STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **6**
to
Contract Number **071B1300185**

CONTRACTOR	FIRST DATA GOVERNMENT SOLUTIONS LP
	3975 NW 120th Avenue
	Coral Springs, FL 33065
	Jason Clark
	(513) 207-5265
	jason.clark@fiserv.com
	CV0060377

STATE	Program Manager	Susan Stephens	TREA
		(517) 636-5089	
		Stephens@michigan.gov	
	Contract Administrator	Jennifer May	DTMB
		(517) 242-6664	
		mayj7@michigan.gov	

CONTRACT SUMMARY

CEPAS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 1, 2011	June 30, 2016	5 - 1 Year	June 30, 2020

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☒	2 Months	August 31, 2021

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$6,823,848.00	$0.00	$6,823,848.00

DESCRIPTION

Effective 6/22/2021, this contract is hereby extended for 2 months with a new expiration date of August 31, 2021, with the use of existing funds ($150,000.00). All other terms, conditions, and specifications remain the same. Per DTMB contractor (request/proposal) and agency (request) agreement, DTMB Procurement approval, and State Administrative Board Approval on 6/22/2021.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **5**

to

Contract Number **071B1300185**

CONTRACTOR	
	FIRST DATA GOVERNMENT SOLUTIONS LP
	11311 Cornell Park Drive , Suite 300
	Cincinnati, OH 45242
	Jason Clark
	(513) 489-9599 x184
	jason.clark@firstdata.com
	CV0060377

STATE			
	Program Manager	Susan Stephens	TREA
		(517) 636-5089	
		Stephenss@michigan.gov	
	Contract Administrator	Jennifer May	DTMB
		(517) 242-6664	
		mayj7@michigan.gov	

CONTRACT SUMMARY

CEPAS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 1, 2011	June 30, 2016	5 - 1 Year	June 30, 2020

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	12 months	☐		June 30, 2021

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$6,808,348.00	$15,500.00	$6,823,848.00

DESCRIPTION

Effective 1/20/2021, this contract is hereby increased by $15,500.00, per the attached Statement of Work. All other terms, conditions, specifications, and pricing remain the same. Per Contractor and Agency agreement, and DTMB Procurement approval.

Contract Administrator has been changed to Jennifer May.

First Data is now fiserv.

Michigan CEPAS

End-to-End Encryption White Paper

Submitted by

First Data Government Solutions LP

To

MI CEPAS

Version 1.1

November 19, 2020

Revision History

Revision Date	Version	Notes
10/29/2020	1.0	[JWC] Initial Creation
11/19/2020	1.1	(JWC) Amy K. edits and corrections have been accepted within the document.

STATEMENT OF WORK FOR

Hardware, Software, and Professional Services

This Statement of Work (**SOW**), effective as of the date last written below (**Effective Date**), is attached to, and made a part of, the Agreement dated July 1, 2011 (the **Agreement**), by and between First Data Government Solutions, LP (**FDGS**) and the State of Michigan contract number 071B1300185 ("MI CEPAS"). All terms and conditions contained in the Agreement shall remain in full force and effect and shall apply to the extent applicable to this SOW, except as expressly modified herein. To the extent that the terms and conditions of this SOW are in conflict with the terms and conditions of this Agreement, or any other incorporated item, this SOW shall control relative to the Work Products and/or Services produced hereunder.

This SOW shall define the scope of the services and the deliverables that First Data shall provide to Customer with respect to the building and delivering the following:

- End-to-End Encryption White Paper documented by Fiserv's E2EE Qualified Security Assessor (QSA) for the PayPoint End-to-End Encryption Solution used by MI CEPAS.

The terms of this SOW are limited to the scope of this SOW and shall not be applicable to any other SOWs, which may be executed between the parties.

This SOW consists of this signature page and the following sections:

Project Description

Responsibilities of the Parties

Key Assumptions

Professional Services Requirements

Software Requirements & Specifications

Hardware Requirements & Specifications

Training

Documentation

Maintenance

Project Schedule

Deliverables

Pricing and Payment

Acceptance

Change Management

Key Contact Information

Miscellaneous

IN WITNESS WHEREOF, the duly authorized representatives of the parties hereto have caused this SOW to be duly executed.

First Data Government Solutions, LP By: First Data Merchant Services, LLC Its General Partner	State of Michigan
By: ___________________________________	By: ____________________________
Name: ________________________________	Name:__________________________
Title: __________________________________	Title: ___________________________
Date: _________________________________	Date: ___________________________

1.0 Project Description

MI CEPAS has requested a white paper to formally document the PayPoint end-to-end encryption solution used by the State of Michigan. MI CEPAS's goal of documenting this solution is to validate the end-to-end encryption process being used by the PayPoint Gateway to reduce the MI CEPAS PCI scope.

FDGS will contract with SecureTrust, a division of Trustwave, to perform certain Services under this SOW. By executing this SOW, MI CEPAS is providing its prior written approval, as required by the Agreement, of SecureTrust as an FDGS subcontractor. Furthermore, by executing this SOW, MI CEPAS confirms the following: (1) State of Michigan has reviewed and approved the one time specific to CN 5, modifications made by SecureTrust to the flow down terms as stated in the Addendum between FDGS and SecureTrust, a copy of which is attached hereto as Attachment 1; and (2) CEPAS waives any objection it may have to SecureTrust performing services as a subcontractor to FDGS under this SOW.

Overview of PayPoint End-to-End Encryption Process

- Card is swiped/inserted/tapped or hand keyed at Ingenico device.
- Card data is encrypted on the card reader terminal using the Ingenico security package.
    - The security package in use by the PayPoint end-to-end encryption solution was signed and provided by Ingenico.
    - The Ingenico security package includes the TSYS public key that is used for encryption.
- Encrypted card data is then sent to the Dynamic-link Library (DLL) that resides on the CEPAS point-of-sale (POS) servers.
    - The DLL makes a web service call and transmits the encrypted card data to the PayPoint gateway.
    - PayPoint submits the payment request to TSYS.
    - TSYS sends back response code for the payment request.
    - At no time does the DLL or PayPoint have un-encrypted card data.
- The TSYS response code is sent back to the DLL on the CEPAS POS servers from PayPoint.
- CEPAS POS servers communicate approval or denial back to the Ingenico credit card terminal.

To perform the audit needed to produce the white paper FDGS requires the following:

- Access to CEPAS POS test lab.
- MI CEPAS will be required to install WireShark and FDK Imager in the MI CEPAS test environment so that the software can be utilized by FDGS.
- MI CEPAS will be required to provide a hard drive that will contain imager data from the audit performed by FDGS. FDGS will take the transactions from their testing in the MI CEPAS test environment and will review those transactions in their environment using forensic tools to determine if any card data leakage occurred during transit from the MI CEPAS environment to TSYS.
    - The hard drive used for the testing and validation will not be returned to MI CEPAS.
    - FDGS will store the hard drive for a period of three (3) years in storage at Iron Mountain.
    - After three (3) years the hard drive will be destroyed.

Phase I: Information Gathering (Remote)

As part of this project, FDGS will work with MI CEPAS to gather and analyze information about the PayPoint end-to-end encryption solution. FDGS will conduct interviews with system architects, application developers, database developers, system administrators, quality assurance (QA) or testing personnel and other FDGS / MI CEPAS personnel who may provide relevant details on the application.

FDGS will examine applicable documentation and may request a remote demonstration of application capabilities.

Topics of information gathering include, but are not limited to, the following:

- Description of the application to provide a fundamental understanding of the application to the assessor;
- Application name and version number as well as supported operating systems and any hardware requirements;
- Description of the components that make up the application under review;
- List of any third-party dependencies required by the application as well as a list of development tools used during design, code development and application integration, as applicable;
- Functional design and technical design documentation including description of application’s data handling processes, design schema(s), data logging and error handling behavior;
- Data encryption implementation technique including integrations with any third-party encryption applications;
- Application interface diagrams and documentation illustrating application interaction and data flow exchange with third parties and merchant networks;
- Transaction flow diagram illustrating the application's data processing, inputs, and outputs to and from the application and to and from a merchant's network;
- List of software testing tools that may be required for lab testing, description of software test scripts and software test environment documentation for data processing, as applicable; and
- MI CEPAS implementation documentation including secure application integration procedures and recommendations for application integration into merchant environments.

Phase II: Application Review

The Application Review phase will take place within SecureTrust’s’s testing lab and within MI CEPAS’s testing lab, depending on the nature and required systems for the application undergoing review and on logistical constraints. Due to COVID-19, all testing and analysis will be done remotely by FDGS.By signing this SOW, MI CEPAS consents to and accepts that portions of the Application Review phase will take place within SecureTrust’s, FDGS’s subcontractor, testing lab.

FDGS will gather a thorough understanding of how the application is configured and protected. FDGS may review business functions, administrative and organization capabilities, current functionality and requirements, as well as present and future initiatives. FDGS may examine critical application parameters such as database schema, logging, or error handling behaviors. FDGS may also review or verify written software development processes, relevant configuration data (e.g. network configuration documentation, production and test data), authentication features, change controls, data storage and encryption, audit logging, and remote maintenance features. Functional testing of controls will be conducted as appropriate to determine the overall security posture of the application. FDGS may request additional application details, review of applicable code areas, documentation, or data handling processes, as applicable to determine the PA-DSS eligibility of the application.

Phase III: Reporting & Deliverables

FDGS will develop a report deliverable documenting all findings and recommendations from the assessment. Including:

- If the PayPoint end-to-end encryption application is found not to be eligible for PA-DSS compliance validation, FDGS will provide MI CEPAS with a report that documents the application's existing security posture, allowing FDGS to detail why the PayPoint end-to-end encryption application is not eligible for PA-DSS validation.
- FDGS will conduct a closeout meeting with Client.

2.0 Responsibilities of the Parties

If the responsibilities below are not met, there will be impacts to the cost and schedule for this project, which must be resolved before continuing this project. FDGS will not be held responsible to deliver within the initial project schedule agreed upon, if tasks are not completed within the timeframes specified, or for reasons beyond FDGS's control.

2.1. FDGS will be required to fulfill the responsibilities below.

2.1.1. Establish and maintain contact with MI CEPAS.
2.1.2. Establish communication and escalation plans.
2.1.3. Create a MI CEPAS account in the FDGS Portal.
2.1.4. Define high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
2.1.5. Schedule and conduct kickoff, periodic status and closeout meetings.
2.1.6. Validate the scope of the engagement.
2.1.7. Create and respond to MI CEPAS action items in Compliance Manager within the FDGS Portal.
2.1.8. Interview appropriate organization personnel and collect information from personnel.
2.1.9. Perform evaluation of the application against the PA-DSS eligibility criteria.
2.1.10. Determine application PA-DSS eligibility status.
2.1.11. Produce either a proposal to undergo full PA-DSS validation, or a report that documents the application's existing security posture detailing why the application is not eligible for PA-DSS validation, depending on the status of the application at the time the assessment occurs.
2.1.12. Create, prepare and deliver to MI CEAS a final report documenting all findings and recommendations from the assessment.

2.2. MI CEPAS will be required to fulfill the responsibilities below.

2.2.1. Establish and maintain contact with FDGS.
2.2.2. Establish communication and escalation plans.
2.2.3. Agree to high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
2.2.4. Accurately provide all necessary information including key stakeholders, applicable Client environment information and configuration requirements.

2.2.5. Inform FDGS of all MI CEPAS environment maintenance activity and changes that may impact the service.
2.2.6. Accurately respond to requests from FDGS teams when establishing contact and collection of required information.
2.2.7. Provide complete and accurate details of the relevant environment and other business operations information.
2.2.8. Make available resources capable of participating in compliance assessment activities.
2.2.9. Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.

3.0 Key Assumptions

- All work for this project will be completed remotely.
- All security and feature updates for the portal software will be included in major version release upgrades.
- FDGS's Application Security Review uses the eligibility criteria of the current PA-DSS version applicable at the time of the service start date.
- The assessment period will begin on the first day of the project engagement. The timeline and end dates will be determined during the kickoff call. MI CEPAS must submit all evidence and provide requested information no later than forty-five (45) business days prior to the end of the assessment period.
- FDGS may request evidence from MI CEPAS's systems and processes as required to prove compliance with any specific requirements. MI CEPAS agrees to provide all such evidence in a timely manner.
- FDGS is not responsible for defining systems in scope or inaccurate information provided by MI CEPAS.
- FDGS retains the right to reject or accept MI CEPAS comments based on the facts and circumstances of the assessment.
- FDGS will perform the service in the English language.
- FDGS will not create or modify MI CEPAS documentation as part of the Application Security Review.
- FDGS will not provide remediation services as part of the Application Security Review.
- FDGS will not offer any legal guidance or counseling.
- The quality and accuracy of the Application Security Review is dependent on MI CEPAS's provision of accurate information and access to MI CEPAS systems and resources to FDGS.

4.0 Professional Services Requirements

- FDGS will assign the necessary resources, including a Project Manager in order to complete these services within the agreed upon project schedule.

5.0 Software Requirements & Specifications

- MI CEPAS will be required to install software within its test environment to support this project. The software needed includes, but may not be limited to, WireShark and FDK Imager.

6.0 Hardware Requirements & Specifications

- MI CEPAS will need to provide a hard drive that will contain imager data from the audit performed by FDGS. FDGS will take the transactions from their testing in the MI CEPAS test environment and will review those transactions in their environment using forensic tools to ensure no card data leakage occurred during transit from the MI CEPAS environment to TSYS.

- The hard drive used for the testing and validation will not be returned to MI CEPAS.
- FDGS will store the hard drive for a period of three (3) years in storage at Iron Mountain.
- After three (3) years the hard drive will be destroyed.

7.0 Training

Not Applicable

8.0 Documentation

White Paper of the PayPoint end-to-end encryption process will be provided by FDGS at the completion of the project.

9.0 Maintenance

Not Applicable

10.0 Project Schedule

A project schedule will be developed and delivered to MI CEPAS after the intial project kickoff meeting.

11.0 Milestones

The milestones for this SOW are:

11.1 Project Schedule

11.2 Completed PayPoint end-to-end encryption white paper.

12.0 Pricing and Payment

Payment for change orders is made according to milestones achieved in delivery of the change order. (Definition of the milestones is given in the section on Acceptance, below.)

Product Description	Amount
PA-DSS Application Security Review and White Paper	$15,500.00

Milestone	Percentage Due
Project Schedule	50%
Completed PA-DSS Application Security Review and White Paper	50%
Total	**100%**

a) The pricing of this SOW is valid until January 31, 2020. This SOW must be signed by both parties before January 31, 2020.

b) Prices are quoted in US dollars.

As milestones are achieved and acknowledged by MI CEPAS the corresponding milestone billing(s) will be included in the next regular monthly invoice to MI CEPAS. If MI CEPAS should terminate this SOW for any reason (lack of funding, etc.) prior to Cutover, MI CEPAS agrees to pay FDGS for that portion of the work that has been performed up to the date of termination.

Optional – White Paper Annual Review

As an optional service, FDGS can perform an annual review of the PayPoint end-to-end encryption process to ensure that the application still meets the PA-DSS standards.

Product Description	Amount
PA-DSS Application Security Review and White Paper	$2,775.00

13.0 Acceptance

13.1 Written acceptance or rejection of the Deliverables must be received within the timeline reflected on the project schedule. Acceptance shall be provided when the Deliverables meet all contractual requirements for that specific Deliverable. If Acceptance is not received within five (5) business days of the date in which the Deliverable was presented to Client, and no issue or concern has been expressed and delivered in writing to FDGS, the Deliverable will be considered Accepted and will be invoiced.

13.2 If the Client does not timely perform its work in the project plan and causes delay in Acceptance of the Deliverables per the agreed upon schedule, the price, schedule, and implementation date will be impacted. Client will have five (5) business days in which to accept revised schedule and additional cost. Should that acceptance not be received, the work detailed in this SOW and any dependent or affected components will be placed on hold until acceptance is received. Should the project be placed on hold Client will be responsible for any payment associated with Deliverables that have been formally Accepted.

13.3 If both parties agree that the issue and/or concern delaying the formal Acceptance of a Deliverable and/or milestone cannot be remedied, either party may decide to terminate the SOW. All previously Accepted Deliverables and/or milestones shall be due and payable.

13.4 Once considered ‘accepted’, the work enters into formal change control; that is, subsequent changes to the work product must undergo review as described in Section 14.

14.0 Change Management

14.1. It may become necessary to amend this SOW for reasons including, but not limited to, the following:

14.1.1. MI CEPAS/FDGS requests changes to the scope of work and/or specifications for the services.

14.1.2. MI CEPAS/FDGS requests changes to the Project Schedule.

14.1.3. Non-availability of resources, which are beyond either party's control.

14.1.4. Material changes to assumptions outlined in this SOW.

14.2. In the event either party desires to change this SOW, the following procedures will apply:

14.2.1. The party requesting the change will deliver a Change Request document (to the other party). The Change Request will describe the nature of the change; the reason for the change and the effect the change will have on the scope of work, which may include changes to the Deliverables and the schedule.

14.2.2. The party receiving the Change Request will review it and offer any input or acceptance within five (5) business days. The parties shall use good faith to resolve any issues and arrive at an executable Change Request as soon as possible.

14.2.3 Upon execution of the Change Request, said Change Request will be incorporated into, and made a part of this SOW.

14.2.4 No Change Requests will be effective until signed by both parties.

14.3. Whenever there is a conflict between the terms and conditions set forth in a fully executed Change Request and those set forth in the original SOW, or previous fully executed Change Request, the terms and conditions of the most recent fully executed Change Request shall prevail.

15.0 Key Contact Information

Amy Kelso

CEPAS Program Manager
Dept. of Treasury - Receipts Processing Division
Phone (517) 636-5372
Fax (517) 636-5401
Email: kelsoa@michigan.gov

Jason Clark

Sr. Account Executive
First Data Government Solutions
Phone: (513) 207-5265
Email: jason.clark@fiserv.com

16.0 Miscellaneous

Limitation of Liability: (a) In no event shall FDGS have any liability or responsibility for any indirect, incidental, punitive, exemplary, special or consequential damages (including, but not limited to, damages arising from loss of profits or data), even if advised of the possibility of such damages; (b) To the maximum extent permitted by applicable law, FIRST DATA' liability for damages hereunder shall not exceed the amount of fees paid under this SOW.

Please contact Jason Clark with any questions or concerns regarding this proposal.

Attachment 1

ADDENDUM to SECURETRUST™ ORDER CONFIRMATION

This Addendum to SecureTrust™ Order Confirmation (**Addendum**) is hereby attached and incorporated into that certain Order Confirmation dated December 31, 2020 and entered between First Data Corporation (**First Data**) and SecureTrust™, a division of Trustwave® (**SecureTrust**).

WHEREAS, First Data has requested SecureTrust to perform certain services for the State of Michigan as a subcontractor to First Data's subsidiary First Data Government Solutions, LP, and SecureTrust has agreed to perform those services; and

WHEREAS, First Data's contract with the State of Michigan requires certain terms to flow down to any subcontractors used in the performance of the services thereunder;

WHEREAS, references to Contractor below shall be to SecureTrust in its capacity as a subcontractor to First Data and any deliverables required to be given to the State of Michigan shall be given to First Data for further forwarding or sublicense to the State as applicable and upon request; and

WHEREAS, this Addendum sets forth those certain flow down terms related to the performance of services under the Order Confirmation.

NOW, THEREFORE, the parties hereby agree to incorporate the following terms into the terms of the MSA, as defined in the Order Confirmation; in the event of a conflict between the terms of the MSA and this Addendum, this Addendum shall govern.

*Defined terms used in the provisions below are defined in the State of Michigan contract and shall have the definition attributed to it in the State of Michigan contract.

SecureTrust agrees the following flow down terms shall apply to the Order Confirmation services to be performed for First Data for the benefit of the State of Michigan.

2.31 MEDIA RELEASES

News releases (including promotional literature and commercial advertisements) pertaining to the RFP and Contract or project to which it relates shall not be made without prior written State approval, and then only in accordance with the explicit written instructions from the State. No results of the activities associated with the RFP and Contract are to be released without prior written approval of the State and then only to persons designated.

2.060 Contract Management

2.61 CONTRACTOR PERSONNEL QUALIFICATIONS

All persons assigned by Contractor to the performance of Services under this Contract must be employees of Contractor or its majority-owned (directly or indirectly, at any tier) subsidiaries (or a State-approved Subcontractor) and must be fully qualified to perform the work assigned to them. Contractor must include a similar provision in any subcontract entered into with a Subcontractor. For the purposes of this Contract, independent contractors engaged by Contractor solely in a staff augmentation role must be treated by the State as if they were employees of Contractor for this Contract only; however, the State understands that the relationship between Contractor and Subcontractor is an independent contractor relationship.

2.62 CONTRACTOR KEY PERSONNEL

(a) The Contractor must provide the Contract Compliance Inspector with the names of the Key Personnel.

(b) Key Personnel must be dedicated as defined in the Statement of Work to the Project.

(c) The State will have the right to approve in writing the initial assignment of Key Personnel, as well as any proposed Key Personnel replacements. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, will introduce the individual to the appropriate State representatives, and will provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(d) When practicable and not prohibited by law, Contractor will notify the State at least 30 days prior to any changes in Key Personnel. Contractor will not be required to provide prior notice of changes in Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation or for cause termination of the Key Personnel's employment, but the Contractor will provide notice to the State as soon as practicable once it becomes aware of a change. The Contractor with the State must review any Key Personnel replacements, and appropriate transition planning will be established.

2.63 RE-ASSIGNMENT OF PERSONNEL AT THE STATE'S REQUEST

The State reserves the right to require the removal from the Project of Contractor personnel found by the State, in the exercise of reasonable judgment and after consultation with the Contractor, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request.

Additionally, the State's request must be based on legitimate, good faith reasons. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed personnel, the State agrees to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any incident with removed personnel results in delay not reasonably anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Service will not be counted for a time as agreed to by the parties.

2.64 CONTRACTOR PERSONNEL LOCATION

All staff assigned by Contractor to work on the Contract will perform their duties either primarily at Contractor's offices and facilities or at State facilities. Without limiting the generality of the foregoing, Key Personnel will, at a minimum, spend at least the amount of time on-site at State facilities as indicated in the applicable Statement of Work. Subject to availability, selected Contractor personnel may be assigned office space to be shared with State personnel.

2.65 CONTRACTOR IDENTIFICATION

Contractor employees must be clearly identifiable while on State property by wearing a State-issued badge, as required. Contractor employees are required to clearly identify themselves and the company they work for whenever making contact with State personnel by telephone or other means.

2.66 COOPERATION WITH THIRD PARTIES

Contractor agrees to cause its personnel and the personnel of any Subcontractors to cooperate with the State and its agents and other contractors including the State's Quality Assurance personnel. As reasonably requested by the State in writing, the Contractor will provide to the State's agents and other contractors reasonable access to Contractor's Project personnel to the extent the access relates to activities specifically associated with this Contract and will not interfere or jeopardize the safety or operation of the Contractor. The State acknowledges that Contractor's time schedule for the Contract is very specific and agrees not to unnecessarily or unreasonably interfere with, delay or otherwise impeded Contractor's performance under this Contract with the requests for access.

2.67 CONTRACT MANAGEMENT RESPONSIBILITIES

Contractor shall be responsible for all acts and omissions of its employees, as well as the acts and omissions of any other personnel furnished by Contractor to perform the Services. Contractor shall have overall responsibility for managing and successfully performing and completing the Services/Deliverables, subject to the overall direction and supervision of the State and with the participation and support of the State as specified in this Contract. Contractor's duties will include monitoring and reporting the State's performance of its participation and support responsibilities (as well as Contractor's own responsibilities) and providing timely notice to the State in Contractor's reasonable opinion if the State's failure to perform its responsibilities in accordance with the Project Plan is likely to delay the timely achievement of any Contract tasks.

The Contractor will provide the Services/Deliverables directly or through its affiliates, subsidiaries, subcontractors or resellers. Regardless of the entity providing the Service/Deliverable, the Contractor will act as a single point of contact coordinating these entities to meet the State's need for Services/Deliverables.

Nothing in this Contract, however, shall be construed to authorize or require any party to violate any applicable law or regulation in its performance of this Contract.

2.68 CONTRACTOR RETURN OF STATE EQUIPMENT/RESOURCES

The Contractor must return to the State any State-furnished equipment, facilities and other resources when no longer required for the Contract in the same condition as when provided by the State, reasonable wear and tear excepted.

