs during the day on Friday.

The payment of claims is completed on a weekly basis. The State makes the payments via check or EFT. Each week, on Thursday nights, the Health PAS Payment Wizard is used to calculate payments and finalize claims into the appropriate statuses.

The finalized claims are then loaded into the Health PAS Flexi Financial module; the claims become selectable accounts payable (AP) invoices. The State then initiates the budget relief process that selects some claims for payment and leaves others in an accounts payable status. Due to the budget relief process, some claims will remain in an AP status. The State determines the provider types that will be paid each week, allowing the State to stay within its budget. Most claims will stay in an AP status for three to four weeks depending on the claim volumes and the State's budgeted expenditures.

Following the budget relief runs, the Flexi Export process is initiated to prepare a check file to be processed by the State. Once the State finishes the payment cycle, the Pay Resolve process is run to update the Health PAS claims into Paid, Denied, or Reversed status.

Claims Process Overview

Claims Input Process

There are two Medicaid claim types (Paper and Electronic).

1. Hard Copy/Paper Claims

   Paper claims are estimated to be 10% of the total number of claims received by Molina. Paper claims are received via mail. The claims are sorted per claim type and screened by mailroom personnel. A sorter's cheat sheet is used by mailroom personnel (screeners) to check specified criteria prior to paper claim transactions being processed.

   The screening criteria are as follows:

   - A valid ten-digit provider number must be on the claim form
   - A valid eleven-digit member ID must be on the claim form
   - A valid nine-digit tax ID must be on the claim form.

   Claims that fail any of the above criteria are segregated, scanned and returned to the provider via mail with an accompanying Return to Provider Letter. Paper claims that are not rejected are also scanned by Molina using Object Assisted Date Entry System. Next, claims are assigned an Interchange Control Number (ICN) that is composed of the Julian date, batch number, and document number which is used to track the claim throughout the process.

   Outside of the mailroom screening, the Quality Assurance (QA) team performs quality assurance testing on 20 claims per claim type per screener in order to check the compliance of the screening process as it relates to paper claims. Findings or errors within this process are reported to Molina Claims Processing management and the screeners are provided with further training.

The paper claims once scanned are permanently stored on image platters for historical references purposes. After scanning the claims are put into batches. A majority of the paper claims, once checked and scanned by Molina, are then sent to a third-party vendor, DataScan, where they are keyed by the vendor to the electronic X12N format. The X12N is a specific billing format defined by the government. Once converted, Molina receives a zip file on a shared server from DataScan. The now electronic claims go through the core system edits (discussed below), and the claims are then processed by Molina.

2. Electronic/EDI Claims

Electronic claims are estimated to be 90% of the total amount of claims received by Molina. Since electronic claims are not imaged, they do not receive an ICN number used for tracking purposes, but are assigned a unique Claim ID. The Claim ID is attached to the claim once it is entered into the Claims module of Health PAS. This module maintains the provider and member information and is mainly used for the adjudication and retrieval of claims.

Preprocessor edits are set up outside of Health PAS to screen electronic claims based upon WV Medicaid rules with regards to format and length of trading partner ID, provider ID, member ID, diagnosis codes, procedure codes, etc. Claims that are rejected by a preprocessor edit will be rejected to the provider on a Business Rejection Report (BRR) and will not be processed in the system. Rejection responses on invalid electronic claims are automatically sent to providers or clearing houses based on the method submitted.

Electronic claims can be received through the following methods:

1. **Value-added Networks**: Direct lines from two traditional clearinghouses to facilitate EDI.

2. **Upload**: Partners/Providers upload preformatted X12N claims through the WV MMIS web portal. The partners/providers must be enrolled and provided with an ID and password prior to submitting claims electronically.

3. **Direct-Data Entry**: Claim forms are entered through the WV MMIS web portal by enrolled partners/providers, which are converted to X12N format after they are entered.

4. **Crossovers**: X12N formatted claims are transferred directly from Medicaid intermediaries for evaluation and payment by Molina and are specific to dual eligible members (members who are eligible to receive both Medicaid and Medicare services and benefits).