2.100 Confidentiality

2.101 CONFIDENTIALITY

Contractor and the State each acknowledge that the other possesses and will continue to possess confidential information that has been developed or received by it. As used in this Section, "Confidential Information" of Contractor must mean all non-public proprietary information of Contractor (other than Confidential Information of the State as defined below), which is marked confidential, restricted, proprietary, or with a similar designation. "Confidential Information" of the State must mean any information which is retained in confidence by the State (or otherwise required to be held in confidence by the State under applicable federal, state and local laws and regulations) or which, in the case of tangible materials provided to Contractor by the State under its performance under this Contract, is marked as confidential, proprietary or with a similar designation by the State. "Confidential Information" excludes any information (including this Contract) that is publicly available under the Michigan FOIA.

2.102 PROTECTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION

The State and Contractor will each use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication or dissemination of its own confidential information of like character, but in no event less than reasonable care. Neither Contractor nor the State will (i) make any use of the Confidential Information of the other except as contemplated by this Contract, (ii) acquire any right in or assert any lien against the Confidential Information of the other, or (iii) if requested to do so, refuse for any reason to promptly return the other party's Confidential Information to the other party. Each party will limit disclosure of the other party's Confidential Information to employees and Subcontractors who must have access to fulfill the purposes of this Contract. Disclosure to, and use by, a Subcontractor is permissible where (A) use of a Subcontractor is authorized under this Contract, (B) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Subcontractor's scope of responsibility, and (C) Contractor obligates the Subcontractor in a written Contract to maintain the State's Confidential Information in confidence. Any employee of Contractor and any Subcontractor having access or continued access to the State's Confidential Information shall be subject to a written confidentiality agreement that shall be no less restrictive than the provisions of this section.

Promptly upon termination or cancellation of the Contract for any reason and receipt of a written request from the State, Contractor must certify to the State that Contractor has destroyed all State Confidential Information in the data base and disposed of all other State information in accordance with Contractor's record retention policies and consistent with Payment Card Industry requirements.

2.103 EXCLUSIONS

Notwithstanding the foregoing, the provisions in this Section will not apply to any particular information which the State or Contractor can demonstrate (i) was, at the time of disclosure to it, in the public domain; (ii) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party; (iii) was in the possession of the receiving party at the time of disclosure to it without an obligation of confidentiality; (iv) was received after disclosure to it from a third party who had a lawful right to disclose the information to it without any obligation to restrict its further disclosure; or (v) was independently developed by the receiving party without reference to Confidential Information of the furnishing party. Further, the provisions of this Section will not apply to any particular Confidential Information to the extent the receiving party is required by law to disclose the Confidential Information, provided that the receiving party (i) promptly provides the furnishing party with notice of the legal request, and (ii) assists the furnishing party in resisting or limiting the scope of the disclosure as reasonably requested by the furnishing party.

2.104 NO IMPLIED RIGHTS

Nothing contained in this Section must be construed as obligating a party to disclose any particular Confidential Information to the other party, or as granting to or conferring on a party, expressly or impliedly, any right or license to the Confidential Information of the other party.

2.105 RESPECTIVE OBLIGATIONS

The parties' respective obligations under this Section must survive the termination or expiration of this Contract for any reason.

2.110 Records and Inspections

2.111 INSPECTION OF WORK PERFORMED

Intentionally omitted.

2.112 EXAMINATION OF RECORDS

For five years after the Contractor provides any work under this Contract (the "Audit Period"), the State may, at its own expense, audit the Contractor's reasonable records related to any payments or service level agreements for the products or Services provided under this Agreement; provided that the State gives Contractor at least thirty (30) days prior written notice and does not conduct such audits more frequently than once in any one (1) year period. Such audit shall be conducted remotely during normal business hours at the State's own expense in a manner that does not disrupt Contractor's business. The State shall abide by all Contractor work rules and security regulations while conducting such audit. The State does not have the right to review any information deemed confidential by the Contractor to the extent access would require the confidential information to become publicly available.

2.113 RETENTION OF RECORDS

Contractor must maintain reasonable records pertaining to the products and Services provided to the State under this Contract for the periods required by Contractor's records retention policies

2.114 AUDIT RESOLUTION

If necessary, the Contractor and the State will meet to review each audit report promptly after issuance. The Contractor will respond to each audit report in writing within 30 days from receipt of the report, unless a shorter response time is specified in the report. The Contractor and the State agree to address issues that the parties mutually agree pose a concern or to address any issues which are identified as a material breach that were identified as a result of the audit.

2.115 ERRORS

If the audit demonstrates any overpayments of more than five percent (5%) by the State, then the amount in error must be reflected as a credit or debit on the next invoice and in subsequent invoices until the amount is paid or refunded in full. However, a credit or debit may not be carried for more than four invoices. If a balance remains after four invoices, then the remaining amount will be due as a payment or refund within 45 days of the last quarterly invoice that the balance appeared on or termination of the contract, whichever is earlier.

2.120 Warranties

2.121 WARRANTIES AND REPRESENTATIONS

The Contractor represents and warrants:

(a) It is capable in all respects of fulfilling and must fulfill all of its obligations under this Contract. The performance of all obligations under this Contract must be provided in a timely, professional, and workman-like manner and must meet the performance and operational standards required under this Contract.

(b) The Contract Appendices, Attachments and Exhibits identify the equipment and software and services necessary for the Deliverable(s) to perform and Services to operate in compliance with the Contract's requirements and other standards of performance.

(c) It is the lawful owner or licensee of any Deliverable licensed or sold to the State by Contractor or developed by Contractor under this Contract, and Contractor has all of the rights necessary to convey to the State the ownership rights or licensed use, as applicable, of any and all Deliverables.

(d) If, under this Contract, Contractor procures any equipment, software or other Deliverable for the State (including equipment, software and other Deliverables manufactured, re-marketed or otherwise sold by Contractor under Contractor's name), then in addition to Contractor's other responsibilities with respect to the items in this Contract, Contractor must assign or otherwise transfer to the State or its designees, or afford the State the benefits of, any manufacturer's warranty for the Deliverable.

(e) The contract signatory has the power and authority, including any necessary corporate authorizations, necessary to enter into this Contract, on behalf of Contractor.

(f) It is qualified and registered to transact business in all locations where required.

(g) Neither the Contractor nor any Affiliates, nor any employee of either, has, must have, or must acquire, any contractual, financial, business, or other interest, direct or indirect, that would conflict in any manner or degree with Contractor's performance of its duties and responsibilities to the State under this Contract or otherwise create an appearance of impropriety with respect to the award or performance of this Agreement. Contractor must notify the State about the nature of the conflict or appearance of impropriety within two days of learning about it.

(h) Neither Contractor nor any Affiliates, nor any employee of either has accepted or must accept anything of value based on an understanding that the actions of the Contractor or Affiliates or employee on behalf of the State would be influenced. Contractor must not attempt to influence any State employee by the direct or indirect offer of anything of value.

(i) Neither Contractor nor any Affiliates, nor any employee of either has paid or agreed to pay any person, other than bona fide employees and consultants working solely for Contractor or the Affiliate, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Contract.

(j) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other bidder; and no attempt was made by Contractor to induce any other person to submit or not submit a proposal for the purpose of restricting competition.

(k) All financial statements, reports, and other information furnished by Contractor to the State as part of its response to the RFP or otherwise in connection with the award of this Contract fairly and accurately represent the business, properties, financial condition, and results of operations of Contractor as of the respective dates, or for the respective periods, covered by the financial statements, reports, other information. Since the respective dates or periods covered by the financial statements, reports, or other information, there have been no material adverse changes in the business, properties, financial condition, or results of operations of Contractor.

(l) All written information furnished to the State by or for the Contractor in connection with this Contract, including its bid, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading.

(m) It is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State or the department within the previous five years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract.

(n) If any of the certifications, representations, or disclosures made in the Contractor's original bid response change after contract award, the Contractor is required to report those changes immediately to the Department of Technology, Management and Budget, Purchasing Operations.

2.122 WARRANTY

Contractor warrants that the Contractor's system will perform in accordance with the specifications in Article 1– Statement of Work of the Contractor's response to Section 1.104 of the RFP.

EXCEPT AS SPECIFICALLY SET FORTH IN THIS CONTRACT, CONTRACTOR DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH RELATE TO THE SERVICES PROVIDED UNDER THIS CONTRACT. FURTHER, CONTRACTOR DOES NOT WARRANT THAT THE STATE'S USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. THIS CONTRACT IS A SERVICE AGREEMENT, ANY EQUIPMENT PROVIDED TO THE STATE UNDER THIS CONTRACT IS INCIDENTAL TO THE SERVICES PROVIDED, AND THE PROVISIONS OF THE UNIFORM COMMERCIAL CODE DO NOT APPLY TO THIS CONTRACT.

2.123 RESERVED

2.124 RESERVED

2.125 RESERVED

2.126 EQUIPMENT TO BE NEW

If applicable, all equipment provided under this Contract by Contractor shall be new where Contractor has knowledge regarding whether the equipment is new or assembled from new or serviceable used parts that are like new in performance or has the option of selecting one or the other. Equipment that is assembled from new or serviceable used parts that are like new in performance is acceptable where Contractor does not have knowledge or the ability to select one or other, unless specifically agreed otherwise in writing by the State.

2.127 PROHIBITED PRODUCTS

The State will not accept salvage, distressed, outdated or discontinued merchandise. Shipping of such merchandise to any State agency, as a result of an order placed against the Contract, shall be considered default by the Contractor of the terms and conditions of the Contract and may result in cancellation of the Contract by the State. The brand and product number offered for all items shall remain consistent for the term of the Contract, unless Purchasing Operations has approved a change order pursuant to Section 2.024.

2.128 CONSEQUENCES FOR BREACH

In addition to any remedies available in law, if the Contractor breaches any of the warranties contained in this section, the breach may be considered as a default in the performance of a material obligation of this Contract.

2.130 Insurance

2.131 LIABILITY INSURANCE

The Contractor must provide proof of the minimum levels of insurance coverage as indicated below. The insurance must protect the State from claims that may arise out of or result from the Contractor's performance of services under the terms of this Contract, whether the services are performed by the Contractor, or by any subcontractor, or by anyone directly or indirectly employed by any of them, or by anyone for whose acts they may be liable.

The Contractor waives all rights against the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents for recovery of damages to the extent these damages are covered by the insurance policies the Contractor is required to maintain under this Contract.

All insurance coverage provided relative to this Contract/Purchase Order is PRIMARY and NON- CONTRIBUTING to any comparable liability insurance (including self-insurances) carried by the State.

The insurance must be written for not less than any minimum coverage specified in this Contract or required by law, whichever is greater.

The insurers selected by Contractor must have an A.M. Best rating of A or better, or as otherwise approved in writing by the State, or if the ratings are no longer available, with a comparable rating from a recognized insurance rating agency. All policies of insurance required in this Contract must be issued by companies that have been approved to do business in the State.

See www.michigan.gov/dleg.

Where specific limits are shown, they are the minimum acceptable limits. If Contractor's policy contains higher limits, the State must be entitled to coverage to the extent of the higher limits.

The Contractor is required to pay for and provide the type and amount of insurance below:

1. Commercial General Liability with the following minimum coverage:

$2,000,000 General Aggregate Limit other than Products/Completed Operations

$2,000,000 Products/Completed Operations Aggregate Limit

$1,000,000 Personal & Advertising Injury Limit

$1,000,000 Each Occurrence Limit

2. If a motor vehicle is used to provide services or products under this Contract, the Contractor must have vehicle liability insurance on any auto including owned, hired and non-owned vehicles used in Contractor's business for bodily injury and property damage as required by law.

3. Workers' compensation coverage must be provided according to applicable laws governing the employees and employers work activities in the state of the Contractor's domicile. If a self-insurer provides the applicable coverage, proof must be provided of approved self-insured authority by the jurisdiction of domicile. For employees working outside of the state of qualification, Contractor must provide appropriate certificates of insurance proving mandated coverage levels for the jurisdictions where the employees' activities occur.

The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company. This provision must not be applicable where prohibited or limited by the laws of the jurisdiction in which the work is to be performed.

4. Employers liability insurance with the following minimum limits:

$100,000 each accident

$100,000 each employee by disease

5. $500,000 aggregate disease

Employee Fidelity, including Computer Crimes, insurance naming the State as a loss payee,

providing coverage for direct loss to the State and any legal liability of the State arising out of or related to fraudulent or dishonest acts committed by the employees of Contractor or its Subcontractors, acting alone or in collusion with others, in a minimum amount of one million dollars ($1,000,000.00).

6. Umbrella or Excess Liability Insurance in a minimum amount of five million dollars ($5,000,000.00), which must apply, at a minimum, to the insurance required in Subsection 1 (Commercial General Liability) above.

7. Professional Liability (Errors and Omissions) Insurance with the following minimum coverage: three million dollars ($3,000,000.00) each occurrence and three million dollars ($3,000,000.00) annual aggregate.

2.132 SUBCONTRACTOR INSURANCE COVERAGE

Intentionally omitted.

2.133 CERTIFICATES OF INSURANCE AND OTHER REQUIREMENTS

Contractor must furnish to DTMB Purchasing Operations, certificate(s) of insurance verifying insurance coverage or providing satisfactory evidence of self-insurance as required in this Section (the “Certificates”) if requested in writing, and not more than once annually. The Certificate must be on the standard “accord” form or equivalent. The Contract Number or the Purchase Order Number must be shown on the Certificate Of Insurance To Assure Correct Filing. All Certificate(s) are to be prepared and submitted by the Insurance Provider. Contractor agrees to provide the Director of Purchasing Operations, Department of Technology, Management and Budget, with 30 days prior written notice, except for 10 days for non-payment of premium, of cancellation of any of insurance coverage required in this Section. The notice must include the Contract or Purchase Order number affected. Before the Contract is signed, and not less than 20 days before the insurance expiration date every year thereafter, the Contractor must provide evidence that the State and its agents, officers and employees are listed as additional insured under each commercial general liability and commercial automobile liability policy. In the event the State approves the representation of the State by the insurer’s attorney, the attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.

The Contractor must maintain all required insurance coverage throughout the term of the Contract and any extensions and, in the case of claims-made Commercial General Liability policies, must secure tail coverage for at least three years following the expiration or termination for any reason of this Contract. The minimum limits of coverage specified above are not intended and must not be construed; to limit any liability or indemnity of Contractor under this Contract to any indemnified party or other persons. Contractor is responsible for all deductibles with regard to the insurance. If the Contractor fails to pay any premium for required insurance as specified in this Contract, or if any insurer cancels or significantly reduces any required insurance as specified in this Contract without the State’s written consent, then the State may, after the State has given the Contractor at least 30 days written notice, pay the premium or procure similar insurance coverage from another company or companies. The State may deduct any part of the cost from any payment due the Contractor, or the Contractor must pay that cost upon demand by the State.

2.200 Federal and State Contract Requirements

2.201 NONDISCRIMINATION

In the performance of the Contract, Contractor agrees not to discriminate against any employee or applicant for employment, with respect to his or her hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of race, color, religion, national origin, ancestry, age, sex, height, weight, and marital status, physical or mental disability. Contractor further agrees that every subcontract entered into for the performance of this Contract or any purchase order resulting from this Contract will contain a provision requiring non-discrimination in employment, as specified here, binding upon each Subcontractor. This covenant is required under the Elliot Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, et seq., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., and any breach of this provision may be regarded as a material breach of the Contract.

2.202 UNFAIR LABOR PRACTICES

Under 1980 PA 278, MCL 423.321, et seq., the State must not award a Contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled under section 2 of the Act. This information is compiled by the United States National Labor Relations Board. A Contractor of the State, in relation to the Contract, must not enter into a contract with a Subcontractor, manufacturer, or supplier whose name appears in this register. Under section 4 of 1980 PA 278, MCL 423.324, the State may void any Contract if, after award of the Contract, the name of Contractor as an employer or the name of the Subcontractor, manufacturer or supplier of Contractor appears in the register.

2.203 WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT

In performing Services for the State, the Contractor must comply with the Department of Civil Services Rule 2- 20 regarding Workplace Safety and Rule 1-8.3 regarding Discriminatory Harassment. In addition, the Contractor must comply with Civil Service regulations and any applicable agency rules provided to the Contractor. For Civil Service Rules, see http://www.mi.gov/mdcs/0,1607,7-147-6877---,00.html.

2.204 PREVAILING WAGE

The rates of wages and fringe benefits to be paid each class of individuals employed by the Contractor, its subcontractors, their subcontractors, and all persons involved with the performance of this Contract in privity of contract with the Contractor shall not be less than the wage rates and fringe benefits established by the Michigan Department of Labor and Economic Development, Wage and Hour Bureau, schedule of occupational classification and wage rates and fringe benefits for the local where the work is to be performed. The term Contractor shall include all general contractors, prime contractors, project managers, trade contractors, and all of their contractors or subcontractors and persons in privity of contract with them.

The Contractor, its subcontractors, their subcontractors and all persons involved with the performance of this contract in privity of contract with the Contractor shall keep posted on the work site, in a conspicuous place, a copy of all wage rates and fringe benefits as prescribed in the contract. You must also post, in a conspicuous place, the address and telephone number of the Michigan Department of Labor and Economic Development, the office responsible for enforcement of the wage rates and fringe benefits. You shall keep an accurate record showing the name and occupation of the actual wage and benefits paid to each individual employed in connection with this contract. This record shall be available to the State upon request for reasonable inspection.

If any trade is omitted from the list of wage rates and fringe benefits to be paid to each class of individuals by the Contractor, it is understood that the trades omitted shall also be paid not less than the wage rate and fringe benefits prevailing in the local where the work is to be performed.

Signatures follow on next page.

IN WITNESS WHEREOF, the duly authorized representatives of the parties hereto have caused this SOW to be duly executed.

First Data Government Solutions, LP
By: First Data Merchant Services, LLC
Its General Partner

By: ________________________________

Name: ______________________________

Title: _______________________________

Date: _______________________________

Trustwave Holdings, Inc.
on behalf of SecureTrust

By: ________________________________

Name:_______________________________

Title: _______________________________

Date: _______________________________

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**
to
Contract Number **071B1300185**

CONTRACTOR	FIRST DATA GOVERNMENT SOLUTIONS LP
	3975 NW 120th Avenue
	Coral Springs, FL 33065
	Jason Clark
	(513) 207-5265
	jason.clark@Fiserv.com
	CV0060377

STATE	Program Manager	Susan Stephens	TREA
		(517) 636-5089	
		Stephens@michigan.gov	
	Contract Administrator	Mike Breen	DTMB
		breenm@michigan.gov	

CONTRACT SUMMARY			
CEPAS			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 1, 2011	June 30, 2016	5 - 1 Year	June 30, 2020

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
☐ P-Card ☐ PRC ☐ Other	☐ Yes ☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	12 months	☐		June 30, 2021

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$6,628,348.00	$180,000.00	$6,808,348.00

DESCRIPTION

Effective with mutual signature the contract is amended to add $180,000.00 in operational funding and to exercise a one year option to 6/30/2021. All other terms and conditions remain the same.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **071B1300185**

CONTRACTOR	First Data Government Solutions LP
	11311 Cornell Park Drive
	Cincinnati, OH 45242
	Jason Clark
	(513) 489-9599 x184
	jason.clark@firstdata.com
	CV0060377

STATE	Program Manager	Susan Stephens	DTMB
		517-636-5089	
		Stephens@Michigan.gov	
	Contract Administrator	James Wilson	DTMB
		(517) 243-0434	
		wilsonj40@michigan.gov	

CONTRACT SUMMARY			
CEPAS TREASURY			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
July 1, 2011	June 30, 2016	5 - 1 Year	June 30, 2018
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-Card	☐ PRC	☐ Other	☐ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☐		☐		June 30, 2020
CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**		
$6,628,348.00	$0.00	$6,628,348.00		

DESCRIPTION

DESCRIPTION
Effective 4/11/2019 The change includes updates to links and language per the latest SOM standard per Attachment# 1. The Program Manager and Contract Administrator have also been updated. All other terms, conditions, pricing and specifications remain the same. Per vendor and agency agreement and DTMB Procurement approval.

Attachment # 1 – 071B1300185 CN# 03 – 4/11/2019

Updating language and links from original contract to latest State of Michigan standards.

1. **Section 2.272 Acceptable Use Policy** - Update Link – Page 121
   - To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, 1340.00.130.02 Acceptable Use of Information Technology Standard
   - All Contractor Personnel will be required, in writing to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

   C2. Operational Controls – D. Security Incident Handling – Page 49

   a. Add item 6. Incident Response Standard Policy – 1340.00.090.01, notification must be within 24 hours of a confirmed breach.
   Added standard

      i. 090 Incident Response (IR-1): SOM IT standard 1340.00.090.01 establishes the Incident Response standards in SOM policy.

         - **IR-6 Incident Reporting**
           - The Information Owner will ensure that the Agency implements and documents the following baseline controls: Requires personnel to report confirmed security incidents to the organization management team and the organizational incident response team (DTMB CIP) **immediately but not later than 24 hours.**
           - Reports security incident information to designated individuals. Confirmed security incidents include, for example, unauthorized system changes or access. The types of security incidents reported, the content and timeliness of reports, and the designated reporting authorities reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

      Contractor will review State Security Standards annually to confirm compliance or follow Federal standards. State will notify Contractor of any changes outside of the annual review.

2. **C2. Operation Controls** – H. Media Destruction and Disposal – Item 1 (Bullet 2) – Page 51

a. Add “flash drive”
b. First Data's Media Handling Standard requires the unrecoverable disposal of electronic and physical media and/or the data for Internal Only (class 2), Confidential (class 3), and Restricted (class 4) information. Destruction: Disintegration, incineration, pulverization, melting, or acid-wash must be performed by a licensed vendor with the facilities to perform such operations securely and safely. Shredding must be performed using an approved method and limit the shred size of the media to no more than those defined in the applicable NIST standards, NAID standards, PCI standard, or Card Association standards for destruction of the class of material. Sanitizing: Overwriting must be performed using a commercially available, non-proprietary product and procedures approved by GCSF. The product must implement at least a triple overwrite process with a final randomized overwrite and should meet DOD 5220-22-m (NISPOM) destruction criteria. Handling: Physical media intended for disposal must be stored in locked containers to prevent unauthorized removal or access to the data. Transport of these materials to a vendor, if necessary, must comply with First Data Standards.

3. **C2. Operational Controls** – I. Data Security – Page 52
   a. Remove Item 3 – Secure Socket Layer (SSL) is no longer considered secure and is to be removed.

4. **C3. Payment Card Industry (PCI) Data Security Standards** – Mastercard – Page 53
   a. Update link for Mastercard’s site for Payment Industry Data Security Standard (PCI DSS)
      i. Revised link - https://www.mastercard.us/en-us/merchants/safety- security/security-recommendations/site-data-protection-PCI.html

5. **Section 2.131 Liability Insurance** – Remove link – Page 104
   a. Removed link – www.michigan.gov/dleg - no longer valid – remove/delete

6. **Section 2.271 Existing Technologies** – Update language – Page 121
   a. **Enterprise IT Policies, Standards and Procedures**
      Contractor at minimum are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractor will provide solutions that meet State IT policies and standards. All services and products provided as a result of this contract must comply with all applicable

      State IT policies and standards. Contractor is required to review all applicable policies provided below and state compliance in their response. Enterprise IT Policies, Standards and Procedures:

PSPs
1340:

- 1340.00.130.02 Acceptable Use of Information Technology Standard

1355:

- Policy 1355 Project Management Methodology

1360:

- Policy 1360 Systems Engineering Methodology

1365:

- Policy 1365 Technology (IT) Standards Adoption, Acquisition, Development

Contractor will review State Security Standards annually to confirm compliance or follow Federal PSP standards. State will notify Contract of any changes outside of the annual review.

Look and Feel Standard
All software items provided by the Contractor must adhere to the Look and Feel Standards:

www.michigan.gov/standards

The application currently meets existing standards effective before May 31, 2018 based on contract being effective July 1, 2011.

End-User Operating Environment

Below is the initial end user operating environment that must be supported by the Contractor. Contractor is expected to keep pace with changes in standard operating environments (e.g. operating system upgrades, web browser upgrades, mobile OS upgrades).

The Solution must not use any specialized or proprietary hardware, devices and/or computers.

The Solution will not use any plugins and will not require Java, Flash, or Silverlight.

Web Browsers
Solution must run under commonly used web browsers. At a minimum, the software must support Internet Explorer v9+, Chrome v36+, Firefox v31+, Safari v5.1+, and Edge 20.1+ under the Windows and iOS operating Solutions

ADA Compliance

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's proposed Solution, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. The State may require that Contractor complete a Voluntary Product Accessibility Template for WCAG 2.0 (WCAG2.0 VPAT) or other comparable document for the proposed Solution. http://www.michigan.gov/documents/dmb/1650.00_2095 67_7.pdf?20151026134 621

7. **Section 2.290 Environmental Provision** – Delete/Not Applicable

8. D18. **Operational Internal Controls:** Update language
   - **a.** Primary site needs to be changed from Denver, Colorado to Chandler, Arizona.
   - **b.** Remove references to Denver and insert Chandler

9. **D2. System Maintenance:**
   - **a.** First Data Government Solutions may perform PayPoint maintenance weekdays after 8:00 pm ET, for updates that do not require system outages. For updates that require system down time, the maintenance window is on Sundays between 2:00 a.m. and 6:00 a.m. ET. The business contact provides notification via email to the State 14-calendar days in advance of the maintenance date. The exception is for a system hot fix that impacts the functionality of the product, which is moved into production as quickly as it can be scheduled.

10. **Emergency Maintenance:**
   - **a.** First Data Government Solutions provides all information to the State when performing emergency maintenance. We provide the patch or hot fix names, as well as the technical details for the patch. We do not proceed without

informing the State prior to change. The exception is in cases of high-risk security issues
and critical performance issues; in which case, changes need to be made before informing the State, with notification within 24 hours of the change.

11. **D3. TSYS Connectivity:**
    a. First Data Government Solutions uses the TLS 1.2 supported HTTPS connectivity to TSYS. We will continue to be responsible for the costs associated with this connection.

12. **D12. System Upgrades / Changes / New Releases:**
    a. First Data Government Solutions will provide a 60-day notice for PayPoint Releases and Hardware upgrades. The notification is sent to the State via email that includes: the Client Release Notes (if applicable), and details for a hardware upgrade or release. A 60-day notification may not be possible for third party vendors (i.e. Microsoft patches). We provide Client Release Notes (if applicable) for PayPoint Releases and hardware upgrade documentation 30-days prior to implementation. A 30-day period may
    not be possible for third party vendors (i.e. Microsoft patches). A testable version of PayPoint Releases and planned hardware maintenance are available 30-days prior to implementation. The exception is a hotfix to address a production issue.

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**
to
Contract Number **071B1300185**

CONTRACTOR	First Data Government Solutions LP
	11311 Cornell Park Drive
	Cincinnati, OH 45242
	Jason Clark
	(513) 489-9599 x184
	jason.clark@firstdata.com
	CV0060377

STATE	Program Manager	Mark Lawrence	TREA
		517-636-6435	
		LawrenceM2@Michigan.gov	
	Contract Administrator	Jennifer Bronz	DTMB
		(517) 249-0493	
		bronzj@michigan.gov	

CONTRACT SUMMARY

CEPAS TREASURY

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
July 1, 2011	June 30, 2016	5 - 1 Year	June 30, 2018

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ Direct Voucher (DV)	☐ Other	☐ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒		☐		June 30, 2020

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$4,628,348.00	$2,000,000.00	$6,628,348.00

DESCRIPTION

Effective 6/26/2018 This contract is exercising the next 2 option years and funds added of $2,000,000.00. The revised contract date is 6/30/2020. All other terms, conditions, pricing and specifications remain the same. Per vendor and agency agreement and DTMB Procurement approval and State Administrative Board approval on 6/26/2018.

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **071B1300185**

CONTRACTOR	First Data Government Solutions LP
	11311 Cornell Park Drive
	Cincinnati, OH 45242
	Jason Clark
	(513) 489-9599 x184
	jason.clark@firstdata.com
	*******2959

STATE	Program Manager	Lawrence, Mark	DTMB
		517-636-6435	
		LawrenceM2@Michigan.gov	
	Contract Administrator	Jarrod Barron	DTMB
		(517) 284-7045	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY

DESCRIPTION: CEPAS Treasury

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
July 1, 2011	June 30, 2016	5 - 1 Year	June 30, 2016

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-card	☐ Direct Voucher (DV)	☐ Other	☐ Yes	x No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	2 years	☐		June 30, 2018

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$3,028,348.00	$ 1,600,000	$4,628,348.00

DESCRIPTION: DESCRIPTION: Effective 06/07/2016 this contract for the Department of Treasury hereby incorporates the following changes.

1. Utilize two option years. New contract end date is June 30, 2018
2. Add funds in the amount of $1,600,000 to finance two option years. Per Ad-Board approval 06/07/2016.
3. Incorporate updated pricing tier table below. New pricing table replaces current table found in Appendix A; Article 1, Attachment A.
4. Update buyer to Jarrod Barron

All other terms, conditions, pricing and specifications remain the same. Per vendor and agency agreement and DTMB Procurement approval.

Range of monthly Transactions	Unit Fee	X Estimated Monthly Volume	Total Estimate
0 - 150,000	$0.15	150,000	$22,500.00
150, 001 - 250,000	$0.14	250,000	$35,000.00
250,001 - 300,000	$0.13	300,000	$39,000.00
300,001 - 350,000	$0.13	350,000	$45,500.00
350,001 - 400,000	$0.12	400,000	$48,000.00
400,001 - 450,000	$0.11	450,000	$51,745.50
450,001 -500,000	$0.095	500,000	$47,500.00
500,001 -550,000	$0.095	550,000	$52,250.00
550,001 -600,000	$0.085	600,000	$51,000.00
600,001- 650,000	$0.085	650,000	$55,250.00
650,001 - 700,000	$0.08	700,000	$56,000.00
700,001 - 750,000	$0.08	750,000	$60,000.00

New Pricing Tier

Form No. DMB 234 (Rev. 1/96)
AUTHORITY: Act 431 of 1984
COMPLETION: Required
PENALTY: Contract will not be executed unless form is filed

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET **February 4, 2011**
PURCHASING OPERATIONS
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

NOTICE OF CONTRACT NO. 071B1300185 between THE STATE OF MICHIGAN and

NAME & ADDRESS OF CONTRACTOR **First Data Government Solutions, LP** **11311 Cornell Park Drive, Suite 300** **Cincinnati, OH 45242** **Email: Jason.clark@firstdata.com**	TELEPHONE **Jason Clark** **(513) 489-9599 x184** CONTRACTOR NUMBER/MAIL CODE BUYER/CA (517) 373-1455 **Laura Gyorkos**

Contract Compliance Inspector: **Mark Lawrence**
Centralized Electronic Payment Authorization System - Statewide

CONTRACT PERIOD: **5 yrs. + 5 one-year options** From: **July 1, 2011** To: **June 30, 2016**

TERMS **N/A**	SHIPMENT **N/A**
F.O.B. **N/A**	SHIPPED FROM **N/A**

ALTERNATE PAYMENT OPTIONS:
□ P-card □ Direct Voucher (DV) □ Other

MINIMUM DELIVERY REQUIREMENTS
N/A

TOTAL ESTIMATED CONTRACT VALUE: $3,028,348.00

Form No. DMB 234 (Rev. 1/96)
AUTHORITY: Act 431 of 1984
COMPLETION: Required
PENALTY: Contract will not be executed unless form is filed

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PURCHASING OPERATIONS
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

CONTRACT NO. 071B1300185
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF CONTRACTOR **First Data Government Solutions, LP** **11311 Cornell Park Drive, Suite 300** **Cincinnati, OH 45242** **Email: Jason.clark@firstdata.com**	TELEPHONE **Jason Clark** **(513) 489-9599 x184** CONTRACTOR NUMBER/MAIL CODE BUYER/CA (517) 373-1455 **Laura Gyorkos**

Contract Compliance Inspector: **Mark Lawrence**
Centralized Electronic Payment Authorization System - Statewide

CONTRACT PERIOD: **5 yrs. + 5 one-year options** From: **July 1, 2011** To: **June 30, 2016**

TERMS **N/A**	SHIPMENT **N/A**
F.O.B. **N/A**	SHIPPED FROM **N/A**

ALTERNATE PAYMENT OPTIONS:
□ P-card □ Direct Voucher (DV) □ Other

MINIMUM DELIVERY REQUIREMENTS
N/A

The terms and conditions of this Contract are those of ITB #071I0200208 this Contract Agreement and the vendor's quote dated 9/2/10. In the event of any conflicts between the specifications, and terms and conditions, indicated by the State and those indicated by the vendor, those of the State take precedence.

Estimated Contract Value: $3,028,348.00

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the ITB No. #071I0200208 Orders for delivery will be issued directly by State Departments through the issuance of a Purchase Order Form.

All terms and conditions of the invitation to bid are made a part hereof.

FOR THE CONTRACTOR:

First Data Government Solutions
Firm Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Greg Faremouth, Director
Name/Title

IT Division
Division

Date

STATE OF MICHIGAN
Department of Technology, Management and Budget
Purchasing Operations

Contract No. **071B1300185**
Centralized Electronic Payment and Authorization System (CEPAS)

Buyer Name: Laura Gyorkos
Telephone Number: 517-373-1455
E-Mail Address: gyorkosL@michigan.gov

Table of Contents

Appendices

DEFINITIONS

Days	Means calendar days unless otherwise specified.
24x7x365	Means 24 hours a day, seven days a week, and 365 days a year (including the 366th day in a leap year).
Additional Service	Means any Services/Deliverables within the scope of the Contract, but not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
Audit Period	See Section 2.110
Business Day	Whether capitalized or not, shall mean any day other than a Saturday, Sunday or State-recognized legal holiday (as identified in the Collective Bargaining Agreement for State employees) from 8:00am EST through 5:00pm EST unless otherwise stated.
Blanket Purchase Order	An alternate term for Contract as used in the States computer system.
Business Critical	Any function identified in any Statement of Work as Business Critical.
Chronic Failure	Defined in any applicable Service Level Agreements.
Deliverable	Physical goods and/or commodities as required or identified by a Statement of Work
DTMB	Michigan Department of Technology, Management and Budget
Environmentally preferable products	A product or service that has a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. Such products or services may include, but are not limited to, those that contain recycled content, minimize waste, conserve energy or water, and reduce the amount of toxics either disposed of or consumed.
Excusable Failure	See Section 2.244.
Hazardous material	Any material defined as hazardous under the latest version of federal Emergency Planning and Community Right-to-Know Act of 1986 (including revisions adopted during the term of the Contract).
Incident	Any interruption in Services.
ITB	A generic term used to describe an Invitation to Bid. The ITB serves as the document for transmitting the RFP to potential bidders
Key Personnel	Any Personnel designated in Article 1 as Key Personnel.
New Work	Any Services/Deliverables outside the scope of the Contract and not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
Ozone-depleting substance	Any substance the Environmental Protection Agency designates in 40 CFR part 82 as: (1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or (2) Class II, including, but not limited to, hydro chlorofluorocarbons
Post-Consumer Waste	Any product generated by a business or consumer which has served its intended end use, and which has been separated or diverted from solid waste for the purpose of recycling into a usable commodity or product, and which does not include post-industrial waste.
Post-Industrial Waste	Industrial by-products that would otherwise go to disposal and wastes generated after completion of a manufacturing process, but do not include internally generated scrap commonly returned to industrial or manufacturing processes.
Recycling	The series of activities by which materials that are no longer useful to the generator are collected, sorted, processed, and converted into raw materials and used in the production of new products. This definition excludes the use of these materials as a fuel substitute or for energy production.
Deleted – Not Applicable	Section is not applicable or included in this RFP. This is used as a placeholder to maintain consistent numbering.

Reuse	Using a product or component of municipal solid waste in its original form more than once.
RFP	Request for Proposal designed to solicit proposals for services
Services	Any function performed for the benefit of the State.
Source reduction	Any practice that reduces the amount of any hazardous substance, pollutant, or contaminant entering any waste stream or otherwise released into the environment prior to recycling, energy recovery, treatment, or disposal.
State Location	Any physical location where the State performs work. State Location may include state-owned, leased, or rented space.
Subcontractor	A company Contractor delegates performance of a portion of the Services to, but does not include independent contractors engaged by Contractor solely in a staff augmentation role.
Unauthorized Removal	Contractor's removal of Key Personnel without the prior written consent of the State.
Waste prevention	Source reduction and reuse, but not recycling.
Waste reduction and Pollution prevention	The practice of minimizing the generation of waste at the source and, when wastes cannot be prevented, utilizing environmentally sound on-site or off-site reuse and recycling. The term includes equipment or technology modifications, process or procedure modifications, product reformulation or redesign, and raw material substitutions. Waste treatment, control, management, and disposal are not considered pollution prevention, per the definitions under Part 143, Waste Minimization, of the Natural Resources and Environmental Protection Act (NREPA), 1994 PA 451, as amended.
Work in Progress	A Deliverable that has been partially prepared, but has not been presented to the State for Approval.
Work Product	Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Contractor as a result of an in furtherance of performing the services required by this Contract.

GLOSSARY

TERMS	DEFINITIONS
Address Verification Service (AVS)	A service that verifies the billing address of a cardholder in a card-not-present transaction to help combat fraud, which then controls charge backs.
Application Program Interface (API)	The interface by which an application program accesses the operating system.
Association	A region or group of merchants established by a Department.
Authorization	Electronic message sent by a merchant to the processor which asks if the credit card presented is valid and can accept the charge.
Automated Clearing House (ACH) Network	A funds transfer system that provides for the inter-bank clearing of electronic entries for participating financial institutions.
Batch	A collection of records or transactions submitted for settlement, usually one day's worth.
CEPAS	The Centralized Electronic Payment and Authorization System (CEPAS) is an enterprise-wide electronic payment solution.
Credit Card	A plastic card in which the issuer (financial institution) establishes a revolving line of credit for its cardholder.
Debit Card	A plastic card used to initiate a debit transaction. In general these transactions are used primarily to purchase goods and services and to obtain cash, for which the cardholder's bank account is debited by the card issuer.
Department	Refers to agencies that make up State of Michigan government, such as Department of Treasury or Department of State.
Electronic Funds Transfer (EFT)	A generic term used to describe any ACH or wire transfer. A transmission of money from one account to another utilizing the ACH network.
End-to-End Encryption	Continuous protection of the confidentiality and integrity of transmitted data by encrypting it at the origin, then decrypting at its destination.
Fiscal Year	The State's fiscal year starts on October 1 and ends on September 30. For example, Fiscal Year 2010 began on October 1, 2009 and ends on September 30, 2010.
Interactive Voice Response (IVR)	An IVR is a software application that accepts a combination of voice telephone input and touch-tone keypad selection and provides appropriate responses back to the caller.
Interchange Fee	A fee applied to a card transaction; applicable to the members participating in the transaction as issuer and acquirer. The applicable interchange fee is determined by the authorization method, settlement period, and data in the authorization/settlement record.
National Automated Clearing House Association (NACHA)	The national association that establishes the standards, rules and procedures that enable depository financial institutions to exchange payments on a national basis.
Notification of Change (NOC)	An advice sent by the RDFI to notify the ODFI the customer information provided is erroneous and needs to be updated.
Originating Depository Financial Institution (ODFI)	A participating financial institution that initiates ACH entries at the request of its customers.
Pre-Notification	A non-dollar entry that may be sent through the ACH network by an originator to alert an RDFI that a live transaction will be forthcoming. Verification of the account information is required.
Receiving Depository Financial Institution (RDFI)	Any financial institution qualified to receive ACH transactions.
Returns	Any ACH entry that has been returned to the ODFI from the RDFI because it cannot be processed. The reason for the return is included with the return in the form of a "reason code".

Routing Transit Number (RTN)	The American Banking Association (ABA) routing number is a unique, bank-identifying number that directs electronic ACH deposits to the proper bank. This number precedes the account number printed at the bottom of a check.
Secure Socket Layer (SSL)	Encryption technology, which reduces the likelihood of payment card data from being intercepted as it passes through the internet.
Standard Entry Class Code	Three character codes that identify payment type within an ACH batch.
State	State of Michigan

Article 1 – Statement of Work (SOW)

1.000 Project Identification

1.001 PROJECT REQUEST

The State of Michigan (State), through the Michigan Department of Treasury, Receipts Processing Division, and the Michigan Department of Technology, Management & Budget (DTMB) has established this contract for an enterprise-wide system for authorization and processing of electronic payments. This centralized system will support multiple electronic payment instruments and a variety of input channels.

This contract is a fixed price contract and has a maximum term of five (5) years with five (5) additional one (1) year renewal periods. Renewal of the contract will be at the sole discretion of the State and will be based upon the acceptable performance of the selected Contractor as determined by the State. If the State chooses to renew the contract, it may do so subject to the requirements of 1.A, Firm Pricing, of Section 1.601 and Section 2.002 of this contract.

1.002 BACKGROUND

The Department of Treasury, Receipts Processing Division is responsible for administration of the State's electronic payment systems and, with DTMB and State agencies, has worked to provide a centralized system for use by all State agencies.

In December 2006 the State entered a contract with its current Contractor to supply an enterprise-wide centralized authorization and payment solution. Within State government, the centralized solution is known as the Centralized Electronic Payment and Authorization System (CEPAS). Currently over 334 payment programs from 15 different State departments are processing through the existing system. The monthly processing volume averages approximately 239,000 transactions for over $27,000,000. Credit card transactions comprise over 95% of current volume.

CEPAS has been designated as the standard for making electronic payments to the State.

Payment programs accept a variety of electronic payment instruments including credit card, debit card (off-line and on-line), and ACH debit. Payment programs can initiate payments through a variety of payment channels including Web, Interactive Voice Response (IVR), remittance processor, kiosks, manual key entry, and/or card swipe device.

The current CEPAS Contractor provides Originating Depository Financial Institution (ODFI) services. The CEPAS Contractor acts as a third party service provider and provides ODFI services by maintaining a relationship with a partnering financial institution. The State does not have a direct contractual relationship with the Contractor's ODFI. It is the intent of the State to continue to have the CEPAS Contractor provide the ODFI services needed to process ACH transactions.

The State has standards and guidelines that Contractors are expected to follow. Specifically, the State's Project Management Methodology (PMM) must be followed. The PMM and other background information may be reviewed at www.michigan.gov/projectmanagement.

1.100 Scope of Work and Deliverables

1.101 IN SCOPE

- Services for payment processing and authorization
  - o configuration
  - o interfaces
  - o integration
  - o testing
- Knowledge transfer to State staff
  - o Training
  - o Train the trainer
  - o End user
  - o Technical

- Documentation, to include
    - User manuals
    - Technical manuals
- Maintenance
    - Support
    - Help Desk
    - Technical
- Other
    - Reserve bank of hours for future enhancements and/or legislative mandates

Summary of Scope

- The State of Michigan currently has a statewide contract for credit and debit card processing services and acceptance of Visa, MasterCard and Discover. State merchant applications will use TSYS (formerly Vital) Payment Services. **It is the intent of the State to continue to use TSYS Processing Services. Proposals that do not include TSYS Processing Services as a processing option will be disqualified from the evaluation process.**
- The Contractor will supply and implement for State use an enterprise-wide system to process both credit/debit (pin-less and pin-based) cards and ACH debit payments that are submitted from multiple agency applications through a variety of payment channels including Web, IVR, Kiosks, Remittance Machine, software which allows Manual Key Entry, and/or card swipe device.
- Note: Hereafter the term “credit card“ refers to both credit and debit cards.
- The Contractor will provide standard Application Program Interfaces (APIs) and Key Entry Screens to allow State of Michigan electronic payments to be collected, securely stored and settled, and the funds credited to the corresponding State bank accounts. The system will provide a response that contains a unique confirmation number and can be printed and used as a customer receipt.
- The Contractor will map applications using the current Contractor’s API that is already programmed into State applications and translate them to the Contractor’s API during implementation.
- The Contractor’s system will be capable of tracking individual business application activity at the application, association (merchant chain), agency, and statewide levels and allow authorized State users access, by authorized level, to search for payments and view details related to each transaction.
- The Contractor’s system must have edits in place to identify and reject duplicate payments, be capable of calculating convenience fees, and be capable of collecting foreign addresses and accommodate processing of payments with foreign addresses.
- The system must be capable of obtaining both real-time and batch authorizations for credit/debit card transactions and be capable of processing credit/debit cards swiped through a card reader, such as a terminal or keyboard card swipe device.
- The system must provide the ability to cancel/void transactions prior to settlement and process full or partial refunds after settlement. For credit cards this includes the capability to process an authorization reversal.
- The Contractor will provide ODFI services to process ACH debit transactions under the contract.
- The Contractor will receive ACH Notifications of Change and Returns and update the system and make Return information available to the agency.
- The Contractor will provide a registration process to allow State customers to set up financial accounts and schedule payments. The Contractor will securely store customer account data and provide a unique registration ID that corresponds to the customer’s financial data.
- The system will allow for future-dated ACH payments.
- The Contractor will be required to assist with migration of State customers with enrolled and scheduled accounts from the existing Contractor by receiving a file from the existing Contractor containing information on enrolled and scheduled customers. The Contractor will map the information in the file to its enrollment database and supply new registration IDs and other required information to the appropriate agency applications to allow the agency applications to continue to process enrolled and scheduled transactions.

- The Contractor's system will provide a customizable generic Web and IVR hosted solution to provide a customer facing front end interface to the Contractor's system functionality for agency units that desire an electronic payment capability but do not have the resources to build their own front end interface.
- The Contractor's system will comply with payment processing rules, regulations, and laws such as the NACHA Operating Rules, Card Association Operating Rules and Regulations, Payment Card Industry Data Security Standards, Federal Regulation E, etc.
- The Contractor's system shall be comprised of redundant hardware and software and a fully functioning back up site that is a mirror image of the production site to provide for 99.9% system availability and minimal periods of downtime.
- The Contractor's system must provide a daily average response time of 3 seconds or less.
- The Contractor's system must not allow duplicate transactions to process.
- The Contractor's system must provide fully functioning Initial Test and User Acceptance Test (UAT) environments that replicates the production environment. The UAT must allow for end-to-end testing and include true credit card and ACH settlement and refunds. The Contractor must also provide system documentation, training, training material, dedicated business and technical contacts, and 24/7 emergency support.
- The Contractor's system must provide robust reporting capability that allows for a variety of production and statistical reporting as well as security reports that track user activity and user access rights.
- The Contractor must provide a daily feedback file that contains details of the previous day's transactions.
- The Contractor must provide a disaster recovery site that is a functionally complete replica of the primary site, utilizing identical software, hardware settings and values, and will provide performance equal to the primary site.

A more detailed description of the services (work) and deliverables sought for this project is provided in Article 1, Section 1.104, Work and Deliverables.

1.102 OUT OF SCOPE

- The State requires the use of TSYS Processing Services. For this contract, any other processing gateway is out of scope.
- The State currently has a statewide contract with a credit and debit card acquirer and for acceptance of Visa/MasterCard and Discover. These services are not included under this contract.
- ACH Disbursements (except reversals and refunds), Electronic Benefit Transfers (EBT), and Wire Transfer processing are not included in this contract.
- Receiving, processing, and depositing ACH Credit transactions initiated by State customers are not included under this contract.

1.103 ENVIRONMENT

Contractor shall abide by all State of Michigan applicable laws and regulations. Contractor shall maintain and implement written policies and procedures regarding data privacy and data security, including but not limited to the safeguarding of customer data designed to comply with the Federal Interagency Guidelines Establishing Information Security Standards. The Contractor's officers and employees are bound by the policies and procedures of Contractor.

1.104 WORK AND DELIVERABLE

Contractor shall provide Deliverables/Services and staff, and otherwise do all things necessary for or incidental to the performance of work identified in Section 1.101, In Scope, as set forth below:

A. GENERAL TASKS

A1. **Proven Product**: The Contractor shall provide a proven product that has been successfully utilized as an enterprise-wide solution to process both credit card and ACH payments from multiple payment applications within the same organization through a variety of input channels.

First Data Government Solutions currently provides all of the services listed above in our PayPoint product. The PayPoint product is installed in Michigan and Nevada in an enterprise environment. The product is also installed in the Alabama Dept. of Revenue, providing payment processing for local municipalities, as well as multiple local jurisdictions around the country (I.e. Columbus, Ohio)

A2. **Contractor Demo:** The Contractor may be required to provide an on-site demonstration of the product. The Contractor will be responsible for all costs associated with presenting the demonstration including travel, lodging, and other costs. The demonstration will include a detailed discussion of all functions and components of the Contractor's solution.

First Data Government Solutions is prepared to provide an onsite demonstration of our PayPoint engine. This Demonstration will include all existing functionality and we will be prepared to address the required enhancements.

A3. **Eastern Time Zone:** All time stamps and time references on the Contractor's system shall be capable of being reflected in Eastern Time.