System edits are also in place to automatically verify Provider Master File data to prevent ineligible providers from submitting claims for payment, based upon the provider's date of service.

Claims Processing

Incoming claims are subject to BMS and Molina-defined edits to validate that the information contained within each claim is complete, accurate and not duplicated prior to the claim being processed. For example: 'Edit 532' prevents duplicate claims from being billed that have already been paid to another provider based on matching values for member, dates of service, service code, pay to, rendering physician and modifier. Once a claim has gone through the editing process by Molina, the claim is issued a status of either PAY, PEND, or DENY. A claim can either be given pended or denied status during the edit process depending upon criteria such as the service code, procedure code and provider or member information listed on the claim. Pended claims are further manually reviewed by the Molina Claims Department and then either denied or approved based upon the desktop instructions' resolutions that have been approved by BMS.

The ability to process claims is restricted to authorized personnel. In addition, access to Health PAS and its respective subsystems is restricted and granted on an individual user basis. Access is further defined by screens and menus, as well as by the ability to add, update and delete production data.

Health PAS automatically uses the Provider Master File data to prevent ineligible providers from submitting claims for payment, based upon the provider's participation status. Within Health PAS, 'Edit 101' checks the claims for any providers without an active provider contract for the date of service to determine if the provider is eligible. In addition, Health PAS automatically checks the Recipient/Member Master File data to prevent claims for ineligible recipients from being paid, based upon the recipients' eligible dates of service. 'Edit 201' corresponds to this control, as it prevents ineligible members with no enrollment segment for the date of service from being paid. In essence, Edit 201 does not allow claims to be paid to ineligible members.

Once claims are processed, the status (i.e., pay, deny, pend) of the claim determines the next step. For instance, if the claim is pended it is investigated for payment.

Claims Adjudication

Claims are adjudicated based upon a series of system edits. Claims that fail an edit are either pended or automatically denied. There are approximately 300 system edits available, 20 of which are pended edits used within the adjudication process to verify that the correct requirements are present prior to claims being paid. Pended claims can be released or overridden only by authorized Claims Resolution Specialists. Individuals belonging to the Claims Supervisor, Claims Manager or Claims Specialist 1 or Claims Specialist 2 groups have the ability to release or override pended claims.

Clean Claims (**Note**: the term "clean claim" is used by Molina) are required to be adjudicated within 15 days after they have been captured within Health PAS. However, adjudication may take longer than 15 days in cases where a claim is pended as a result of system edits and could not be resolved immediately. Claims that cannot be adjudicated within that time period (i.e., Pended claim) are reported, tracked and processed by the Claims personnel. Molina must adjudicate Pended claims ten days after a pending/problem claim has been identified.

Once a claim is ready for adjudication, Health PAS automatically calculates the price based upon the contract associated with the Provider Master File. Pricing information is stored in various places within Health PAS; however, the Fee Table within the Fee Schedule module is the main pricing table that contains the prices for corresponding provider procedure codes. The contract term that is chosen points the system to the correct fee schedule to use for a specific line/claim.

In instances where a claim must be manually priced, as there is no procedural code defined within the pricing structure to process the correct payment, manual pricing criteria are dictated by the State and are communicated to Claims personnel via Desktop Procedures. The Procedures are written by the State and are used as instruction manuals that provide manual pricing guidance to claims personnel depending upon the claim type.

Claims Payment

The Financial Analysts receive the claims that are ready for payment once the adjudication cycle is complete. Claim payments are calculated in QNXT, which calculates the pricing based upon the Master File Maintenance data.

The Claims Payment cycle is run once every week on Friday. The same payment process is executed for emergency pay runs that occur per the State's request Monday through Thursday. Emergency pay runs are rare and occur when the State may need to make emergency payment(s) to a provider or a provider type. Claims that would be part of an emergency pay run go through the same process as other claims; however, the process is expedited to accommodate the needs of the State.