First Data's PayPoint engine meets this requirement.

B. PAYMENT PROCESSING TASKS

B1. **Numbering System:** The Contractor will provide a numbering system to uniquely identify each agency and application. This number should function like a credit card "merchant number". Each transaction should be associated with this program-unique identification number.

First Data Government Solutions' PayPoint product assigns a unique number to each application. This number is used to uniquely represent the State's merchant application(s).

B2. **Track Program Activity:** The Contractor's system must be capable of tracking individual business application activity at the application level, association level (like merchant chain or region), agency level, and statewide level and summarizing transactions at the association, agency, and statewide level.

PayPoint supports three tracking levels including Site, Agency, and Application. All payment-related reports allow the capability to run payment activity and summary reports by Site, Agency, and multiple Applications. From a reporting perspective, this effectively supports the ability to group multiple applications into an association level. Payment searches allow the capability to run payment activity and summary reports by Site, Agency, and individual Applications. User management and Security Reports are available at the sate-wide level. Reports, Payment History, and Settlement allow the capability to summarize transactions at a Site, Agency and Application.

B3. **Application Program Interface (API):** The Contractor will be required to supply standard Application Program Interfaces (APIs) to allow State and third party vendor hosted applications to connect to the Contractor and perform various payment functions. It will be the Contractor's responsibility during implementation to map applications using the current CEPAS Contractor's API that is already programmed into State applications and translate them to the Contractor's API. See **Appendix D** for data requirements.

First Data Government Solutions' PayPoint product provides two different standard API interfaces, which include Web Services and HTTPS.

B4. System Compliance: The Contractor is responsible for system upgrades to ensure the system complies with changes to NACHA Rules and Regulations, Credit Card Rules, Federal Regulation E, Payment Card Industry Data Security Standards, and any other applicable law or rule/regulation change. The system must be in compliance by the time the change takes effect. The Contractor will provide written documentation to the Project Manager or designee describing any changes made to the system to maintain compliance at least 30 days before beginning the change. The system changes will be tested by the Contractor to ensure the changes produce the expected result.

First Data Government Solutions' PayPoint product is compliant with NACHA Rules and Regulations, Credit Card Rules, Federal Regulation E. Annual PCI audits are performed to ensure compliance with Credit Card and security requirements. As part of our TSYS Certified Partner and other associations, we are able to identify rules as they are released and assess the change/impacts to the product and deploy those changes within guidelines identified by the various ruling bodies. For major releases, First Data Government Solutions provides documentation to the Project Manager describing these changes within 30 days of the change. For minor releases or hotfixes, First Data Government Solutions provides documentation to the Project Manager describing these changes within seven (7) days of the change.

B5. **Application Configuration:** The Contractors system must be capable of setting up each State application with a flexible set of configuration settings based on the State's application needs.

The PayPoint product uses a hierarchical approach for configuration changes. Configuration settings can be made at the state-wide level, while individual application-level configuration settings can be adjusted to meet the business rules for each application.

B6. **Duplicate Check:** The Contractor will provide the ability to perform a duplicate payment check that is based on receiving the same payment information within a configurable time period. The duplicate check will be a configuration setting that is selected at application set up. The system will compare account information, payment amount, transaction date and time, and information contained in the Comments field to determine if the payment has been duplicated. If a duplicate payment is detected the duplicate is rejected with the appropriate error message returned.

PayPoint supports the ability to identify duplicate payments by all of the required elements listed in this requirement. The time period (in minutes) in which PayPoint checks for duplicate payments is configurable on an application-by-application basis, including the ability to skip duplicate checks.

B7. **Convenience Fees:** The Contractor's system must have the ability to calculate a convenience fee if the merchant/application charges a convenience fee. The convenience fee must be processed as required by Visa, MasterCard, and Discover rules (e.g. Visa requires the payment and the convenience fee to be combined and processed as one transaction).

PayPoint supports the ability to calculate convenience fees on an application-by-application basis. Convenience fees can be calculated as a percentage or fixed amount. Payments processed using convenience fees are stored as separate transactions. PayPoint makes sure that, if either the primary or convenience fee fails to authorize, the entire payment is voided and a decline is returned to the merchant's application.
Depending on the compliance rules (i.e. Visa), PayPoint can process the primary payment and convenience fee as two separate payments or combined as one payment (i.e. Visa).

B8. **Settlement:** Contractor's system must allow for settlement seven (7) days a week.

The PayPoint settlement system is capable of settling seven (7) days a week. Payment Settlement processing is based on a cut off time established on an Application-by-Application basis. Only payments processed prior to the cut off are processed in that day's settlement and are included in the batch.

B9. **Key Entry Payment Screen:** The Contractor will provide a payment data collection screen to allow for authorized State users with appropriate user access rights to manually key or card swipe and submit a credit card or ACH payment. The minimum fields to be included on the screen are defined in **Appendix C - Key Entry Payment Screen Fields**. Once the payment has been submitted, the Contractor will send a real-time response message accepting or declining the payment. The contents of the response message will include a unique confirmation number, date, dollar amount, authorization code (if credit card), application name, and customer information. The screen shall allow for current date and post-dated ACH payments. The screen shall also allow for editing of rejected payment requests so the user can make changes to fields containing errors or invalid information and re-submit the payment without re-entering the entire transaction.

PayPoint supports the ability for authorized users to make payments via our Administrative Web. Our New Payment option allows users to submit payments manually or using a card swipe through a Web interface. Users are provided with a payment results screen that includes the required information identified in this requirement. If a payment is not successful, the user is presented with an option to edit the payment information and re-submit it as many times as desired. A history of all failed payment attempts is stored for historical purposes including the reason for the failure.
When making ACH payments, the ability to enter a post-dated payment date is supported. In this case, the routing number is verified against the list of routing numbers from the Federal Reserve. Our system submits post-dated payments once a day for processing. Any negative activity is reported back on the payment. In addition, a notification is sent via email to the State and/or consumers of any failures in processing the payment successfully on its posting date.

B10. **Foreign Addresses:** The State of Michigan accepts credit card and ACH payments for various products and services. The State receives payments from customers with Non-U.S. addresses. To accommodate customers, the State requires a system that can accept Non-U.S. addresses. The following outlines the requirements:

A.) The Contractor's system must allow the collection of foreign addresses, including alphanumeric zip codes.

PayPoint supports foreign address information.

B.) The Contractor's system must have the capability to store the address as collected (including registered and scheduled payments).

Paypoint supports the capability to store foreign addresses as collected including registered and scheduled payments.

C.) The system must have the capability to process authorization requests and retain the approval codes. For transactions that receive a successful approval, the system must have the capability of settling the transactions to TSYS/ODFI. This would mean the system would need to identify transactions with foreign addresses at the time of settlement and change the fields to data acceptable to TSYS/ODFI prior to sending the files. For example, transactions with alphanumeric zip codes may need to be changed to all zeros.

PayPoint supports the ability to store approval codes associated with successful payments. The approval codes are stored as part of the Payment History detail for each payment. Our Payment History search allows users to view the approval code associated with historical payments.

PayPoint is certified with Total Systems Services, Inc. (TSYS). PayPoint has been successfully processing foreign addresses to TSYS since 2007.

D.) The system must provide the capability to research transactions that have foreign addresses and display the foreign address when the transaction is queried.

PayPoint supports Foreign Address information and this information is available in the detailed payment search results.

B11. **Credit/Debit Card Tasks**

Currently, the State accepts Visa, MasterCard, and Discover credit/debit cards. The Michigan Department of Treasury (Treasury) administers the credit card contracts and utilizes Bank of America as the depository bank for credit/debit card revenue. The State will use Fifth Third Processing Solutions as the merchant Acquirer. The Contractor must be capable of managing multiple State agency credit/debit card applications.

The Contractor shall provide the logic to capture the credit/debit card information and send the information to TSYS for authorization of the transaction. The transaction may be for corporate or consumer cards. The credit card transactions may be initiated through Internet, IVR (phone), fax, kiosk, mail, interface, point-of-sale devices, manual key entry, card swipe, and face to face. Both card-present and non card-present transactions will occur. Credit/Debit Card processing must be in compliance with Federal Regulation E, Merchant Operating Guides for the credit cards, Payment Card Industry Data Security Standards, and other regulations that may apply.

NOTE: Debit card (on-line) processing with pin number access authorization. System verifies funds are available and funds are withdrawn from the checking account instantly. This type of debit transaction can only be used in a card present situation where the merchant has a pin pad so the customer can key in his/her personal identification number (PIN). This type of transaction incurs lower merchant fees.

Debit card (off-line) processing. Acts like a credit card for authorization. Transaction verifies the account is active, funds requested are available and the card is not stolen or expired. The funds are debited from the checking account with a two or three day settlement period. This type of debit transaction can be used at any merchant that accepts Visa or MasterCard or Discover.

If Debit card (on-line) non-face-to-face (pinless debit) is available, the State may be interested in pursuing this option with a Contractor-provided solution.

The following is a list of requirements for credit/debit card transactions.
PayPoint supports the ability to process Credit Card, PINless Debit and PIN-based debit

A.) **Payment Methods:** The Contractor's system must accept the following payment methods:

a.) Credit and off-line debit card – Visa, MasterCard, and Discover processed through the credit card network. Credit Card processing supports Visa, MasterCard, Discover, and American Express credit/debit cards via our TSYS gateway.

b.) Debit Cards, PIN less – These transactions are processed through the debit card network. Debit Card (Off-Line) is supported for the STAR, PULSE, and NYSE networks via our BuyPass gateway.

c.) Debit Cards, on-line PIN based – Card present where the card holder is required to enter a PIN number and are processed through the debit network. Debit Card (On-Line) is supported for the STAR, PULSE, and NYSE networks via our TSYS gateway.

B.) **Payment Channels:** The payment will be single entry. The Contractor's system must have the ability to accept payments initiated by:

a.) Internet
b.) Interactive Voice Response Unit (IVR)
c.) Remittance Machine by batch
d.) Kiosk
e.) Manual Key Entry
f.) Point of Sale Device (e.g. credit/debit card terminal, wedge reader, card swipe keyboard, etc).
g.) Other Interfaces.

PayPoint meets the requirements (a through g) by providing open system-based API interfaces that can accept payments by Internet, IVR, Batch, Kiosk, Manually Keyed Entry, Point of Sale, and any other interface that supports either integration via Web Services or HTTPS protocols.

C.) **Capture Data:** The Contractor's system must capture and store the following:

a.) Credit/debit card number
b.) Expiration Date
c.) Customer Name

d.) Customer Billing Address
e.) Transaction date
f.) Settlement date
g.) Comments field (field Contractor provides for program to use for non-sensitive information that ties the payment to the programs legacy system. For example, invoice number or company ID.)
h.) Card Verification Value (CVV2), Card Validation Code (CVC2), Card Security Code (3CSC)
i.) All fields required to qualify for the best interchange rates as required by Visa, MasterCard, and Discover (e.g. sales tax, purchase ID, authorization code, E-Commerce indicator, etc.)
j.) Other data as required by Visa, MasterCard, and Discover.
k.) A shipping address if different from the billing address.

PayPoint supports all the required data capture elements (a through k) identified in these requirements. We provide up to 254 characters to store comments; however, in order to support wildcard searches, these comments are not encrypted. We do not prevent the integrating application from storing encrypted data.

D.) **Search Criteria:** With appropriate user access security (See Security Section), the Contractor's system must provide the ability for users to access, search and retrieve transaction information by utilizing individual or combinations of the following information:

a.) Customer Name

b.) Confirmation Number (unique number assigned to each transaction)

c.) Transaction Date (and date ranges)

d.) Amount

e.) Settlement Date (and date ranges)

f.) Comments field (field Contractor provides for program to use for non-sensitive information that ties the payment to the programs legacy system. For example, invoice number or company ID).

g.) Authorization Code

h.) Application Name/ID

i.) Agency Name

j.) Associations (multiple programs within an agency)

k.) Truncated Credit/Debit Card Number (e.g. Last 4 numbers)

l.) Payment Date (with a minimum search date range of 6 months of transaction data for a single search)

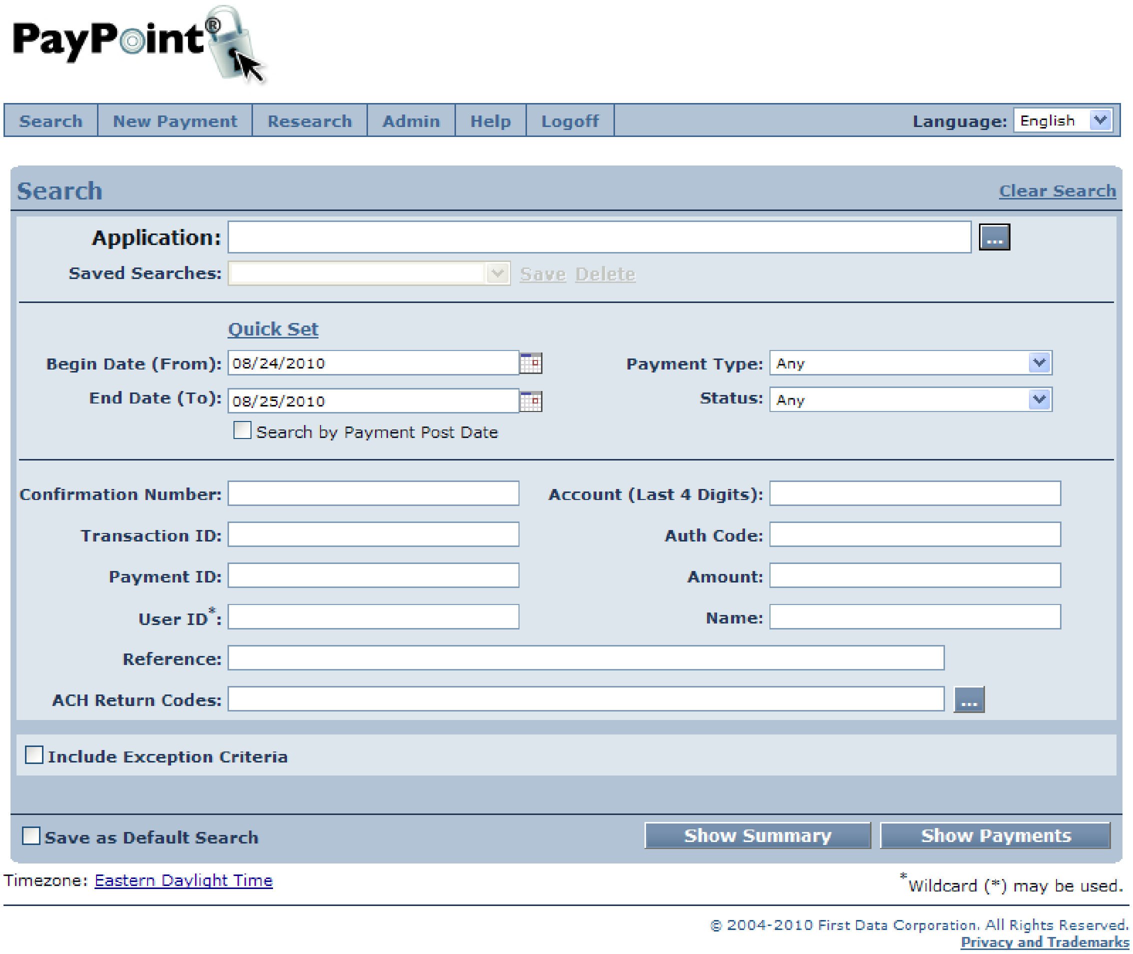
m.) Payment Status

The Contractors system must be capable of exporting search results in Excel or CSV format. The search function must allow a search date range of at least 3 months in a single search.

FDGS understands the State of Michigan's requests to have the ability to search payments up to three months in the past, and is looking to provide this ability as a future enhancement. Due to project and environmental constraints to provide this capability and capacity, First Data is unable to make a commitment on a delivery date for this enhancement, but is targeting an implementation date of August 2011.

PayPoint currently supports the search requirements detailed in a through m, with the exception of j (Associations). At this time, PayPoint provides the ability to search the hierarchy of Site, Agency, and Application, but not associations.

PayPoint currently supports the ability to search payment history by Customer Name, Confirmation Number, Transaction Date, Amount, Comments, Application, Agency, last four (4) numbers of the Credit/Debit Card Number, and Authorization Code. These search options, along with others, allow the ability to search using partial values (wildcard search), where appropriate. A sample of the PayPoint Search and Search Result screens are shown below:



Application:			
Saved Searches:			
Begin Date (From):	08/24/2010	Payment Type:	Any
End Date (To):	08/25/2010	Status:	Any
□ Search by Payment Post Date			
Confirmation Number:		Account (Last 4 Digits):	
Transaction ID:		Auth Code:	
Payment ID:		Amount:	
User ID*:		Name:	
Reference:			
ACH Return Codes:			

□ Include Exception Criteria

□ Save as Default Search

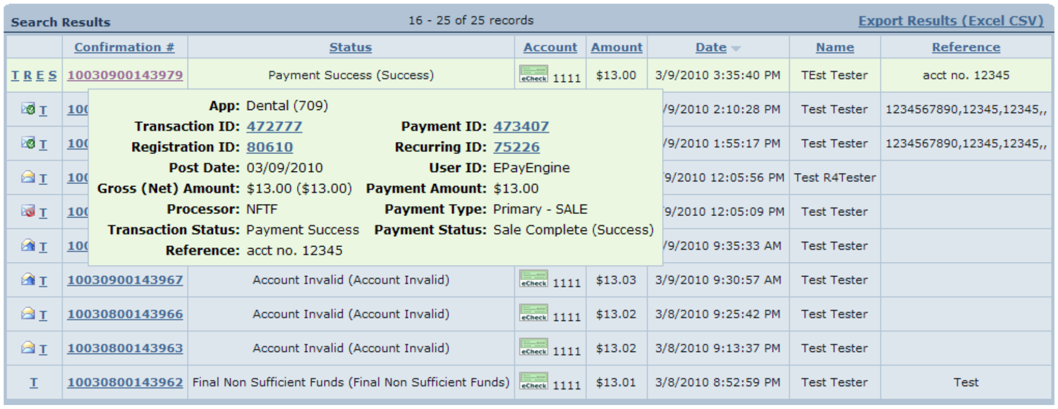
Timezone: Eastern Daylight Time

*Wildcard (*) may be used.

© 2004-2010 First Data Corporation. All Rights Reserved.
Privacy and Trademarks

Settlement Search Capabilities

PayPoint provides real-time authorizations for payments, and then performs a nightly settlement batch process to fund the accounts. The settlements can be searched for and limited based on specific search criteria. When the settlement results are displayed, the user will be able to quickly view the details such as the data/time stamp, settlement result, the count of payments included in the settlement, and the amount of the settlement. Three (3) settlement batches run each day – one for credit card, one for E-Check, and one for PINless debit.

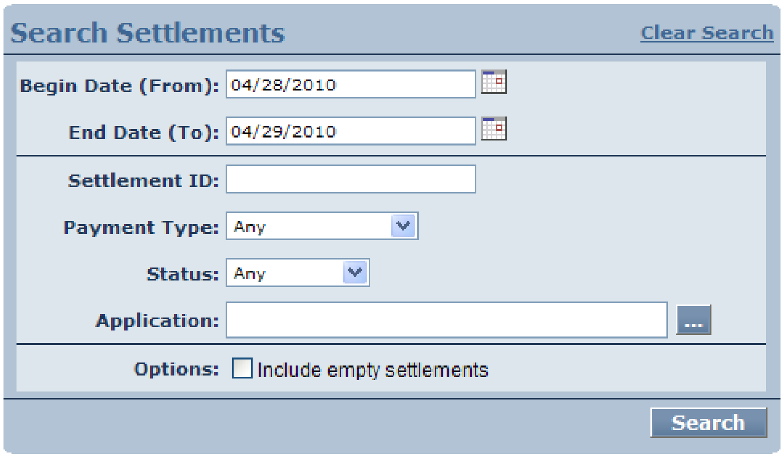


Search Results — 16 - 25 of 25 records

	Confirmation #	Status	Account	Amount	Date	Name	Reference
T R E S	10030900143979	Payment Success (Success)	1111	$13.00	3/9/2010 3:35:40 PM	TEst Tester	acct no. 12345
T	100				/9/2010 2:10:28 PM	Test Tester	1234567890,12345,12345,,
T	100				/9/2010 1:55:17 PM	Test Tester	1234567890,12345,12345,,
T	100				/9/2010 12:05:56 PM	Test R4Tester	
T	100				/9/2010 12:05:09 PM	Test Tester	
T	100				/9/2010 9:35:33 AM	Test Tester	
T	10030900143967	Account Invalid (Account Invalid)	1111	$13.03	3/9/2010 9:30:57 AM	Test Tester	
T	10030800143966	Account Invalid (Account Invalid)	1111	$13.02	3/8/2010 9:25:42 PM	Test Tester	
T	10030800143963	Account Invalid (Account Invalid)	1111	$13.02	3/8/2010 9:13:37 PM	Test Tester	
T	10030800143962	Final Non Sufficient Funds (Final Non Sufficient Funds)	1111	$13.01	3/8/2010 8:52:59 PM	Test Tester	Test

App:	Dental (709)		
Transaction ID:	472777	Payment ID:	473407
Registration ID:	80610	Recurring ID:	75226
Post Date:	03/09/2010	User ID:	EPayEngine
Gross (Net) Amount:	$13.00 ($13.00)	Payment Amount:	$13.00
Processor:	NFTF	Payment Type:	Primary - SALE
Transaction Status:	Payment Success	Payment Status:	Sale Complete (Success)
Reference:	acct no. 12345		

Settlement Search Screen:



Search Settlements

Begin Date (From): 04/28/2010

End Date (To): 04/29/2010

Settlement ID:

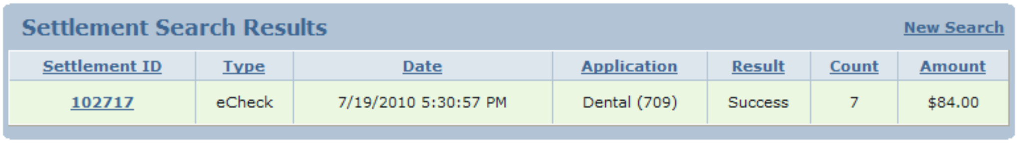
Payment Type: Any

Status: Any

Application:

Options: □ Include empty settlements

Settlement Search Result Screen:

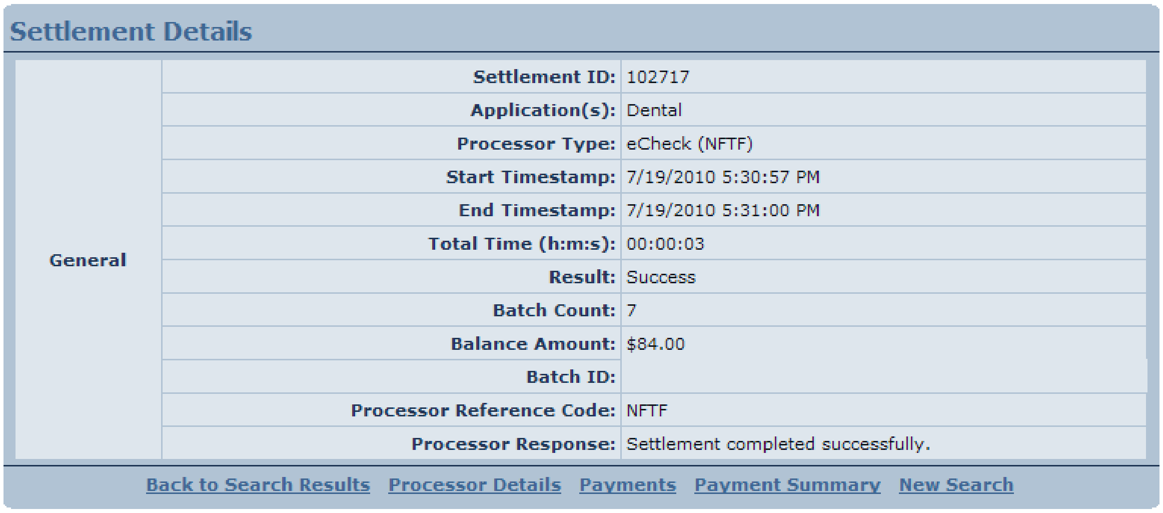


Settlement Search Results

Settlement ID	Type	Date	Application	Result	Count	Amount
102717	eCheck	7/19/2010 5:30:57 PM	Dental (709)	Success	7	$84.00

By selecting the specific Settlement ID, more details are available to the administrator. These details include the ability to see a listing of the specific payments that are included in the settlement job, in addition to a summary view of the payments. Should further details need to be examined with one of the individual payments; the user can click on the payment confirmation number to pull up the full payment details.

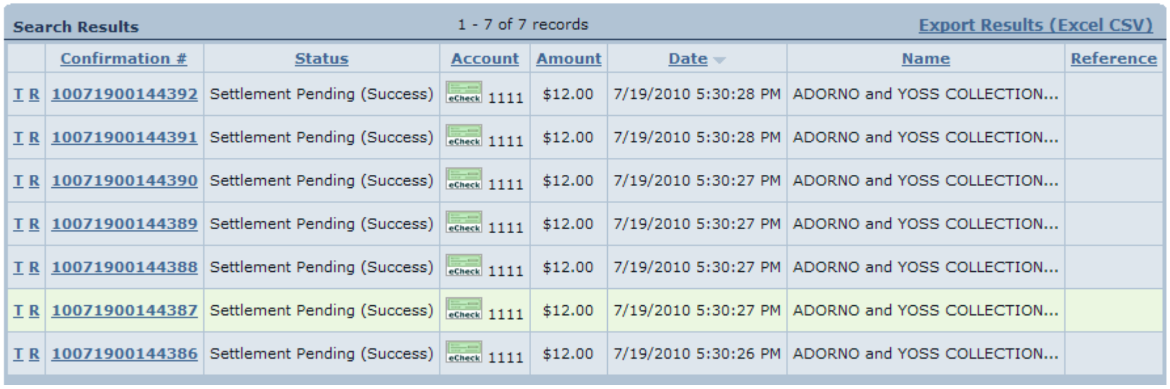
General Settlement Details Screen



Settlement Details

General	Settlement ID:	102717
	Application(s):	Dental
	Processor Type:	eCheck (NFTF)
	Start Timestamp:	7/19/2010 5:30:57 PM
	End Timestamp:	7/19/2010 5:31:00 PM
	Total Time (h:m:s):	00:00:03
	Result:	Success
	Batch Count:	7
	Balance Amount:	$84.00
	Batch ID:	
	Processor Reference Code:	NFTF
	Processor Response:	Settlement completed successfully.

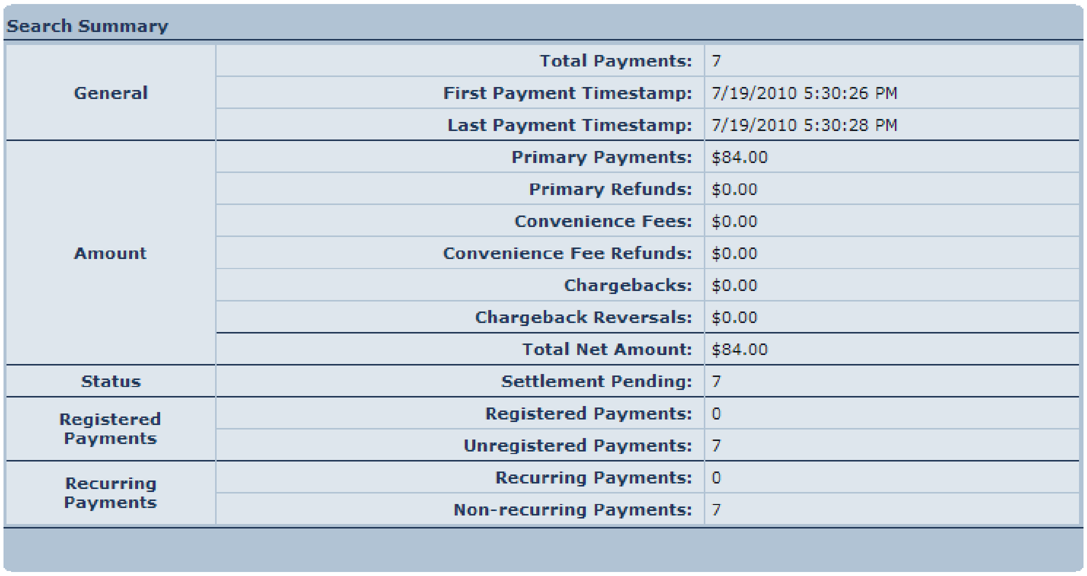
Settlement Payments Screen



Search Results 1 - 7 of 7 records Export Results (Excel CSV)

	Confirmation #	Status	Account	Amount	Date	Name	Reference
T R	10071900144392	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:28 PM	ADORNO and YOSS COLLECTION...	
T R	10071900144391	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:28 PM	ADORNO and YOSS COLLECTION...	
T R	10071900144390	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:27 PM	ADORNO and YOSS COLLECTION...	
T R	10071900144389	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:27 PM	ADORNO and YOSS COLLECTION...	
T R	10071900144388	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:27 PM	ADORNO and YOSS COLLECTION...	
T R	10071900144387	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:27 PM	ADORNO and YOSS COLLECTION...	
T R	10071900144386	Settlement Pending (Success)	eCheck 1111	$12.00	7/19/2010 5:30:26 PM	ADORNO and YOSS COLLECTION...	

Settlement Payment Summary Screen:



Search Summary

General	Total Payments:	7
	First Payment Timestamp:	7/19/2010 5:30:26 PM
	Last Payment Timestamp:	7/19/2010 5:30:28 PM
Amount	Primary Payments:	$84.00
	Primary Refunds:	$0.00
	Convenience Fees:	$0.00
	Convenience Fee Refunds:	$0.00
	Chargebacks:	$0.00
	Chargeback Reversals:	$0.00
	Total Net Amount:	$84.00
Status	Settlement Pending:	7
Registered Payments	Registered Payments:	0
	Unregistered Payments:	7
Recurring Payments	Recurring Payments:	0
	Non-recurring Payments:	7

Payment search results can be exported in csv format to Excel.

Currently, PayPoint supports a duration of 32 days for Payment Details searches and 65 days for Payment Summaries. PayPoint is undergoing on-going performance improvements efforts and will consider the three-month requirement as a future enhancement.

E.) **<u>Transaction Detail</u>:** The Contractor’s system must display details of the processed transactions. Details must include (but not limited to):

a.) Truncated Credit/Debit Card Number (e.g. Last 4 numbers)
b.) Card Expiration Date
c.) Amount (Original sale and subsequent refund(s))
d.) Transaction date
e.) Authorization Code
f.) Issuer response to Authorization
g.) Address Verification Response code (If applicable)
h.) CVV2/CVC2/CID Response code (If applicable)
i.) Invoice/Purchase ID
j.) Time authorization request sent to TSYS (available in Eastern Time)
k.) Time authorization response received from TSYS (available in Eastern Time)
l.) Payment time stamp (available in Eastern Time)
m.) Confirmation Number (unique number assigned to each transaction)
n.) Status of payment (Approved, Declined, Settled, etc.)

o.) Customer Name (if collected)
p.) Customer Address (if collected)
q.) Settlement Date
r.) Agency name
s.) Application/Merchant Name
t.) Other fields required by Visa, MasterCard, and Discover.
u.) Comments field (field Contractor provides for program to use for non-sensitive information that ties the payment to the programs legacy system. For example, invoice number or company id.)
v.) Customer Phone Number (if collected)
w.) Customer Email Address (if collected)
x.) Shipping address, if different from billing address
y.) Association

PayPoint currently displays the following requirements listed in this requirement:

a) Truncated Credit/Debit Card Number (i.e. Last four numbers)
b) Card Expiration Date
c) Amount (Original sale and subsequent refund(s)
d) Transaction date
e) Authorization Code
f) Issuer response to Authorization
g) Address Verification Response code (If applicable)
h) CVV2/CVC2/CID Response code (If applicable)
i) Invoice/Purchase ID
j) Time authorization request sent to TSYS
k) Time authorization response received from TSYS
l) Payment time stamp (in Eastern Time)
m) Confirmation Number (unique number assigned to each transaction)
n) Status of payment (Approved, Declined, Settled, etc.)
o) Customer Name (if collected)
p) Customer Address (if collected)
q) Settlement Date
r) Agency name
s) Application/Merchant Name
t) Other fields required by Visa, MasterCard, Discover, and American Express.
u) Comments field (field Vendor provides for program to use for non-sensitive information that ties the payment to the programs legacy system. For example, invoice number or company id.)
v) Customer Phone Number (if collected)
w) Customer Email Address (if collected)
x) Shipping address, if different from billing address

The following element will not be available within PayPoint's product:

Association – PayPoint currently supports payment categorization by Site, Agency, and Application. The State may name the application in a way that shows what Association it has, but it is not possible to create a fourth tier within PayPoint to provide a unique element to represent the Association.

F.) **Authorizations:** The Contractor's system must provide the ability for on-line real time authorizations and also must allow for batch authorizations as dictated by the application (e.g. Remittance processing equipment uses a batch authorization process).

PayPoint supports batch payment authorizations. Batch files are submitted in a pre-defined XML format, which is documented in our Merchant Integration Guide . Files delivered before 12:00 AM EST are processed by 6:00 AM EST. A standardized XML response file is picked up at that time to view and process the results of the authorizations processed in the batch, including success/failure indicators and confirmation numbers.

1. The authorization process must be capable of running unimpeded concurrently with the settlement process.

   Settlement processing is independent and has no impact on the ability for real-time payments to be processed at the same time a settlement job is running.

2. Authorization requests must be returned in 3 seconds or less.

   PayPoint processes payments within with an average time of under three (3) seconds; however, we cannot guarantee the timing of third party gateways, such as TSYS, when processing an authorization.

G.) **Cancellation/Void:** The Contractor's system must provide the ability to cancel or void the transaction prior to settlement. The Contractor's system will process authorization reversals for transactions voided in the same day.

PayPoint fully supports the ability to cancel or void transactions prior to settlement via real-time API capabilities or via our Administrative Web interface for users with appropriate rights to perform cancellations.

H.) **Refunds:** The Contractor's system must have the ability to process full and partial refunds for credit/debit card transactions with appropriate agency on-line approvals and limited user access. The Contractor's system will ensure that the refund amount does not exceed the original payment amount.

PayPoint fully supports the ability to process full and partial refunds. These refunds are processed via our real-time API capabilities or via our Administrative Web interface for users with the appropriate rights to perform cancellations. As part of normal processing, PayPoint does not allow a payment to be refunded for more than its original payment value.

1. The Contractor's system must have the ability to process refunds on expired cards without requiring the user to input a valid expiration date.

PayPoint supports the ability to process refunds on expired cards without requiring the user to input a valid expiration date. For merchants that use BuyPass, PayPoint 2.5 Hotfix 5 is adding the feature to require an updated expiration date. However, this will not apply to TSYS Vital payments because of previous requirements identified by Michigan. PayPoint fully supports this requirement today and will support this with payments through TSYS Vital in the future.

2. The Contractor's system will only allow refunds of previously processed transactions.

PayPoint only allows refunds on previously successful payments with a valid authorization code for the processor.

3. If the State changes Acquirers, the Contractor's system must be capable of processing refunds on sales processed under a different merchant number and Acquirer.

PayPoint supports the ability to process refunds through TSYS on sales processed under a different merchant number and Acquirer.

I.) **Card Present Transactions:** The Contractor's system must have the ability to process card present transactions where the card is swiped through a card reader (e.g. credit/debit card terminal, wedge reader, card swipe keyboard, etc).

The State application, which is sending payments via our real-time API, only needs to be able to support our open-standard API Web Service or HTTPS interface. Our Real-time API supports passing any track data received in the transaction onto the Processor.

Ad-hoc payments are made through our Administrative Web interface for users with appropriate rights. This includes the ability to utilize a wedge reader or card swipe keyboard attached to the terminal, which is logged into the PayPoint Administrative Web.

1. The Contractor's system must have safeguards that limit the fields allowed to be populated with the contents of the card's magnetic strip. For example, on a Contractor's key entry screen that allows a State employee to enter payment information, the contents of the magnetic strip should not be allowed in any other fields except the field dedicated for capture of magnetic strip data.

   PayPoint's Administrative Web interface supports the ability for users with appropriate rights to make Ad Hoc payments. This interface supports the ability to tab to a Track Data field where swiped track data is captured to automatically fill card information on the payment screen. We do not currently support the ability for the user to swipe the data anywhere on that screen. The user must be positioned on the Track Data field prior to swiping the card through a keyboard or wedge reader.

J.) **Customer Receipt:** The Contractor's system must provide a confirmation number, settlement date, amount, authorization code and other data as required by the credit card companies in order for the agency application to provide the data back to the customer to act as a receipt. The Contractor must provide the ability to create a receipt for transactions processed through the manual key-entry screen.

PayPoint supplies the required data, including payment receipts for ad-hoc payments made through the PayPoint Administrative payment interface. PayPoint has the ability to re-produce a payment receipt on any historical payment.

K.) **Association and Merchant Number:** The Contractor's system must capture and store the merchant number and association number. Association can be defined as a sub-set of agency, similar to a Region or group of merchants.

Example –

Agency – Department of Natural Resources

Association – Park Field Offices

Merchant – Algonac Park

Merchant – Hartwick Park

Association – Waterways/Docks

Merchant – East Tawas

Merchant – Port Austin

PayPoint currently supports a hierarchy of three (3) levels of categories associated with a payment. These levels include Site, Agency, and Application. The State does have control over how the application is named and can create as many applications as necessary to meet their Association needs. In addition, we support production of reports by multiple application groupings that may represent an Association.

If the State requires a physical layer in the hierarchy to represent Association, PayPoint cannot support this.

L.) **Settlement:** The Contractor's system must provide the ability to establish and change daily cut off times in order to meet the State's Credit Card Processor's settlement times for the State to get the lowest interchange and transaction rates available through the credit card companies and maximize the State's cash flow for timely deposit of funds.

PayPoint supports the ability to define a payment cut-off time on an Application-by-Application basis. Our Settlement system settles only transactions received on or before the settlement time identified in the application's configuration.

1. Contractor's system must allow for settlement seven (7) days a week.

   PayPoint supports settlement seven (7) days per week.

2. The Contractor's system must collect all transactions processed up to the State's established settlement cut-off and send the transactions (in Batch form) to TSYS. Transactions processed after the established settlement cut-off time will be held until the next day's settlement. For example: If the State's settlement cut-off time were 11:59 p.m. ET, the settlement batch would contain transactions processed from 12:00 a.m. ET. to 11:59 p.m. ET.

   The PayPoint solution currently supports these requirements for the State and will continue to support this requirement.

3. The Contractor will settle one batch per merchant/program to TSYS daily at the settlement time established by the State.

   PayPoint supports settlement times established per merchant/program to TSYS on a daily basis.

4. The Contractor will have edits/internal controls in place to ensure transactions are settled/processed accurately (e.g. correct card #, merchant/program, amount, etc.) and timely (daily at State's established settlement cut-off).

   PayPoint's settlement system has edits/internal controls in place to make sure that only successfully authorized transactions are included in a settlement batch. After submission of a batch, PayPoint validates the results of the batch received from the process and automatically compares the results with information submitted in the batch. Discrepancies are audited and alert our 7x24 monitoring staff who are able to work with the processor to determine cause of the discrepancy and make appropriate adjustments, as necessary.

   Settlements are executed at the times specified by the State.

5. The Contractor must process the required transaction data in the required time frames to Visa, MasterCard, and Discover in order for the State to receive the lowest applicable interchange (processing fee) rate.
   If the Contractor fails to meet the requirements for the State to receive the lowest interchange rate, the Contractor will be responsible for reimbursing the State for the difference between the lowest applicable interchange rate and the downgraded rate and any fines that may apply.
   Interchange reimbursement(s) will be credited to the State's monthly invoice.
   The Contractor must correct the problem(s) within 48 hours of notification of such inaccuracies.

   First Data Government Solutions understands the State's desire to receive the best possible rate on their transactions. Our settlement is executed at the time and days identified by the State. PayPoint has built in auditing and alerting mechanism to alert 7X24 Operational staff of any delays or errors in processing settlement. First Data Government Solutions' staff will work immediately on resolution of any problems, and will make every best effort to resolve all issues within 48 hours. Should delays occur that are under the control of FDGS, we will adhere to the agreed upon Service Level Agreements.

M.) **Fraud Prevention:** The Contractor's system must provide the ability to use Address Verification Service (AVS), Card Verification Value (CVV2), Card Validation Code (CVC2), Cardholder ID (CID) and other fraud prevention tools as required or introduced by Visa, MasterCard, and Discover.

PayPoint currently supports AVS, CVV2, CVC2, CID, and 3SCS.

PayPoint does not currently support Verified by Visa or MasterCard SecureCode.

N.) **End-to-End Encryption:** The State is considering utilizing End-to-End Encryption (E2E) for its Point of Sale (POS) devices in order to minimize Payment Card Industry Data Security Standard (PCI DSS) exposure.

The Department of State currently has approximately 1,200 POS devices that are located in branch offices throughout the state that process transactions through CEPAS. The Department of Natural

Resources park locations may also be included at a later date. The solution must be capable of processing with TSYS. For information purposes only, please provide a list of other payment gateways that are certified on your platform.

The contractor can partner with a third party to provide an E2E solution.

Providing end-to-end encryption capabilities will require further discussion between the State and First Data Government Solutions. Further information detailing the POS devices and requirements of TSYS will need to be researched and evaluated before specifics, time frames, and costs could be provided.

A.) Estimated time frame to implement an E2E solution.
Please see response at the end of question N.

B.) Estimated cost to implement an E2E solution with a detailed breakdown of each implementation component, including equipment costs. The State reserves the right to purchase equipment separately from a different vendor.

Please see response at the end of question N.

C.) Type of encryption and why this type was selected.

Please see response at the end of question N.

D.) Describe the role Tokenization plays in the solution.

Please see response at the end of question N.

B12. **Automated Clearing House (ACH) Tasks:** The following tasks are related to ACH payment processing:

A.) **Payment Channels:** ACH debit transactions will be initiated through the Internet, IVR, and manual key entry. Other interfaces are possible in the future.

PayPoint supports ACH debit transactions from any interface capable of integrating with our open-standard Web Service or HTTPS API capabilities.

B.) **Search Criteria :** With appropriate user access security, users will have the ability to access or retrieve payment information by using:
a.) Customer Name
b.) Confirmation Number (unique number assigned each transaction)
c.) Transaction Date (when both initiated and processed and date ranges)
d.) Amount
e.) Settlement Date (and date ranges)
f.) Routing Transit Number (RTN) and truncated account number (ex. Last 4 digits)
g.) Comments Field data
h.) Statewide
i.) Agency
j.) Association
k.) Application
l.) Truncated account number only

All date range searches must be capable of searching at least 3 months of transaction data in a single search. The Contractors system must be capable of exporting search results in Excel or CSV format.

PayPoint supports the following search criteria, including the ability to search using wild card values where appropriate.

a) Customer Name
b) Confirmation Number (unique number assigned each transaction)
c) Transaction Date (when both initiated and processed and date ranges) d.) Amount
d) Settlement Date (and date ranges)
e) Truncated account number (ex. Last 4 digits)
f) Comments Field data
g) Statewide
h) Agency
i) Application
j) Truncated account number

PayPoint currently supports searching by Site, Agency or Application and cannot support the ability to add an Association level for searching

C.) **Search Capability:** The Contractors system will allow users with the appropriate access rights to search a minimum date range of 3 months in a single search.

When searching over date ranges, PayPoint supports the 32-day searches for Payment Details and 65 days for Payment Summaries. PayPoint is undergoing on-going performance improvements efforts and will consider the three-month requirement as a future enhancement.

FDGS understands the State of Michigan's requests to have the ability to search payments up to three months in the past, and is looking to provide this ability as a future enhancement. Due to project and environmental constraints to provide this capability and capacity, First Data is unable to make a commitment on a delivery date for this enhancement, but is targeting an implementation date of August 2011.

D.) **Transaction Detail:** The Contractor's system must display details of the processed transactions. Details must include (but not limited to):

a.) Truncated Account Number (e.g. Last 4 numbers)
b.) Amount (Original sale and subsequent refund(s))
c.) Transaction date
d.) Payment time stamp (in Eastern Time)
e.) Confirmation Number (unique number assigned to each transaction)
f.) Status of payment (Approved, Declined, Settled, etc.)
g.) Customer Name (if collected)
h.) Customer Address (if collected)
i.) Settlement Date
j.) Agency name
k.) Application/Merchant Name
l.) Comment field (field Contractor provides for program to use for non-sensitive information that ties the payment to the programs legacy system. For example, invoice number or purchase order number.)
m.) Customer Phone Number (if collected)
n.) Customer Email Address (if collected)
o.) Shipping address if different from billing address

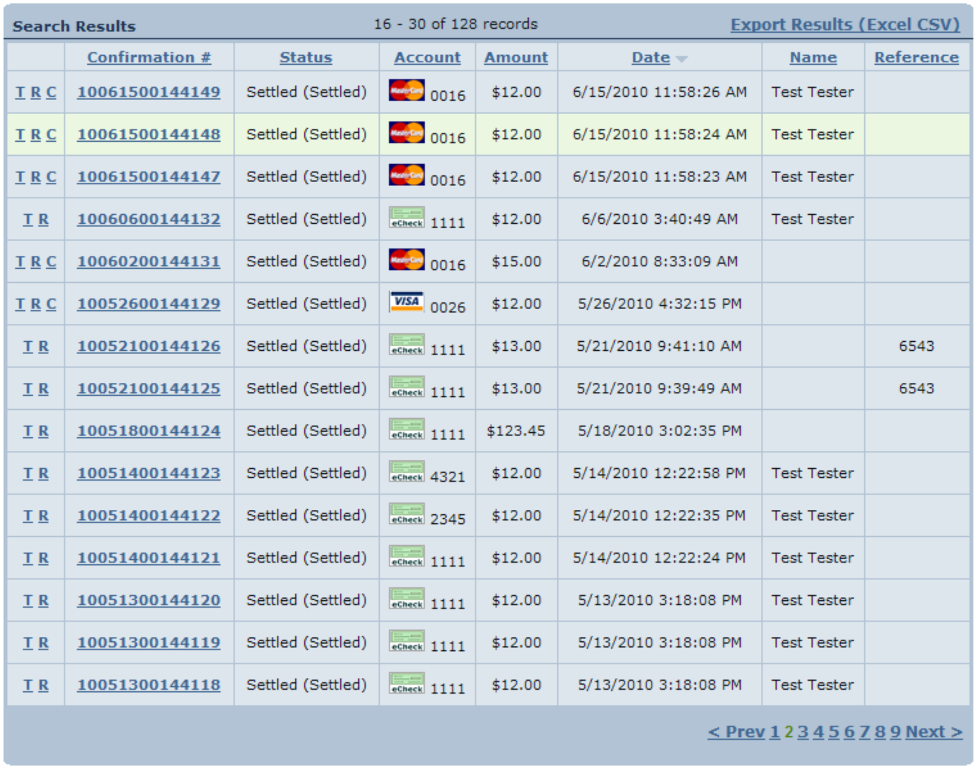
PayPoint currently display of the following requirements listed in this requirement:

a) Truncated Account Number (e.g. Last 4 numbers)
b) Amount (Original sale and subsequent refund(s))
c) Transaction date
d) Payment time stamp (in Eastern Time)
e) Confirmation Number (unique number assigned to each transaction)
f) Status of payment (Approved, Declined, Settled, etc.)
g) Customer Name (if collected)
h) Customer Address (if collected)

i) Settlement Date
j) Agency name
k) Application/Merchant Name
l) Comment field (field Vendor provides for program to use for non-sensitive information that ties the payment to the programs legacy system. For example, invoice number or company ID.)
m) Customer Phone Number (if collected)
n) Customer Email Address (if collected)
o) Shipping address, if different from billing address

Screen shots of the payment details provided by the Payment Search capabilities are shown below:

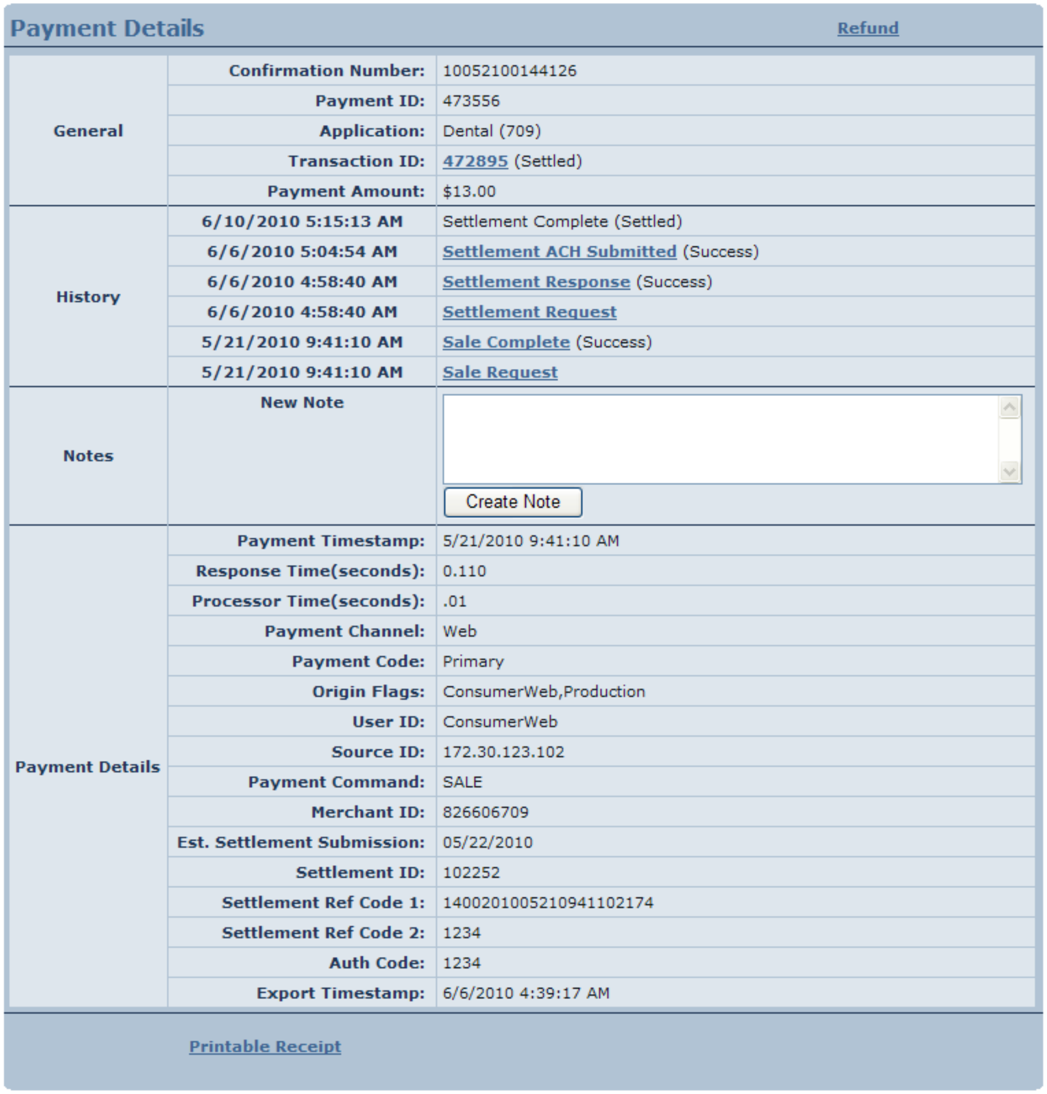
Show Payments View:



Search Results 16 - 30 of 128 records Export Results (Excel CSV)

	Confirmation #	Status	Account	Amount	Date	Name	Reference
T R C	10061500144149	Settled (Settled)	MasterCard 0016	$12.00	6/15/2010 11:58:26 AM	Test Tester	
T R C	10061500144148	Settled (Settled)	MasterCard 0016	$12.00	6/15/2010 11:58:24 AM	Test Tester	
T R C	10061500144147	Settled (Settled)	MasterCard 0016	$12.00	6/15/2010 11:58:23 AM	Test Tester	
T R	10060600144132	Settled (Settled)	eCheck 1111	$12.00	6/6/2010 3:40:49 AM	Test Tester	
T R C	10060200144131	Settled (Settled)	MasterCard 0016	$15.00	6/2/2010 8:33:09 AM		
T R C	10052600144129	Settled (Settled)	VISA 0026	$12.00	5/26/2010 4:32:15 PM		
T R	10052100144126	Settled (Settled)	eCheck 1111	$13.00	5/21/2010 9:41:10 AM		6543
T R	10052100144125	Settled (Settled)	eCheck 1111	$13.00	5/21/2010 9:39:49 AM		6543
T R	10051800144124	Settled (Settled)	eCheck 1111	$123.45	5/18/2010 3:02:35 PM		
T R	10051400144123	Settled (Settled)	eCheck 4321	$12.00	5/14/2010 12:22:58 PM	Test Tester	
T R	10051400144122	Settled (Settled)	eCheck 2345	$12.00	5/14/2010 12:22:35 PM	Test Tester	
T R	10051400144121	Settled (Settled)	eCheck 1111	$12.00	5/14/2010 12:22:24 PM	Test Tester	
T R	10051300144120	Settled (Settled)	eCheck 1111	$12.00	5/13/2010 3:18:08 PM	Test Tester	
T R	10051300144119	Settled (Settled)	eCheck 1111	$12.00	5/13/2010 3:18:08 PM	Test Tester	
T R	10051300144118	Settled (Settled)	eCheck 1111	$12.00	5/13/2010 3:18:08 PM	Test Tester	

Payment Detail Screen:



Payment Details

General	Confirmation Number:	10052100144126
	Payment ID:	473556
	Application:	Dental (709)
	Transaction ID:	472895 (Settled)
	Payment Amount:	$13.00
History	6/10/2010 5:15:13 AM	Settlement Complete (Settled)
	6/6/2010 5:04:54 AM	Settlement ACH Submitted (Success)
	6/6/2010 4:58:40 AM	Settlement Response (Success)
	6/6/2010 4:58:40 AM	Settlement Request
	5/21/2010 9:41:10 AM	Sale Complete (Success)
	5/21/2010 9:41:10 AM	Sale Request
Notes	New Note	
Payment Details	Payment Timestamp:	5/21/2010 9:41:10 AM
	Response Time(seconds):	0.110
	Processor Time(seconds):	.01
	Payment Channel:	Web
	Payment Code:	Primary
	Origin Flags:	ConsumerWeb,Production
	User ID:	ConsumerWeb
	Source ID:	172.30.123.102
	Payment Command:	SALE
	Merchant ID:	826606709
	Est. Settlement Submission:	05/22/2010
	Settlement ID:	102252
	Settlement Ref Code 1:	14002010052109411102174
	Settlement Ref Code 2:	1234
	Auth Code:	1234
	Export Timestamp:	6/6/2010 4:39:17 AM

E.) **<u>Verification of Routing Transit Numbers:</u>** The Contractor's system will have the ability to:

a.) Compare routing transit number at time of entry to an up-to-date accurate database (such as the Federal Reserve's) to verify if a routing transit number is valid.

b.) If not valid, provide a clear response to the on-line customer that the routing transit number is invalid and to enter the valid information or select another payment method.

c.) The customer should only have to reenter the invalid information.

First Data Government Solutions meets the requirements listed in objects a through c.

First Data Government Solutions supports validating the routing number against the Federal Reserve's list of valid routing numbers for post-dated payments and registered accounts. This list is updated electronically, on a daily basis, from the Federal Reserve. As an enhancement, PayPoint is adding the ability, in September, 2010, to also check for routing numbers for real-time payments. This will be a configuration setting on an Application, Agency, or Site level.

When using PayPoint's administrative interface, users are alerted when routing numbers do not match and have the ability to edit their transaction and resubmit. When editing payment details, the user is only required to update the elements that caused the error, such as a routing number.

F.) **Cancellations/Refunds:** The Contractor's system will have the ability to cancel previously initiated transactions prior to the settlement cut off time.

a.) After the settlement cut off time, the system will allow users with the appropriate security to refund either all or a portion of a previously settled transaction.
b.) Cancellations and refunds can be manually processed using the system's administrative screens and functionality or by utilizing a refund/cancel payment function through the API.
c.) The Contractor's system will limit the refund amount to the amount of the original transaction and refunds can only be issued on previously processed transactions.

First Data Government Solutions meets the requirements listed in objects a through c. PayPoint allows cancellations of previous, successful payment authorizations via its Real-time API interfaces, as well as through its Administrative Web interface for users with appropriate rights. As part of the normal processing rules, all refunds are limited to the value of the original payment.

G.) **Customer Receipt:** The payment response sent to the customer from the Contractor's system will contain the application name, customer name, transaction number (unique number assigned to each transaction), date, amount, authorization language, and allow the customer to print the response to act as a receipt for the transaction. The Contractor must also provide the ability to create a receipt for transactions processed through the manual key-entry screen.

PayPoint supports the ability to provide required feedback information to a payment request via a real-time API request and/or a payment processed manually through our Administrative Web. A user that issues payments via our Administrative Web site is presented with options to present a payment receipt, including reproduction of the receipt subsequent to the sale completion.

H.) **Cancel Pending Transactions:** The Contractor's system must allow State users, with the appropriate access rights, to access the system's administrative screens and cancel future dated ACH transactions that are being warehoused by the Contractor. The cancellation must take place prior to the transaction being processed for settlement.

First Data Government Solutions fully supports the ability to cancel a post-dated payment prior to settlement, as well as after settlement, via our Administrative Web Interface for users with appropriate rights.

I.) **Settlement:** The Contractor will submit files to the ODFI seven days a week.
a.) Separate Batches: At the designated settlement cut off time of 11:59 p.m. ET the Contractor's system will assemble the day's ACH transactions into one file with multiple batches in standard ACH format and forward to the Contractor's ODFI.

b.) The file will contain a separate batch for the ACH transactions for each State application.

c.) The Contractor's system must also have the ability to change daily cut off times in order to meet processing needs.

d.) The Contractor will have edits or internal controls in place to ensure transactions are settled/processed accurately and timely. The controls will also ensure that processed transactions are accurately reflected on the Contractor's system.

First Data Government Solutions meets the requirements listed in objects a through d.
PayPoint supports the ability to define settlement cut-off times on an application-by-application basis. Payments received prior to the cut-off are included in the batch for that day's settlement. Batches are generated by application. The cut-off time is changed on an application-by-application basis.
PayPoint's Settlement system has controls built-in that confirm the results of a settlement request, including validation of the payments included and the total amount of the ACH settlement. Should issues arise with the settlement, PayPoint has an audit and alerting system that notifies 7x24 operational staff of delay or discrepancy in settlement processing. This staff addresses the issue immediately

J.) **Application Identification:** The Contractor will collect information during application set up to populate the “Company Name” and “Company Entry Description” fields of the Batch Header of the standard NACHA ACH file. This information will be used to identify the State application and purpose of the ACH debit so it will appear on the customer’s bank statement.

First Data Government Solutions supports Company Name and Company Description, which are identified during the boarding process.

K.) **Prenotifications:** The State will not use prenotifications for ACH transactions processed under this contract. Although the State does not anticipate using prenotifications, the contractor may be required to generate prenotifications at a later date.

PayPoint does not support pre-notifications and that functionality is not currently scheduled for any of our future releases. If, at some point in the future, this functionality is required, First Data Government Solutions will have further conversations with the State to determine the possibility of adding this as an enhancement.

L.) **Standard Entry Class Codes:** The Contractor must use the appropriate NACHA Standard Entry Class Codes for ACH transactions processed under this contract. Indicate standard entry class codes believed to be applicable to the type of processing described in this section.

The following Standard Entry classes are used by our ACH solution: WEB, TEL, PPD, and CCD.

M.) **Legal and Rule Compliance:** The Contractor agrees that all processes related to ACH processing are in compliance with the NACHA Operating Rules, applicable State legislation, Federal Regulation E, and any other provisions of U.S. law and will remain in compliance throughout the contract term.

First Data Government Solutions agrees to process ACH in compliance with NACHA Operating Rules, applicable State legislation, Federal Regulation E, and other provisions of U.S law and remains in compliance.

N.) **Warehousing:** The Contractor will warehouse future dated transactions until one day prior to the settlement date. Warehousing of transactions will not exceed 365 days.

PayPoint supports the ability to warehouse payments up to 365 days. The State identifies the number of days to warehouse a payment on an application-by-application basis. Payments are issued for settlement on the settlement date defined at the time of payment receipt.

O.) **Originating Depository Financial Institution (ODFI):** The following tasks relate to the ODFI:

1.) The Contractor will provide for ODFI services to process ACH transactions under this contract. Any cost associated with the ODFI services are to be included in the per transaction fee price submitted in the Contractor’s price proposal.

First Data Government Solutions provides the ODFI services and cover any cost associated with the ODFI services.

2.) The Contractor is responsible for all costs associated with establishing a secure telecommunication connection with the ODFI to ensure information contained in the ACH files is safe from unauthorized access.

First Data Government Solutions covers cost associated with secure processing with its ODFI.

3.) The Contractor will originate ACH debit files on behalf of the State. The ODFI shall be responsible for transmitting/receiving files of ACH entries to/from the Contractor.

Our system is capable of submitting ACH files on behalf of the State. Our current ODFI is PNC, who is responsible for transmitting/receiving files of ACH entries to/from the systems.

4.) The Contractor will be the point-of-contact for questions and issues relating to the performance and daily operations of the ODFI. The Contractor is expected to provide detailed responses to routine questions relating to ODFI issues within 24 hours of the question being presented to the Contractor's designated contact. Emergency issues will require response within 30 minutes of the question being presented to the Contractor's designated contact.

Our customer service help desk is the main point of contact for all support of this solution, including issues related to performance or daily operation of our ODFI. This team is available via phone or email. All incoming issues will receive a response within one hour (or less), and will be worked according to established severity levels.

5.) The ODFI utilized by the Contractor must maintain a principal or branch office within the State of Michigan.

Our ODFI is PNC, which currently has branches in the State of Michigan.

6.) The Contractor shall create a separate batch for each State application in the daily ACH settlement file. At set up, each State application will provide the Contractor with a Routing Transit and Account Number for the ODFI to deposit the funds for the application's daily settlement. On the settlement/effective date of the transactions, the ODFI will credit the corresponding application's account for the total dollar value of its batch of transactions.

Our solution currently creates separate batches for each State application as part of settlement batch processing. These batches include the State Routing Transit and Account Number, which the ODFI uses to deposit the applications settlement funds on a daily basis for the total dollar value of each batch of transactions.

7.) The Contractor is responsible for ensuring that the ODFI is in full compliance with NACHA Operating Rules, including the requirement that the ODFI undergo an annual compliance audit. The Contractor must provide a copy of the ODFI's annual compliance audit results to the Project Manager or designee upon completion of each annual audit.

FDGS receives an annual SAS 70 report from the ODFI to ensure that they are in compliance with NACHA operating rules. Upon award of the contract, a copy of the ODFI's SAS 70 can be provided.

8.) The Contractor will provide complete and thorough documentation that describes the processing flow, unique processing rules, risk mitigation techniques, and set up requirements of the ODFI and/or any ACH processing partner.

Upon the awarding of this contract, First Data Government Solutions will provide documentation to the State.

P.) **Notification of Change (NOC):** NOCs shall be handled to ensure customer account information stored on the Contractor's database is corrected prior to processing the next live entry.

PayPoint's ACH payment gateway fully supports the management of NOCs. We have a special arrangement with our ODFI to manage NOCs on our behalf. They maintain a database of NOCs and correct entries prior to processing for any future entry.

Q.) **Return Entries:** ACH return entries shall be handled so that State agency application staff can access information daily on return entries received.

PayPoint reports any negative ACH activity, including returns to the State in its daily posting file. In addition, the State utilizes our Administrative Web Payment History options to search for returns. First Data Government Solutions PayPoint supports an ACH process that will provide specific return codes on returned transactions.

1. The Contractor is required to ensure that return entries are posted to the State agency application bank account individually and not as one total amount.

   First Data Government Solutions' PayPoint product supports Net and Gross Settlement.

2. The Contractor must allow entries that are returned for insufficient or uncollected funds to be reinitiated up to two times following the return of the original entry at no additional cost. The Contractor is responsible for the reinitiating of entries. Reinitiating of return entries will be optional at the discretion of each State application and communicated to the Contractor at application set up. Return entries must be processed timely to reduce the risk of additional ACH transactions being initiated to the same accounts.

   First Data Government Solutions supports the ability to reinitiate the payment up to two different times following the return of an original entry. On an application-by-application basis, the State determines if they want this feature enabled and how many different times they wish to reinitiate the original entry. Our system reinitiates returns on the same day the negative activity is received through our ODFI.

3. The State may require the Contractor to provide a process that generates an email to the customer to inform them of the return entry and provide information on how the customer can contact the application staff or resubmit payment.

   First Data Government Solutions supports a customer notification system for payments processed as recurring or post-dated payments. This feature is configurable on an application-by-application basis, including providing the ability to send notification for successful and/or failed payments; the State email address, a configurable subject line, email header message, and email footer.

   First Data Government Solutions also supports the capability to email a notification to consumers making ACH payments that are returned.

4. The Contractor must ensure that the actual return code that was received by the ODFI is presented on the Contractor's system. No consolidation of return codes is allowed.

   First Data Government Solutions PayPoint supports an ACH process that will provide specific return codes on returned transactions.

R.) **Guarantee Option:** The State may have agency applications that require that the Contractor guarantee ACH transactions. The guarantee service will require the Contractor, for a fee, to take on the risk associated with the transaction being returned. If a guarantee service is available provide an estimated cost associated with this service in Article 1, Attachment A, Price Proposal, Table 3.

We support an option that is enabled on an application-by-application basis for Warranty ACH transactions. First Data Government Solutions assumes the risk for a fee, which guarantees coverage of the payment obligation.

S.) **Timely Processing:** The Contractor must provide timely processing of ACH transactions. If the Contractor fails to meet the daily cutoff times, the Contractor will be responsible for reimbursing the State for the lost interest earnings on the transactions. Interest earnings will be calculated based upon the value of the total ACH transactions settled late, multiplied by the earnings credit rate earned by the State at Bank of America and the numbers of days lost in settling the transactions.

Interest reimbursements to the State will be credited to the State's monthly invoice.

The Contractor must correct the problem within 48 hours of notification of such inaccuracies.

First Data Government Solutions understands the State's desire to receive funds on a timely basis to ensure proper credit of interest. Our settlement is executed at the time and day identified by the State. PayPoint has built in auditing and alerting mechanism to alert 7X24 Operational staff of any delays or errors in processing settlement. Operational staff goes to work immediately on resolution of any problems. Should delays occur that are under our control, we discount the monthly statement for the difference in the lost interest associated with the payments. Further, we resolve issues within 48 hours.

T.) **Risk Settings:** The Contractor shall describe in detail any configurable risk or fraud detection processes that will impact ACH transactions processed through the Contractor's system. The state will have the right to require a configuration that results in the best processing environment for its applications.

Upon award of the contract, First Data Government Solutions will provide documentation on the risk or fraud detection systems available.

B13. **Registration, Scheduled, and Future Dated Transactions:** The Contractor's system must be capable of registering customers and securely storing customer credit card and bank account information. The system must also allow for scheduling and future dating of payments.

PayPoint supports the ability to receive and store registrations that uniquely represent a consumer and for each unique account. PayPoint returns a unique registration id, which is used to retrieve, view, update, or delete the consumer's account information through our real-time API interface. When making payments, this unique registration number is passed to PayPoint on the payment request.
PayPoint also supports the ability to schedule payments on a variety of types of schedules such as daily, specific days of month, monthly, bi-monthly, yearly, etc.
While we have the capability of managing registrations and recurring payment processing, our solution assumes that the integrating application provides the interfaces to request registration and recurring payment information.

A.) **Registration Process:** The Contractor will provide APIs and other functionality that will allow State customers to setup financial accounts and schedule payments. To create a registration the State application will authenticate customers and securely pass registration information to the Contractor's system. The Contractor's system will create a registered account and pass back a unique identifier to the State application. The Contractor's system will securely store customer account data. The unique identifier will relate to the financial accounts stored in the Contractor's database. Customers will also have the capability to update or delete a previously established registered account.

First Data Government Solutions will provide an HTTPS-based API interface that allows State application to integrate payment execution through our Enrollment system. The calling application will have to pass key information associated with their specific payment, such as application identifiers, password, payment amount, and reference data, to the enrollment system for use in the payment process. In addition, the calling application will have to identify a response URL in which the users will be redirected back to their application upon completion of the payment process through our enrollment system. Users will be redirected to the PayPoint enrollment site to create (for first time users) or authenticate (for existing users) themselves within the enrollment site. Once in, they will get through the Make Payment process described above. At the completion of the payment, we will redirect the user back to the State's application, along with the results of the payment process.

The following tasks relate to the registration process:

1. **Create Registered Accounts:** The customer will create registered accounts by accessing the State business application. After completing an authentication process they will provide bank account or credit card information and other information as required by the application and Contractor system. The Contractor will perform a preliminary edit of financial account information to identify and reject invalid Routing Transit Numbers, credit card numbers that do not pass check digit routines, have invalid expiration dates, etc. Failed/erred transactions will be communicated to the customer so they can enter again to correct. The Contractor system will securely store the registration information and provide a unique identifier to the State business application that corresponds to the customer's registration information. Customers may set up multiple registered accounts within each business application. Each will be identified with its own unique identifier. The business application will store the unique identifier(s) and associate it to the customer. When the customer logs in and chooses to make a registered payment, the business application will present a list of registered accounts. After the customer selects an account, the business application will include the unique identifier associated with the chosen registered account with its payment request sent to the Contractor's system. The Contractor will use the account information associated with the unique identifier to execute the payment.

   During the creation of registered accounts, First Data Government Solutions' Account Management performs edits on the credit card numbers and expiration dates to ensure they are valid card numbers and valid E-Check routing numbers (the Federal Reserve's latest routing number information at the time a consumer creates an account). Our Web interface clearly identifies any incorrect information and allows users to correct their information and re-attempt to save the account information. Accounts are not stored unless they pass our edits. Unique identifiers are associated with each account the user has on file. We provide the ability for a consumer to print-off all of their Account identifiers and information to keep as an offline record of their enrollment. Account numbers on this output display only the last four (4) digits of any account number.

2. **Registered Account Information:** The customers can set up both credit/debit (pin-less) card and ACH debit accounts in one registration session. The Contractor's system will allow customers to create, view, update, or delete financial and other registered data. For example, only the last four (4) digits of the account number will be displayed.

   Our solution supports the ability to store an unlimited number of accounts, or to restrict the number of accounts for each registration to meet the State's needs. This allows large business payers to manage any number of accounts they may use to pay State obligations. Each account is specific to the payment medium, such as Credit Card, PINless Debit, and e-Check. Account Management features are included to allow users to view, update, and delete accounts.

3. **State Business Application:** When the customer is accessing their account information through a State business application, the application will pass information identifying the application, the payment amount, and other required information to the Contractor's system. The Contractor's system will pass payment status information to the business application for presentation to the customer. Financial account information contained in the response must be truncated. The State business application will present a confirmation page to the customer.

   First Data Government Solutions provides a Consumer Payments interface that allows state applications to pass key information associated with their specific payment, such as payment amount and reference data to the Consumer Payments Web site. In addition, the calling application identifies a response URL in which the users are redirected back to their application upon successful completion of the payment process through Consumer Payments. Once in, they go through the Make Payment process described above. At the completion of the payment, we redirect the user back to the State's site along with the results of the payment process. Results contain confirmation number, payment amount, and reference data.

4. **Customer Notification:** The Contractor's system must be capable of sending an email notification to a registered customer 30 days in advance of their credit/debit (pin-less) card expiration date informing the customer that their registered card is about to expire.

   Currently, email notifications are not sent prior to a registered user's card expiration date. To accomplish this for future application deployments, custom development will need to be provided.

   FDGS will evaluate the requirements to enable this functionality and include this in our enhancement list for the PayPoint product.

5. **Inactive Accounts:** The Contractor's system will include the ability for State users to manually inactivate and enable previously registered accounts.

   PayPoint allows the ability to manually activate and inactivate recurring schedules. The individual user's registered payment account can be managed by the user, but is not accessible to the State's users.

   PayPoint supports the ability to delete, create and inactivate recurring schedules.

6. **Security:** The Contractor will ensure that financial data transmitted over the Internet will be encrypted using a minimum of 128-bit Secure Socket Layer (SSL) encryption. A minimum of 128-bit encryption will be used for storage of confidential information.

   The Enrollment site will enforce the use of SSL 128-bit encryption. In addition, all sensitive data, such as passwords and account numbers, will be encrypted within our backend database using 128-bit AES-compliant encryption.

7. **Agency Access:** The Contractor's system must allow agency staff, with the appropriate access rights, to view registration information and all payments generated from the customer's unique Registration ID. All credit card numbers and account numbers will be truncated. Only the last four (4) digits of the account number will be displayed.