The claims received by the Financial Analysts go through the Fee-For-Service process, where the fees are applied to the services billed. The Financial Analysts assign a "Pay" status to the claim, which creates a QNXT payment record and changes the claim to "Wait-XYZ" status;

indicating that the claims are finalized for payment and cannot be modified at this point. Adjudication process changes the claim from OPEN to PAY, DENY, or PEND based on the edits. The fee for service process changes the claims to a WAIT status.

The file containing provider updates and new claims to be paid is then exported from QNXT into Flexi. Flexi is an Accounts Payable system owned and maintained by the State, which is mainly used by the State to create budget relief files that show record of what needs to be paid. This payment file is created by running an SQL Server Data Transformation Services (DTS) job entitled Flexi Claims/Prov Import. The DTS jobs are built-in packages that only Molina executes. Molina personnel receive an automated confirmation e-mail verifying that the import has been completed successfully. Molina Operations Team runs reconciliation reports to verify that the necessary claims were loaded into Flexi and if any claims failed to import, then the Financial Manager may elect to run the import process again. Molina personnel generate the Flexi financial reports, specifically the AP Net Aging Report, which lists the payables and receivables specific to each provider. The AP Net Aging Report is sent to the State on Friday morning and the State's CFO office processes payments via the Flexi software, verbally notifying Molina via telephone upon completion via email.

Another SQL Server DTS job, Flexi Prelim Resolve, is then run to update QNXT with the payment data to indicate which claims were paid, denied, or reversed and loads the Remittance table. SQL scripts are run to verify that the payment data from the Flexi pay run was successfully imported back into QNXT and that the Remittance table is balanced. In order to verify that the payment cycle ran and the claims-related transactions were processed accurately and timely, the Financial Analysts utilize a Remittance Reconciliation Report to determine if what was placed into QNXT agrees with what was paid in Flexi. The report is sent to Molina and State personnel via e-mail on the following Saturday and lists any discrepancies noted within QNXT and Flexi synchronization in addition to the details of the synchronization.

In order to verify the amount of the payment checks provided by Molina to the State Auditor to process and cut, SQL scripts are also run to verify that no mathematical errors are present. Another DTS job, Flexi Payfile Export, is then manually run to generate the check payfile and place on the File Transfer Agent server located in the Albuquerque, New Mexico Data Center. Upon job completion, an e-mail containing the payfile batch totals is automatically sent to the State and Molina Operations Management. This indicates that the payment process is completed.

Claims that are rejected from payment due to erroneous or missing data, such as the provider does not have a vendor code, are accumulated within a weekly Failed Claims Report. This report is reviewed by the Molina Finance Adjustment team which works to resolve these failed claims with the help of other Molina departments and the State. The Failed Claims Report, Claims Payment Report, as well as other reports required by the State, are accessible to the State via the Cypress Reporting package which allows for proper change and access management by Molina.

Section IV. Control Objectives, Controls, Tests and Results of Tests

Tests Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of our testing of the controls specified by Molina we considered the aspects of Molina's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Control Objectives, Controls Specified and Tests Performed

Molina has specified its control objectives and identified its controls to achieve these control objectives. The service auditor has determined the nature, timing and extent of testing to be performed. Any exceptions noted from the testing procedures considered relevant to user auditors have been documented within the testing matrices.

Information Systems Control Objectives

Application Development and Systems Software Changes

Control Objective 1: Controls provide reasonable assurance that changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
1.1	Policies and procedures on requesting, approving, developing, testing and implementing application changes are documented in WV Health PAS Configuration Management Plan and Production Change Control policies and procedures.	Inspected the policies and procedures on requesting, approving, developing, testing and implementing, and noted that these are included in the WV Health PAS Configuration Management Plan and Network Operating Center policies and procedures.	No deviations noted.
1.2	Operating system, database and Health PAS application software development and maintenance activities are conducted in response to BMS-initiated modifications or as a result of internal Molina WV MMIS-initiated change requests. All modifications must be: • Requested within Clear Quest • Documented and tested or reviewed for quality assurance (QA) • Authorized by Molina management	Examined a sample of operating system, database and Health PAS application software changes, and determined that the changes were appropriately authorized, tested/reviewed for QA, reviewed and approved before being migrated into the production environment.	No deviations noted.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
1.3	Programmers, system analysts, and/or end users perform testing on changes to application software. Test results are provided to the appropriate application manager for review and approval prior to the implementation of each change.	Examined a sample of operating system, database and Health PAS application software changes, and noted that the changes were appropriately authorized, tested, reviewed and approved before being migrated into the production environment.	No deviations noted.
1.4	Production change request status reports are reviewed Monday – Friday on the daily review calls.	Examined a sample daily change management meeting report and determined that production change requests were categorized.	No deviations noted.
1.5	Only authorized personnel are allowed to promote changes within the clear case source code management tool into the Health PAS production environment.	Inspected system user profiles for those that are authorized to move changes from the clear case software management tool into test and production environments, noting that access is limited only to designated Network Operating Center personnel.	No deviations noted.

Logical Access

Control Objective 2: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
2.1	Access to Health PAS system is granted via single sign-on authentication through the Citrix application, which requires users to enter a valid username and password. Users are required to change their password on a periodic basis, and password must be at least eight characters in length.	Determined through online observation that the system requires a valid username and password upon login to the network. Inspected the password parameters in place for the Windows active directory environment for reasonableness including password expiration and complexity.	**Deviation noted:** In a population of five (5) settings, two (2) password settings do not comply with the Company's password policy. The mitigating three (3) settings in place were tested and in compliance with the Company password policy. **Management Response:** Password settings while not in direct compliance with the Company password policy have been implemented to include password complexity, minimum length and password expiration to mitigate the risk of unauthorized access to the system.
2.2	Only approved requests supported by Security Access Request Forms/RQMS tickets are granted access to the Health PAS system. This form must include the signature of the Account Manager or the delegated Access Coordinator.	For a sample of new users, consisting of Molina personnel added to Health PAS, inspected the related supporting Security Access Request Form/RQMS ticket, noting that the request had been approved and that the roles assigned to the user were appropriate.	No deviations noted.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
2.3	The Network Administrator updates individual access profiles and terminates access of users who leave the organization.	For a sample of terminated employees, observed user accounts online to ascertain whether Health PAS system access had been removed or disabled.	**Deviations noted:** Seven of in all terminated users tested had an active QNXT account and two accounts were not disabled timely, however access was not used post termination. **Management Response:** Management has reviewed this access and determined access was not used inappropriately during the period.
2.4	Powerful roles within the Health PAS application are granted on a business-need basis only and restricted to authorized personnel based on job responsibility.	Inspected the users granted with System Administrator, User Security, and Super-User roles in Health PAS and confirmed that their access was consistent with job responsibilities.	No deviations noted.
2.5	Powerful groups in the Windows active directory environment are restricted to authorized IT personnel only.	Inspected a system-generated listing of members within the Domain and Local Admin groups, noted that no end-users belong to this group.	No deviations noted.
2.6	Access to the SQL Database is limited to authorized programs and Database Administrators only.	Inspected a system-generated listing of members within the SQL Database Administrators group for reasonableness and noted that no end-users belong to this group.	No deviations noted.
2.7	Logical security audits are performed on a periodic basis to review appropriateness of users' access to the Health PAS application	Inspected a sample of the security audit reports and noted that exceptions identified during the audit were investigated and corrected, as necessary.	No deviations noted.

Physical Access

Control Objective 3: Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized and appropriate personnel.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
Molina Charleston, WV Facility			
3.1	Physical access to the Molina Charleston Medicaid facility is controlled through magnetic key cards. An e-mail requesting the activation of card is sent by the office manager to the IT Department of WV American Water Company (third party and building owner) in order to activate a key card in the system. Physical access to the facility is removed for terminated employees.	For a sample of employees with access to the Molina Charleston Medicaid facility, determined that a request for activation was made and access is appropriate based on the employees' employment status.	No deviations noted.
3.2	Visitors to the facility must sign in and wear a visitor's badge.	Observed that visitors are required to sign in upon entering the facility and are given a visitor's badge while they are present on site.	No deviations noted.
3.3	Unassigned key cards are stored in a locked cabinet and only the office manager has access to it.	For a sample of unassigned key cards, determined that they are kept in a locked cabinet and monitored by the office manager.	No deviations noted.
3.4	Physical access to the Molina Charleston, WV computer room is provided to authorized IT individuals only.	Inspected a system-generated listing of access to the Charleston, WV computer room, and determined that only IT personnel with appropriate job responsibilities are granted access.	No deviations noted.