   The agency staff will have access to our Administrative Enrollment system to view account information. Account information will be limited to the last four (4) digits

8. **Batch Registrations:** The Contractor will provide a batch interface process to allow for submission of a batch of customer data to create enrolled accounts. The process will include an initial edit of account data such as validating the RTN for ACH accounts and ensuring the credit card expiration date is valid. After assigning a Registration ID to each valid customer in the batch, the Contractor will provide a feedback file to the submitting agency application. The feedback file will contain the original customer data with the account number truncated (for example the last four (4) digits are displayed) along with the newly assigned Registration ID.

   First Data Government Solutions supports batch enrollment capabilities. PayPoint provides a unique enrollment id back to the State's application to provide batch data that could be uniquely matched to a consumer enrollment for the purpose of sending a batch.

9. **Notification of Change (NOCs) and Returns:** The Contractor is responsible for updating ACH account information prior to initiating a live transaction when an NOC is received for a registered account. When a Return is received, the Contractor will reinitiate returns for non-sufficient or uncollected funds (NSF) transactions if the agency application has selected a reinitiating option at set up. If the return is not eligible for reinitiating or the reinitiated entries fail, the Contractor will disable the registered account so it cannot be used for future transactions until the cause of the return has been resolved. State employees, with appropriate access, must be able to override the inactivation.

   PayPoint supports the management of accounts and Notification of Change information. For ACH payments that have been returned, PayPoint supports the ability to re-initiate these payments up to two (2) additional times. This functionality is configurable by application. Inactivation and reactivation of accounts can be manually performed through our Administrative Enrollment Web component; however, automated account inactivation on returned ACH transactions is not currently available. Upon the award of the contract, First Data Government Solutions will discuss and work with the State to determine requirements and establish plans for incorporating the automatic account inactivation needs.

FDGS will evaluate the requirements to enable this functionality and include this in our enhancement list for the PayPoint product.

10. **Migration Assistance:** The Contractor is required to assist with migration of State customers with registered and scheduled accounts from the existing Contractor. The existing Contractor will provide a file containing full credit card and bank information, application identification, registration ID, and any other information collected from the customer. The file will be transferred to the Contractor using a secure process. The timing of the migration and process to be used will be determined by the State during implementation. More than one file transfer may be necessary. The Contractor will map the information in the file to its registration database and supply new registration IDs and other required information to the appropriate agency applications to allow the agency applications to process enrolled transactions.

    Upon contract termination, FDGS will work with the State of Michigan to migrate all necessary information to the new contractor. Since each contractor's solution is unique and will require custom processes and effort, FDGS will handle this as a separate project using the hourly rate in Appendix A. This migration effort is not included in this contract pricing. Once the data has been transferred to the State, all applications, user accounts, and registrations will be purged from the PayPoint system upon written request from the State to delete and purge the information.

B.) **Scheduled Payments:** The Contractor must provide the capability for enrolled customers to schedule recurring payments. The identical payment amount will be initiated on a certain specified day at specified intervals. The Contractor's system must allow for daily, weekly, monthly, quarterly, and semi-annual intervals. Scheduled payments will be assigned a unique ID.

First Data Government Solutions' PayPoint has the ability to allow the user to schedule their payment as a recurring payment. Our API can provide optional instructions that identify if the payment is eligible for recurring payment processing, and potential recurrence patterns allowed (e.g. weekly, monthly, quarterly, semi-annually, annually).

The following tasks relate to Scheduled Payments:

1. **Agency Access:** The Contractor's system must allow agency staff, with the appropriate access rights, to view scheduled payment information and all scheduled payments generated from the customers scheduled payment ID. All credit card numbers and account numbers will be truncated. Agency staff must have the ability to reactivate disabled accounts.

   First Data Government Solutions' Enrollment system will provide an Administrative Web Interface for agency staff to view consumer enrollment information including general enrollment information, accounts, post dated payments, and recurring payment schedules. Administrative staff will have the ability to disable and enable enrollments, as well as recurring payment schedules. Payment sensitive information, such as credit card and ACH account numbers, will be truncated – showing only the last four (4) digits. Access to this functionality will be administered by the roles and permissions granted to the individual user.

2. **Update and Cancel:** The Contractor's system must allow the customer to access their scheduled payments through the Registration access processes using a User ID and Password and update or cancel scheduled payments prior to the transaction being picked up for settlement. Deadlines and timeframes for customers to update or cancel scheduled transactions will be clearly communicated to the customers during scheduled payment set up.

First Data Government Solutions provides Consumer Enrollment management features through its Consumer Enrollment site that will allow consumers to update and/or cancel post-dated payments or recurring schedules. Rules will exist to stop these actions on payments, which are about to or have already gone through submission.

3. **Automatic Disable:** The Contractor's system must be capable of being configured to automatically disable a scheduled payment if a specified number of consecutive payments have been returned.

   Automated account inactivation on returned ACH transactions is not currently available. Upon the award of the contract, First Data Government Solutions will discuss and work with the State to determine requirements and establish plans for incorporating the automatic account inactivation needs.

   FDGS will evaluate the requirements to enable this functionality and include this in our enhancement list for the PayPoint product.

C.) **Future Dated Payments:** The Contractor's system will allow customers to assign future dates to ACH debit transactions. The Contractor's system will warehouse the transaction until the appropriate date then automatically pick up and process the transaction for payment.

The following tasks are related to Future Dated Payments:

1. **Warehouse Limits:** The Contractor's system will limit warehousing of payment transactions to 365 days.

   The Enrollment system we have described is built on top of existing PayPoint functionality, which includes the ability to Warehouse payments for up to 365 days.

2. **ACH Only:** The Contractor will limit future dated payments to ACH debit transactions only. No future dated credit cards will be accepted at this time.

   PayPoint payment-processing functionality currently supports post-dated ACH debit transaction and will not allow posted-dated credit card transactions.

B14. **Customizable Generic Web and IVR Hosted Solution:** The Contractor will provide a Contractor hosted generic payment processing solution that is available through Web and Interactive Voice Response (IVR) channels. This solution will provide a customer facing front end interface to the Contractor's system functionality for agency units that desire an electronic payment capability but do not have the resources to build their own front end interface. The front end interface will be capable of customization to provide a seamless transition from the agency's website.

PayPoint supports Consumer Payments Web and IVR which provides customer facing front end interface for agency units that desire an electronic payment capability but do not have the resources to build their own front end interface. The agency can send data to the Consumer Payments site through query string integration.

A.) **Hosted Solution:** The Contractor's solution will be hosted by the Contractor at their highly secure, scalable, and redundant hosting facility. The solution will be fully monitored to detect and prevent security breaches.

PayPoint's Consumer Payments interface is hosted in First Data's data centers. These data centers (located in Denver, CO and Omaha, NE) provide a secure and scalable environment with disaster recovery capabilities. Security in our data centers is paramount and critical to First Data and the PayPoint product. They are managed and monitored through three (3) components: Physical Security, Environmental Security, and Data Security.

Physical Security – Our data centers are C2 compliant. They have security guards staffed 24-hours a day, seven (7)-days a week to monitor the facility. Visitor access is restricted, access cards are needed for entrance, and video monitors record activity in and around the data centers.

Environmental Security – Each of the data centers are engineered to withstand local natural disasters and provide redundant electrical and mechanical systems.

Data Security - Users are only given access to servers and data as it is required to fulfill their job requirements. Systems and processes are constantly monitored to ensure everything is functioning as expected.

B.) **Payment Methods:** The solution will support collecting payments via all major credit cards, E-Check, and PINless Debit.

Consumer Payments supports collecting payments via all major credit cards, E-Check, and PINless Debit.

C.) **Branding and Customization:** The Contractor's solution will provide a design toolkit that will allow State staff to customize the generic web pages to mimic the look of agency home websites. The solution must provide user friendly URLs, a toll free telephone number for the IVR, custom web styling and page content, and integration with custom data collection.

PayPoint Consumer Payments includes a design toolkit that allows State staff to customize the generic Web pages to mimic the look of Agency home Web sites. The solution must provide user-friendly URLs, a toll free telephone number for the IVR, custom Web styling and page content, and integration with custom data collection.

D.) **Registered and Scheduled Payments:** The Contractor's solution will include functionality to allow customers to set up registered accounts and schedule payments.

PayPoint Consumer Payments includes functionality to allow customers to setup registered accounts and schedule payments.

E.) **Data Management:** The Contractor's solution will accept custom data sent real-time through query strings from the agency home website or from files sent through the web or batch. The data management component must include the capability to create and update data requirements, upload data files through the Contractor's website, delete data, and search the data. Data will be used to authenticate customers and display custom information on the Web screen.

PayPoint Consumer Payments will accept custom data sent real-time through query strings from the Agency home Web site, or from files sent through the Web or by batch. The Data Management component includes the capability to create and update data requirements, upload data files through the Contractor's Web site, and search and delete data. Data can be used to authenticate customers and display custom information on the Web screen.

F.) **IVR Features:** The Contractor will provide a toll-free telephone number for customer use. The IVR will only be used by non-registered customers to make payments.

PayPoint Consumer Payments will provide a toll-free telephone number for customer use. PayPoint Consumer Payments IVR only supports payments from non-registered customers.

G.) **Website Connection Options:** The Contractor's solution must allow customers to utilize friendly URLs to connect directly to the agency application hosted on the Contractor's system. Customers will also be able to be redirected from the agency home web page. The solution will also provide the capability to use advanced query strings to exchange customer specific data between the agency application hosted by the Contractor and the agency home web page.

PayPoint Consumer Payments allows customers to utilize friendly URLs to connect directly to the Agency application, hosted on the FDGS system. Customers will also be able to be redirected from the Agency home Web page. The solution provides the capability to use advanced query strings to exchange customer-specific data between the Agency application hosted by the Contractor and the Agency home Web page.

H.) **Pricing:** Separate per item fees will be charged for transactions processed through the hosted solution. See Table 4 of Article 1, Attachment A, Price Proposal. The Contractor is expected to enter a separate per item fee for utilizing the solution. This is in addition to the transaction fee in Table 1 of Article 1, Attachment A, Price Proposal. Also the Contractor will enter separate additional per item fees for utilizing other functions of the solution (Authentication data, Registration, IVR). This method of pricing is being used so that the cost of using the Customizable Web and IVR Solution and its different functions are charged to those agencies that require this service instead of being spread across all CEPAS users.

In the best interest of presenting a response to the State that is environmentally friendly, First Data Government Solutions has included a link*, below, to the current PayPoint documentation requested, housed in eRoom (Log-in: paypoint; Password: paypoint).

https://eroom.fdgs.com/eRoom/Projects-Active/FDGSPaypoint/0_35f12

The documents for the State's review include: Consumer Payments Integration Guide, PayPoint Merchant Integration Guide, and the PayPoint User Guide.

These Guides will also be included on the accompanying CDs.

C. SECURITY CONTROL REQUIREMENTS

On award of the contract, the Contractor shall comply with State and Federal statutory and regulatory requirements, and rules; Payment Card Industry (PCI) Data Security Standards; all other industry specific standards; National Institute of Standards and Technology (NIST) publications; Control Objectives for Information and Related Technology (COBIT); national security best practices and all requirements herein.

The Contractor must perform annual testing of all security control requirements to determine they are working as intended. Annual certification must be provided in writing to the Project Manager or designee in the form of a SAS70 report. Additionally, PCI compliance must be reported quarterly.

As the incumbent vendor, our solution meets this requirement. First Data Government Solutions undergoes regular audits and certifications for the Credit Card and NACHA transactions. A SAS70 security report can be provided to the State, upon request, that details the results of the most recent audit, performed by Ernst and Young, LLP. The PCI Certification will be provided to the State upon request.

C1. Management Controls

A.) **Security Risk Assessment**

The assessment of potential risks and the type of risk (personnel, equipment, customer, logistics, or organization) are imperative throughout the project. The security risk assessment is a tool used by the State of Michigan, Departments of Information Technology and Treasury to identify risks and determine mitigation strategies to reduce that risk or completely eliminate it. Controls should be based on the potential risks.

1. The Contractor will be required to conduct assessments of risks and identify the damage that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the state. The Contractor shall ensure that reassessments occur whenever there are significant modifications to the information system and that risk assessment information is updated.

2. The Contractor must have a documented risk assessment policy and procedure. The policies and procedures must be consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance.

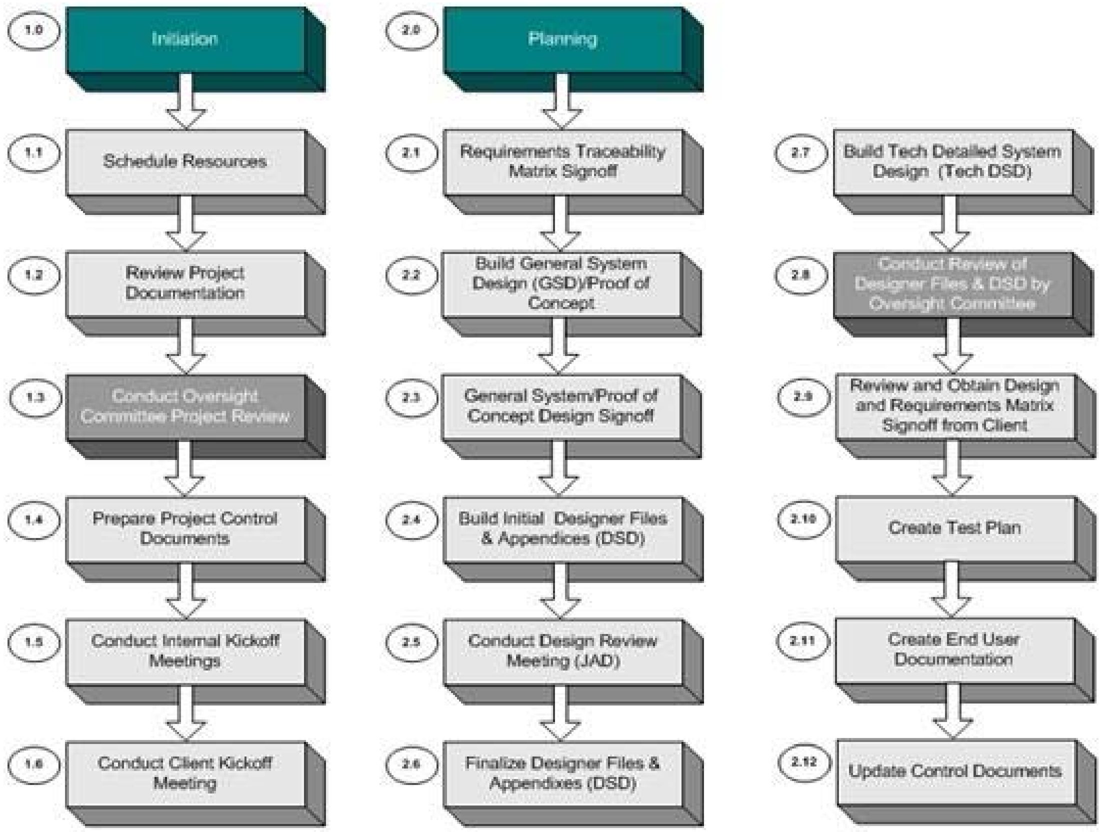
As the incumbent provider, First Data Government Solutions currently has the processes and procedures in place and will continue to meet the State's requirement. The First Data Corporation (FDC) Security Assessment Center maintains an assessment methodology as a basis for performing evaluations of the security posture of selected FDC Web-based points of presence. These assessments are performed in addition to the SAS70 audits.

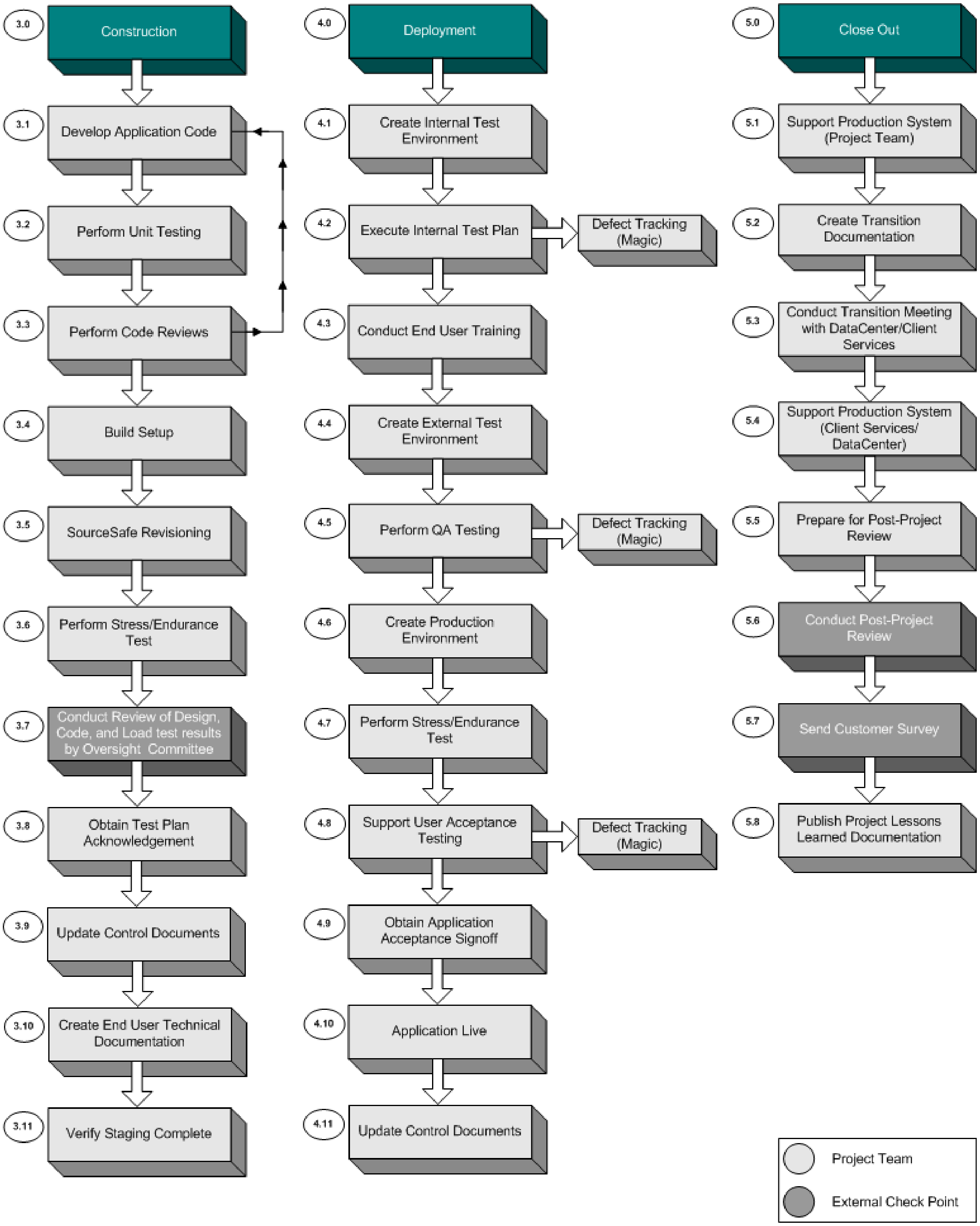
B.) **System Life Cycle Management**

System Life Cycle Management is the process of evaluating and monitoring the project management processes that exist for a given project and ensuring that the stated process conforms to the project plan. It is important that the life cycle of the project, product or service is managed throughout the sequential phases, which include initiation, development/acquisition, implementation, operation, and disposal.

1. The Contractor is required to review the security controls in every phase of the system life cycle and report to the Project Manager or designee the results of the review.

First Data Government Solutions follows a detailed project lifecycle management process. The five stages of this plan are Initiation, Planning, Construction, Deployment, and Close Out. This lifecycle is shown in the following flow chart.


1.0
Initiation
1.1
Schedule Resources
1.2
Review Project Documentation
1.3
Conduct Oversight Committee Project Review
1.4
Prepare Project Control Documents
1.5
Conduct Internal Kickoff Meetings
1.6
Conduct Client Kickoff Meeting
2.0
Planning
2.1
Requirements Traceability Matrix Signoff
2.2
Build General System Design (GSD)/Proof of Concept
2.3
General System/Proof of Concept Design Signoff
2.4
Build Initial Designer Files & Appendixes (DSD)
2.5
Conduct Design Review Meeting (JAD)
2.6
Finalize Designer Files & Appendixes (DSD)
2.7
Build Tech Detailed System Design (Tech DSD)
2.8
Conduct Review of Designer Files & DSD by Oversight Committee
2.9
Review and Obtain Design and Requirements Matrix Signoff from Client
2.10
Create Test Plan
2.11
Create End User Documentation
2.12
Update Control Documents


3.0
Construction
3.1
Develop Application Code
3.2
Perform Unit Testing
3.3
Perform Code Reviews
3.4
Build Setup
3.5
SourceSafe Revisioning
3.6
Perform Stress/Endurance Test
3.7
Conduct Review of Design, Code, and Load test results by Oversight Committee
3.8
Obtain Test Plan Acknowledgement
3.9
Update Control Documents
3.10
Create End User Technical Documentation
3.11
Verify Staging Complete
4.0
Deployment
4.1
Create Internal Test Environment
4.2
Execute Internal Test Plan
Defect Tracking (Magic)
4.3
Conduct End User Training
4.4
Create External Test Environment
4.5
Perform QA Testing
Defect Tracking (Magic)
4.6
Create Production Environment
4.7
Perform Stress/Endurance Test
4.8
Support User Acceptance Testing
Defect Tracking (Magic)
4.9
Obtain Application Acceptance Signoff
4.10
Application Live
4.11
Update Control Documents
5.0
Close Out
5.1
Support Production System (Project Team)
5.2
Create Transition Documentation
5.3
Conduct Transition Meeting with DataCenter/Client Services
5.4
Support Production System (Client Services/ DataCenter)
5.5
Prepare for Post-Project Review
5.6
Conduct Post-Project Review
5.7
Send Customer Survey
5.8
Publish Project Lessons Learned Documentation
Project Team
External Check Point

C.) **System Security Certification**

It is imperative that the system has security certification. It is used to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This shall address the specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. The Project Manager or designee will have the information needed from the security certification to determine the risk to State's operations, assets, or individuals; and will be able to render an appropriate security accreditation decision for the information system.

1. Upon award of the contract and when major modifications occur, the Contractor shall provide a security certification report that addresses the adequacy of the security controls implemented or planned.

   First Data Government Solutions recognizes its responsibility to provide a secure data processing environment during normal operations and during major modifications. Changes that could affect the integrity of the environment, such as new applications, servers, firewalls or other networking changes, require assessment and approval by The FDC Security Assessment Center. Methodologies are in place to make sure that security controls are implemented during system modifications. Reports detailing the changes and security implications can be available upon request.

D.) **System Security Accreditation and Assurance**

In order to assure that the remaining known information system vulnerabilities pose an acceptable level of risk to the State's operations, the system accreditation decisions and documentation must be completed. The residual security threats identified must be acceptable to Michigan's Office of Enterprise Security and the Michigan Department of Treasury's Security Division. The Project Manager or authorized designee will have 1) authorization to operate the information system; 2) an interim authorization to operate the information system created by the Contractor; or 3) denial of authorization to operate the information system. Completing a security accreditation ensures that an information system will be operated with appropriate management review.

1. The Contractor shall have a formal documented accreditation policy and procedures that addresses purpose, scope, roles, responsibilities, and compliance.
2. The Contractor shall perform a security control test and evaluation to demonstrate that the management, operational and technical security controls are implemented correctly and are effective The Contractor will provide a copy of the test results and evaluation to the Project Manager or designee.

The PayPoint solution undergoes annual testing and certifications. This includes PCI and Trustwave audits. Upon award, audit reports are may be available for review by formal request.

First Data is continuously reviewing and testing the security associated with its applications. Methodologies and processes are monitored and assessed through scheduled audits, including PCI, TrustWave, and SAS70. Upon award, audit results can be made available to the State.

E.) **System Security Plan**

The Contractor shall develop, publish, maintain and disseminate a formal security plan, for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. The security plan must be reviewed periodically and revised to address system/organizational changes or problems identified during security plan implementation or security control assessments.

The Contractor shall periodically test and evaluate the effectiveness of information security policies, procedures and practices performed with a frequency depending on risk that includes testing of management, operational, and technical controls for every critical information system.

An extensive security plan is in place through the FDC Security Assessment Center. The security plan contains confidential details and can be made available to the State upon award.