Job Scheduling

Control Objective 4: Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
4.1	All production jobs are maintained within the WV Interfaces Runbook, which is used to define start times, discrepancies and other criteria that control the overall execution and monitoring of production jobs.	Inspected the Interfaces Runbook and noted that schedules of job run and personnel responsible are defined.	No deviations noted.
4.2	A limited number of Computer Operations personnel have the ability to add, change, and/or delete production/interfaces jobs.	Inspected the list of individuals with access to add, change, and/or delete production jobs and noted that access is consistent with job responsibilities.	No deviations noted.
4.3	A Schedule Status report is generated on a daily basis, which is completed by Computer Operations, listing the status of all production jobs run. This report is distributed to management for review and resolution.	Inspected a sample of Daily Job Schedule Status Reports and noted that reports were generated, including completion status of jobs, and were distributed to management.	No deviations noted.

Application Processing Control Objectives

File Maintenance – Master File Data

Control Objective 5: Controls provide reasonable assurance that master file data (i.e., recipient, provider, reference, and claims) used in WV MMIS system processing is authorized, complete, and valid, and the correct versions are used in production processing.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
5.1	A formal Provider Enrollment Tracking System ("PROCESS MANAGER") manual and Provider Enrollment Procedure manual are in place.	Inspected the formal PROCESS MANAGER manual and Provider Enrollment Procedure manual.	No deviations noted.
5.2	Access to the Provider Module is restricted based upon view or modify rights. Only required job roles are granted the rights to modify the Provider Module, all other employees have view only capabilities.	Inspected a listing of individuals who have access to the Provider module and determined that they are current Molina employees and their access rights are consistent with their job responsibilities.	No deviations noted.
5.3	Provider enrollment documents are required in order to create a new provider record within the system. Provider enrollment personnel utilize criteria sheets to verify the criteria required for enrollment per provider type. Applications that do not meet the criteria are returned to the provider. Provider enrollment document images are stored within the Process Manager system for future reference and retrieval purposes. Approval for new providers is communicated to the Provider group by the Provider Relations group.	For a sample of providers enrolled during the period, determined that enrollment documents were complete based on the criteria per provider type.	No deviations noted.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
5.4	Procedure code updates are discussed and approved by the State before being implemented into production.	For a sample of procedure code updates, determined that the defined change management process was followed and included approval by the State.	No deviations noted.
5.5	The ability to update member records is restricted to personnel based on job responsibility.	Inspected a listing of individuals who have the ability to update member records and determined that they were current Molina employees and their access rights were consistent with their job responsibilities.	No deviations noted.
5.6	On a daily basis, Member Interface Analysis ("MIA") Reconciliation Reports are created to reconcile member records in RAPIDS/FACTS to what is loaded into Health PAS.	For a sample of days, inspected the MIA Reconciliation Reports, including successful upload of member records into Health PAS.	No deviations noted.
5.7	Molina monitors the variance rate of the information within the RAPIDS reconciliation and ensures that it is within the target floor of 2% and ceiling of 4% based upon the average number of active members.	For a sample of months, determined that management monitors the reconciliation reports provided from RAPIDS to ensure that it is within the target floor of 2% and ceiling of 4% based upon the average number of active members.	No deviations noted.
5.8	Quality assurance procedures are performed on a regular basis to verify whether scheduled production jobs, including RAPIDS and FACTS interfaces, are regularly and successfully completed.	For a sample of months, determined through inspection of the Quality Assurance Report Cards, which list the status of production jobs, including RAPIDS and FACTS interfaces, that jobs were completed.	No deviations noted.

Report Distribution

Control Objective 6: Controls provide reasonable assurance that WV MMIS system output is secured and routed to the appropriate user(s).

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
6.1	Access to view reports via the Cypress Reporting package is restricted to authorized persons only.	Inspected a sample of individuals with access to the Cypress Reporting system and determined that they were current Molina/BMS employees and their access rights were appropriate.	No deviations noted.
6.2	Reports are available online via the Cypress Reporting package.	Observed a sample item to validate that WV MMIS reports are available online through the Cypress Reporting system.	No deviations noted.
6.3	Access to create/modify reports within the Cypress Reporting package is restricted to authorized personnel.	Inspected a list of individuals with access to create/modify reports and determined that they were current Molina employees and their access rights were appropriate.	No deviations noted.
6.4	Quality Assurance procedures are performed daily to ensure that EDI reports are generated and available.	Inspected a sample of monthly Quality Assurance Report Cards to validate that daily EDI reports are generated and available.	No deviations noted.

Claims Input

Control Objective 7: Controls provide reasonable assurance that claims are received only from authorized sources.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
7.1	Preprocessor edits are set up in the system to screen claims based on WV Medicaid business rules. Rejection responses on invalid electronic claims are automatically sent to providers or clearing houses.	Performed tests using invalid claim entry data to determine that system edits rejected such invalid claims. Determined through inspection that a rejection response report was generated for the sample invalid claim.	No deviations noted.
7.2	Paper claims are screened in the mailroom to ensure that certain criteria are met before the transactions are processed, for example: • A valid ten-digit provider number must be on the claim form. • A valid 11-digit member ID must be on the claim form. • A valid nine-digit tax ID must be on the claim form. If a paper claim does not meet all of these criteria, the claim is returned to the provider with an accompanying Return to Provider letter.	Observed mailroom imaging and data entry procedures, noting that incomplete paper claims are segregated before being imaged for their return to the provider. Inspected a sample of paper claims that did not meet the criteria and determined that a Return to Provider letter was sent in a timely manner.	No deviations noted.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
7.3	Quality assurance procedures are performed on a regular basis to verify that relevant criteria such as Tax ID, Provider ID, Member ID, amount, etc. are met before claims are imaged.	Determined through inquiry and observation that QA procedures are performed on a regular basis to verify that relevant criteria such as Tax ID, Provider ID, Member ID, amount, etc. are met before claims are imaged.	No deviations noted.
7.4	Paper claims are keyed and submitted for adjudication as a result of the imaging process, after which paper claims are imaged for historical purposes. Images are permanently stored on image platters for historical reference purposes.	Inspected a sample of claims screen prints and confirmed that each paper claim image was retrievable.	No deviations noted.
7.5	Paper and electronic claims are assigned a unique Tracking Control number, which can be used to track the claim throughout its lifecycle.	Inspected a sample of claims screen prints and confirmed that each claim was assigned a unique Tracking Control number.	No deviations noted.
7.6	System edits are in place to automatically verify Provider Master File data to prevent ineligible providers from submitting claims for payment, based upon the provider's participation status.	Inspected a sample of claims and determined that each claim was submitted by a valid provider included within the Provider Master file, noting that the claim was only paid if Provider Status was Active.	No deviations noted.

Claims Processing

Control Objective 8: Controls provide reasonable assurance that claims received are entered in an accurate and timely manner.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
8.1	Claims are subject to BMS-specified and Molina-defined edits and audits to validate that information contained within each claim is complete, accurate and not duplicated.	Inspected the edit configurations in the system including, but not limited to, duplicate claim number and required field edits; determined that the sample edits and audits were activated. Inspected a sample of pended claims and noted that claims that failed the edits are properly identified for resolution.	No deviations noted.
8.2	The ability to process claims is limited to authorized personnel only. Access to Health PAS and its respective subsystems is assigned on an individual user basis.	Inspected user access listing to determine only authorized individuals have access to process claims.	No deviations noted.
8.3	WV MMIS automatically uses Provider Master File data to prevent ineligible providers from submitting claims for payment, based on the provider's participation status.	For a sample of claims, inspected the Provider Master File data noting that the provider was eligible to submit claims as of the date of service for the respective claim.	No deviations noted.
8.4	The WV MMIS automatically reviews Recipient Master File data to prevent claims for ineligible recipients from being paid, based on the recipient's eligible dates of service.	Inspected a sample of screen prints for claims and confirmed that each claim was for a valid member.	No deviations noted.

Claims Adjudication

Control Objective 9: Controls provide reasonable assurance that Medicaid claims are validated and adjudicated in an accurate and timely manner.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
9.1	Claims are adjudicated based on a series of system edits and audits. Claims that failed an edit are either pended or denied.	Performed tests using invalid claim entry data to determine that system edits rejected such invalid claims. Determined through inspection that a rejection response report was generated for the sample invalid claim.	No deviations noted.
9.2	Pended claims due to edits can be released or overridden only by a Claims Supervisor, Claims Manager or Claims Specialist.	Inspected an access listing and corresponding role report of those individuals who hold a Claims Supervisor, Claims Manager, or Claims Specialist position. Obtained confirmation from the Claims Manager that the individuals included on the access listing were appropriate and that their corresponding access was appropriate.	No deviations noted.
9.3	Pended claims are reported, tracked, and processed by the Claims personnel in a timely manner.	Inspected a sample of pended claims and determined that adjudication was performed timely. Inspected screen prints of a sample of claims and determined that each claim, with the exception of the Denied and Reversed claims, was adjudicated within 15 days.	No deviations noted.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
9.4	Health PAS automatically calculates the amount to be paid for each claim based on the information contained within the master file data.	Inspected screen prints of a sample of claims and confirmed that each claim, with the exception of the Denied and Reversed claims, was adjudicated within 15 days. For a sample item, determined that the amount to be paid was commensurate with the information contained within the master file data.	No deviations noted.

Claims Payment

Control Objective 10: Controls provide reasonable assurance that adjudicated claims are paid in an accurate and timely manner.

Item	*Controls Specified by Molina*	*Test Performed by Ernst & Young*	*Testing Results*
10.1	Health PAS automatically calculates the amount to be paid for each claim based on the information contained within the master file data.	Inspected screen prints of a sample of claims and determined that the amount paid agreed to the amount adjudicated.	No deviations noted.
10.2	Reconciliation procedures are performed to verify that the payment cycle ran and processed all claims-related transactions accurately and timely.	For a sample reconciliation file generated for the sample payment cycle, determined through inspection that the cycle ran and discrepancies were reviewed and resolved. The claims were paid and agreed to the payment feedback file from DHHS. Inspected a sample of electronic claims and determined that the payment cycle ran and processed all claims-related transactions accurately and timely.	No deviations noted.

Summary of Complementary User Entity Controls

Molina WV MMIS's procedures and processes were designed with the assumption that certain controls would be implemented by the State of West Virginia. In certain situations, the application of specific controls at the State of West Virginia is necessary to achieve the control objectives included in this report.

This section describes additional controls that should be in operation at the State of West Virginia to complement Molina's controls. User auditors should consider whether the following controls have been placed in operation at the State of West Virginia.

1. Molina WV MMIS depends on the timely, accurate and authorized communication from BMS and HIM to its Network Administrator regarding granting, revoking and changing of users' access with respect to individual state users and their respective access capabilities. BMS and HIM should perform regular access reviews for their employees to validate access is appropriate based on a user's job responsibilities. (Applies to Control Objective ("CO") 2.)

2. BMS is responsible for coordinating transmission of the RAPIDS and FACTS files to Molina WV MMIS to update the member master file. (Applies to CO 6.)

3. BMS is responsible for checking of eligibility of members; Molina WV MMIS relies on the information provided by RAPIDS. (Applies to CO 6.)

4. The State of West Virginia BMS has the responsibility to review reports received from WV MMIS, and to notify WV MMIS if report(s) are not received. (Applies to CO 7.)

5. BMS is responsible for the creation and issuance of checks through its treasury management system, to which Molina does not have access. Payment decisions regarding the timing and amount of payments are controlled by BMS. BMS should ensure that the controls over the recording of payment transactions are in place and functioning. (Applies to CO 10.)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: FAR140001

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)

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

Company

Authorized Signature

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012