F.) **Acquisition**

The Contractor must include required security controls either explicitly or by reference in information system acquisition contracts based on an assessment of risk. Any subcontractor must comply with State and Federal statutory and regulatory requirements and rules; Payment Card Industry (PCI) Data Security Standards; all other industry specific standards; National Institute of Standards and

Technology (NIST) publications; Control Objectives for Information and Related Technology (COBIT); and national security best practices. The Contractor shall have a formal documented system and service acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and formal documented procedures to facilitate the implementation.

[1]The Information Technology Audit Team uses the COBIT model from the IT Governance Institute to:

(1) Assess technology and related business risks,

(2) Plan procedures,

(3) Execute the procedures, and

(4) Assess the results of audit procedures.

The COBIT model is augmented with guidance from:

(1) The 'Federal Financial Institutions Examination Council's IT Examination Handbook',

(2) Regulations promulgated by the Securities and Exchange Commission, Office of the Comptroller of the Currency, Office of Thrift Supervision, etc.,

(3) Regulations promulgated by card associations and companies,

(4) Standards promulgated by the International Organization for Standardization (ISO), and

(5) Guidance from other professional and industry organizations.

G.) **Security Performance Reporting**

The Contractor will be required to supply monthly reports that reflect system performance including average response times, number and duration of outage events, erroneous transactions, and other information required to monitor the performance of the system. The details and timing of the reports will be determined during implementation.

First Data Government Solutions provides an Incident Matrix Report on a monthly basis that shows average response times, number and duration of outage events, erroneous transactions, etc.

H.) **SAS 70 and PCI Reports**

SAS 70 and PCI Reports:

1. The Contractor will supply the Project Manager or designee annual SAS 70 audits and will email quarterly confirmation that Contractor has run PCI scans and will follow First Data and PCI standard procedures for addressing any findings identified by the scans. See Section 1.104.

2. PCI reports will also be required from each applicable subContractor.

3. The Contractor will be responsible for obtaining SAS 70 reports or use other tools that document management assurance of internal controls for subContractors. These reports will be submitted to the Project Manager or designee.

4. Any areas of weakness will require follow-up of Contractor and/or subContractor and reporting of corrective action plans and completion of those plans to the Project Manager or designee.

PayPoint meets the SAS70 and PCI reporting requirements detailed in items 1 through 4. First Data Government Solutions undergoes regular audits and certifications for the Credit Card and NACHA transactions. A SAS70 report can be provided to the State, upon request, detailing the results of the most recent audit, performed by Ernst and Young, LLP. The PCI Certification can be provided to the State upon request.

C2. **Operational Controls**

Operational Controls include those policies, procedures and instructions in place to minimize potential adverse impact on the State of Michigan's information or an information system processing, storing, and/or transmitting personal, confidential or sensitive information or information processed, stored, and/or transmitted on behalf of the State.

[1] SAS70 Audit Page 9

A.) **Personnel Security**

The Contractor shall have a formal documented, published, maintained and disseminated personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and formal documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. The Contractor is required to define the job responsibilities, determine the sensitivity of the position by designating a risk to all positions and establish screening criteria for individuals filling those positions. Once a position has been broadly defined, the Contractor shall determine the type of computer access needed for the position and screen individuals requiring access before authorizing access. Contractor certifies that any of its employees having access or continued access to the State's Confidential Information will acknowledge in writing the Contractor's Code of Conduct, a current copy of which is attached hereto, and will comply with the Acceptable Use Policy 1460 (See Policy at http://www.michigan.gov/dit/0,1607,7-139-34305-107739--,00.html) upon award of the contract. Also see Section 2.054.

In addition, the Contractor shall review, modify or terminate information system/facilities access authorization when individuals are reassigned, transferred to other positions or vacate positions, and initiate appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing information system access authorization).

As the incumbent provider, First Data Government Solutions has the operational controls in place and will continue to meet the State's requirement. Physical Security is handled through First Data's Corporate Security group. In addition, our hosted data centers have a variety of physical security features that restrict access that includes: security presence at all points of entry, digital access card requirement, CCTV surveillance of all entry points and data centers 24x7, Mantrap Entrance for data centers, and temporary-use digital access cards required for data center access. In addition, all persons must pass a background verification, and supply fingerprints and handwriting analysis before they are granted access to FDC facilities and systems. Authorized data center personnel must escort any outsiders.

While corporate nondisclosures are in place, First Data policy restricts individual employees from signing nondisclosure agreements.

B.) **Business Continuity and Disaster Recovery Planning**

The Contractor and its third-party service providers shall develop, periodically update, and regularly test disaster recovery and business continuity plans designed to ensure the availability of Department of Treasury's information in the event of an adverse impact to the Contractors information systems due to a natural or man-made emergency or disaster event. The Contractor and its third-party service providers shall:

1. Describe the methodology and components incorporated in business continuity and disaster recovery plans.

2. Develop and implement business continuity and disaster recovery plans and procedures addressing contingency roles, responsibilities and activities associated with restoring system after a disruption or failure.

3. Test each plan periodically to determine the plan's effectiveness and the organization's readiness to execute the plan. The plan should be reviewed at least annually and revised to address system/organizational changes.

Also see Section 2.203.

First Data Government Solutions' primary data center is in Denver, Colorado. The disaster recovery (DR) data center is in Omaha, Nebraska. Applications are rolled to the DR site by manually rolling the Domain Name System (DNS). Rolling the DNS means that the IP address used to resolve the URLs is changed to point from the active servers (Denver) to the IP addresses of the servers in the DR site (Omaha). The applications will become active in the DR site after the DNS is rolled because the DR site is a hot site and is always running.

The Web Farm Troubleshooting guide provides a decision tree for actions that should be taken in the event of a system outage. If an application is down, a Severity 1 ticket is created and pages are sent to the on-call support team in First Data Government Solutions and FDT. A bridge call is established so the problem can be investigated with the various groups following the trouble-shooting guide. If the service cannot be restored within 45 minutes, the Manager on-call can decide to roll all of the applications to the DR site.

First Data Government Solutions conducts biweekly DR readiness meetings to discuss current events and any change management or performance concerns. The team performs DR load test exercises to assess DR readiness from a data processing perspective. First Data encourages our clients to schedule DR functionality testing with us and direct a portion of their applications that normally run in the UAT environment, over to the DR facility to prove application functionality.

C.) **Backup and Recovery**

The Contractor shall:

1. Backup personal, confidential or sensitive information and store it at appropriately secured facilities, on-site and off-site and ensure prompt restoration.
2. Encrypt personal, confidential or sensitive information at rest.
3. Develop, disseminate and periodically review/update formal documented procedures to facilitate full recovery and reconstitution of the information system.

PayPoint meets the Backup and Recovery requirements detailed in items 1 through 3. Confidential and sensitive information that needs to be stored is encrypted in the database, and masked when displayed to all users of the application. Data is replicated in real-time to the DR facility.

FDGS includes tape media in its backup and recovery procedures. Tapes are stored in a secure off site location.

D.) **Security Incident Handling**

Computer security incidents can result from a computer virus, other malicious code, a system intruder either an insider or an outsider, system failures, denial of service or breaches of confidentiality.

1. The Contractor shall develop, document, and update an Incident Response policy and procedures for detecting, reporting, and responding to security incidents.
2. The Contractor shall track and document information system security incidents, the corrective action taken and any recommendation to prevent such incidents.
3. The Project Manager must be immediately informed of all security incidents. When feasible, decisions on how to handle the issues should include input from the Project Manager or designee.
4. Incident Response testing at least annually.
5. Personnel trained in their incident response roles and responsibilities at least annually.

First Data Government Solutions meets requirements 1 through 5 by receiving and evaluating the Microsoft and other vendor hot fixes on a monthly basis. If it is determined the hot fix is addressing a legitimate security issue, the patches are applied first to the QA environment, and then moved to production.

Additionally, we have detailed policies detailing how security incidents are handled, managed, and reported. First Data Government Solutions has a Data Privacy Office that participates in any data security concern. First Data Government Solutions' employees are required to take Data Privacy and Incident Response training, and receive certification annually.

First Data Government Solutions has a Data Privacy Office that participates in any data security concern. The FDGS support staff are required to take annual Data Privacy and Incident Response training. Additionally, the support staff receives annual reviews from their management.

E.) **Physical and Environmental Security**

The Contractor shall establish physical and environmental security controls to protect systems, the related supporting infrastructure and facilities against threats associated with their physical environment.

1. The Contractor shall establish environmental protection for magnetic and other media from fire, temperature, liquids, magnetism, smoke, and dust.
2. The Contractor shall control all physical access points to facilities containing information systems (except those areas within the facilities officially designated as publicly accessible), review physical security logs periodically, investigate security violations or suspicious physical access activities, and initiate remedial actions.
3. The Contractor shall periodically review the established physical and environmental security controls to ensure that they are working as intended.
4. The Contractor is required to have a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and formal documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

PayPoint meets the Physical and Environmental Security requirements detailed in item one (1) through four (4).

Physical Security is handled through First Data's Corporate Security group. Processes and controls are constantly monitored to improve security and efficiencies. The data centers are managed and monitored by the Corporate Security group through three (3) components: Physical Security, Environmental Security, and Data Security

Physical Security – The First Data data centers are C2-compliant and have security guards staffed 24-hours a day, seven (7)-days a week to monitor the facility. Visitor access is restricted – access cards are required for entrance and video monitors record activity in and around the data center.

Environmental Security – Each of the data centers is engineered to withstand local natural disasters and provide redundant electrical and mechanical systems.

Data Security – Users are only given access to servers and data where it is needed to fulfill their job requirements. Systems and processes are constantly monitored to ensure everything is functioning as expected.

F.) **Configuration Management**

1. The Contractor shall develop, document, and maintain a current baseline configuration of the information system and an inventory of the system's components.
2. The Contractor shall develop and implement formal change control procedures, configure the security setting to the most restrictive mode, configure the information system to provide only essential capabilities and prohibit default functions and services, document and audit configurations and settings, and maintain audit logs for all access to operational program source and object libraries.
3. The Contractor shall have a formal documented configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and formal documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

First Data Government Solutions meets the requirements listed in items 1 through 3 and currently has a dedicated Configuration Management group whose responsibility it is to migrate new code into QA, UAT, and production environments. All of these code moves have an audit trail, and require Impact Records to be created and prior approvals to move. Additionally, there are weekly meetings with the Chief Technology Office and Global Technology Solution teams to discuss and review change control.

G.) **Media Protection**

1. The Contractor shall implement a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media containing personal, confidential or sensitive information to prevent the loss of confidentiality, integrity, or availability of information including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output.
2. The Contractor shall ensure that only authorized users have access to information in printed form or on digital media removed from the information system, physically control and securely store information media, both paper and digital, restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.
3. The Contractor shall have a formal documented, published, maintained and disseminated Media Protection Policy that addresses purpose, scope, roles and responsibilities, and compliance; and formal documented procedures to facilitate the implementation of the policy and controls.

As the incumbent provider, First Data Government Solutions is currently protecting and managing the media requirements requested by the State and will continue to meet the State's requirements. First Data Government Solutions resides within secured suites and uses Data Guard to dispose and shred hardcopy media. First Data Government Solutions' employees attend mandated sensitive data usage and retention training annually – with periodic reminder bulletins and awareness campaigns throughout the year. This training addresses all media types that may be encountered in a work situation. Additionally, privacy officers review all non-secured cubicles and common areas to ensure no confidential data is present. Hardcopy media is disposed of in Data Guard bins. Any screen shots of the application would have sensitive information masked. Protecting and properly disposing of sensitive material is addressed in the federally-mandated annual UNAX training, which is attended by First Data Government Solutions employees.
First Data will keep data two years on- line and the oldest partition will be rolled off quarterly and stored off-site for an additional period of seven years.

H.) **Media Destruction and Disposal**

1. The Contractor shall sanitize or destroy information system digital media and printouts containing personal, confidential or sensitive information before its disposal or release for reuse to prevent unauthorized individuals from gaining access to and using information contained on the media.
   - Personal, confidential or sensitive information must be destroyed by burning, mulching, pulverizing or shredding. If shredded, strips should not be more than 5/16-inch, microfilm should be shredded to affect a 1/35-inch by 3/8-inch strip, and pulping should reduce material to particles of one inch or smaller.

   - Disk or tape media must be destroyed by overwriting all data tracks a minimum of three times or running a magnetic strip over and under entire area of disk at least three (3) times. If the CD, DVD or tape cannot be overwritten it must be destroyed in an obvious manner to prevent use in any disk drive unit and discarded. Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal. Electronic data residing on any computer systems must be purged based on retention periods required by the Department of Treasury.

2. The Contractor must track, document and verify media sanitization actions; and provide certification attesting that personal, confidential or sensitive data has been removed from digital media before disposing or releasing for reuse.

3. The Contractor shall have a formal, documented, published, maintained and disseminated Media Destruction and Disposal policy that addresses purpose, scope, roles, responsibilities and compliance; and formal documented procedures.

PayPoint meets the requirements listed in items 1 through 3. First Data Government Solutions uses Data Guard to dispose of and shred hardcopy media. Our employees attend mandated sensitive data usage and retention training annually – with periodic reminder bulletins and awareness campaigns throughout the year. This training addresses all media types that may be encountered in a work situation. Additionally, privacy officers review all non-secured cubicles and common areas to make sure no confidential data is present. Hardcopy media is disposed of in Data Guard bins. Any screen shots of the application would have sensitive information masked. Protecting and properly disposing of sensitive material is addressed in the Federally-mandated annual UNAX training that is attended by First Data Government Solutions employees. First Data Government Solutions incorporates a two-phase destruction process; 1) FDGS degausses tapes to ensure erasure; 2) FDGS contracts with Iron Mountain for final destruction of the media. Iron Mountain does actual physical shredding of media and, if requested, a certificate of destruction will be provided.

I.) **Data Security**

Describe how the State of Michigan customer's personal and financial information will be protected from unauthorized use and theft addressing each of the issues below.

1. The Contractor will serve as the custodian of State of Michigan's personal, confidential or sensitive information and shall comply with State and Federal statutory and regulatory requirements and rules; Payment Card Industry (PCI) Data Security Standards; all other industry specific standards; National Institute of Standards and Technology (NIST) publications; Control Objectives for Information and Related Technology (COBIT); and national security best practices regarding protection of confidentilaity, intergity, and availability of data. Personal, or confidential data includes but is not limited to customer's personal and financial information, such as Social Security Numbers, credit card numbers, bank account numbers, name, address etc.
2. The Contractor shall have in place appropriate technical and organizational internal and security controls to protect the personal and financial data against unauthorized disclosure or access, accidental loss, alteration, and accidental or unlawful destruction which provide a level of security appropriate to the risk represented by the nature of the data to be protected.
3. The Contractor shall provide secure and acceptable methods of transmitting personal, confidential or sensitive information over telecommunication devices such as data encryption, Secure Socket Layer (SSL), dedicated leased line or Virtual Private Network (VPN).
4. The Contractor must use data encryption techniques whenever personal, confidential or sensitive data is transmitted to and from a remote site with the exception of the dedicated leased line.
5. The Contractor shall process personal, confidential and sensitive data only for purposes described in the contract.
6. The Contractor shall not disclose or transfer personal, confidential or sensitive data to a third party unless it is approved under this contract.
7. The Contractor shall not use data transferred by the Department of Treasury as a result of this contract for marketing purposes

First Data Government Solutions places a high priority on data security. As the current provider for the State, we understand the sensitivity and requirements necessary to protect your data. During the current Payment and Authorization System's implementation, FDGS succeeded in providing a secure solution and will continue to meet the State's requirements.

1. The PayPoint solution is PCI-compliant, undergoing system and security audits to ensure that confidential data is protected. Audit reports can be made available upon award. Additionally, First Data Government Solutions' employees are required to take Data Privacy and Incident Response training, receiving certification annually. Secure mail is used in sending emails that contain sensitive data deemed critical. FDGS recommends phone calls when sensitive or confidential information must be communicated.
2. Payment information is contained in a secure, hosted data center with technical and organizational processes in place to ensure only authorized users have access to the system.
3. A dedicated frame relay is set-up between the FDC data centers and Michigan's processor of choice (TSYS). SSL is utilized when transmitting data to First Data Government Solutions' PayPoint APIs.
4. Sensitive data is encrypted and stored within the PayPoint solution. When communicating to the State's processor, a dedicated frame relay connection is used.
5. First Data Government Solutions will only access payment and confidential information for purposes detailed in the contract with the State of Michigan.

6. First Data Government Solutions will not disclose or transfer personal, confidential, or sensitive data to a third party, unless approved under the contract.
7. First Data Government Solutions will not use data transferred by the Michigan Department of Treasury for marketing purposes.

J.) **Information System Maintenance**

System maintenance requires either physical or logical access to the system. Support and operations staff or third-party service providers may maintain a system. Maintenance may be performed on site, or it may be necessary to move equipment to a repair site. Maintenance may also be performed remotely via communications connections.

1. The contractor shall take additional precautions, such as conducting background investigations of service personnel, supervising system maintenance personnel, authenticating the maintenance provider using call-back confirmation, encrypting and decrypting diagnostic communications; using strong identification and authentication techniques, such as tokens; and using remote disconnect verification.
2. The Contractor shall have a formal documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated controls.

Background investigations of employees, prospective employees, and vendor employees are performed and outlined in the Security SAS70. When accessing our infrastructure, strong passwords are utilized within PayPoint, and RSA SecurID tokens are utilized in order to gain access into the infrastructure externally.

Documented system maintenance policies are used when accessing the server to perform system maintenance.

C3. **Payment Card Industry (PCI) Data Security Standards**

Contractors with access to credit/debit card cardholder data must adhere to the Payment Card Industry (PCI) Data Security Standards (PCIDSS).

Information about the Payment Card Industry (PCI) Data Security Standards can be found on Visa's site www.visa.com/cisp, MasterCard's site https://sdp.mastercardintl.com, and the PCI Security Council site www.pcisecuritystandards.org.

1. Contractor acknowledges that they are responsible for security of cardholder data in their possession.

As the current vendor, our solution meets this requirement today, and adheres to PCI data security standards. Upon request, we will provide the State with certification letters from last year's audit by the TrustWave Corporation.

2. Contractor acknowledges and agrees that data can ONLY be used for assisting the State in completing a transaction, supporting a loyalty program, supporting the State, providing fraud control services, or for other uses specifically required by law.

Client Data is not utilized for any purpose other than what is listed above.

3. Contractor agrees to provide business continuity in the event of a major disruption, disaster or failure.

First Data Government Solutions' staff is on-call 24x7 to maintain and restore service in the event of problems or failures. In the case of a disruption in service, a Severity 1 is created, and pages are sent to all on-call support team members within First Data Government Solutions and First Data Technology (FDT). A bridge call is established and the issues are worked until service is restored.

4. In the event of a security intrusion, the Contractor agrees the Payment Card Industry representative, or a Payment Card Industry approved third party, will be provided with full cooperation and access to conduct a thorough security review. The review will validate compliance with the Payment Card Industry Data Security Standard for protecting cardholder data.

First Data Government Solutions will provided full cooperation if the above scenario is ever encountered.

5. Contractor agrees to properly dispose sensitive cardholder data when no longer needed.

Cardholder data will be purged properly.

6. Contractor will continue to treat cardholder data as confidential upon contract termination.

Data integrity will be maintained upon contract termination. Upon contract termination, FDGS will work with the state of Michigan to migrate all necessary information. Once the data has been transferred to the State, all applications, user accounts, and registrations will be purged from the PayPoint system.

7. The Contractor will contact the Michigan Department of Treasury immediately to advise them of any breaches in security where card data has been compromised.

Unless otherwise prohibited by law, the Contractor will contact the Department of Technology, Management and Budget, Financial Services, CEPAS Program Manager or Receipts Processing Administrator to advise them of any breaches in security where the State's card data has been compromised within 2 business days after the compromise has been confirmed by the Contractor's Privacy Office. In the event of a security intrusion, the Contractor agrees to cooperate with Payment Card Association requirements.
.

8. The contractor will provide the Michigan Department of Treasury documentation showing (PCI) Data Security certification has been achieved.

First Data Government Solutions will provide the State documentation showing PCI Certification.

9. The Contractor will advise the Michigan Department of Treasury of all failures to comply with the PCI Data Security Requirements. Failures include, but are not limited to system scans and self-assessment questionnaires. The Contractor will provide a time line for corrective action.

As the current provider for the State, First Data Government Solutions understands the sensitivity and requirements necessary to protect your data. The PayPoint solution is PCI-compliant and undergoes system and security audits to ensure that confidential data is protected. Audit reports can be made available upon award. In the instance where a security concern is detected, First Data Government Solutions will notify the State and provide a time line for corrective action.

10. Data Compromise – Has the Contractor's system ever experienced a security breach where cardholder data was at risk of being misused or was misused as a result of the breach?

    Note: Information supplied in this contract is public information under the Freedom of Information Act (FOIA).

First Data Government Solutions has never experienced a security breach where cardholder data was at risk of being compromised or misused.

IN THE EVENT OF A BREACH OF THE CONTRACTORS SYSTEM WHERE CARDHOLDER DATA HAS BEEN COMPROMISED, THE CONTRACTOR WILL BE RESPONSIBLE FOR ANY AND ALL COSTS INCURRED BY THE STATE ASSOCIATED WITH THE BREACH, SUBJECT TO SECTION 2.221, LIMITATION OF LIABILITY.

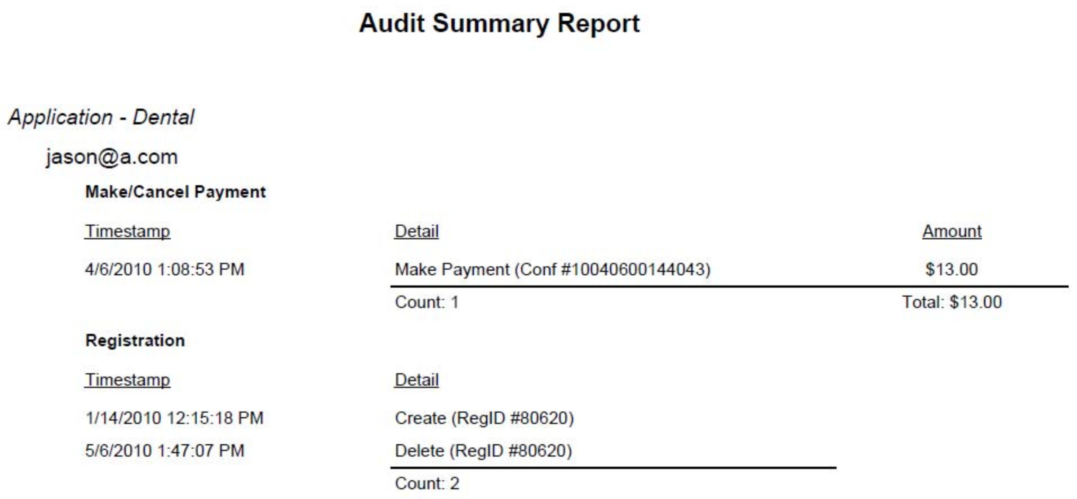
C4. Security User Monitoring Reports

The Contractor shall have effectively implemented audit logs that assist in selecting pertinent information to create monitoring reports. The audit log fields include but are not limited to:

User Name
User Identification Code
User Department
Applicaton Name
User Role
Action taken
Date and time of action
Before and after information.

The Contractor must generate security audit reports in electronic format.

PayPoint provides an Audit Summary Report which details the updates that have been made to an application. From this report, the user, application, timestamp, action taken, and details are shown. Currently, there is no way to display the before and after information. An example of the Audit Summary Report is shown below



Audit Summary Report

Application - Dental

jason@a.com

Make/Cancel Payment

Timestamp	Detail	Amount
4/6/2010 1:08:53 PM	Make Payment (Conf #10040600144043)	$13.00
	Count: 1	Total: $13.00

Registration

Timestamp	Detail
1/14/2010 12:15:18 PM	Create (RegID #80620)
5/6/2010 1:47:07 PM	Delete (RegID #80620)
	Count: 2

C5. Technical Controls

Technical controls include those policies, procedures and instructions in place that focus on security controls that the computer system executes. The controls must provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

A.) Access Control

Access controls are put in place to authorize or restrict the activities of users and system personnel within the application. Access to the State's information and information systems will be based on each user's access privileges. Access privileges shall be granted on the basis of specific business need (i.e., a "*need to know*" basis). Hardware and software features shall be designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and detect unauthorized activities. The Contractor shall ensure that even legitimate users cannot access stored information unless they are authorized to do so.

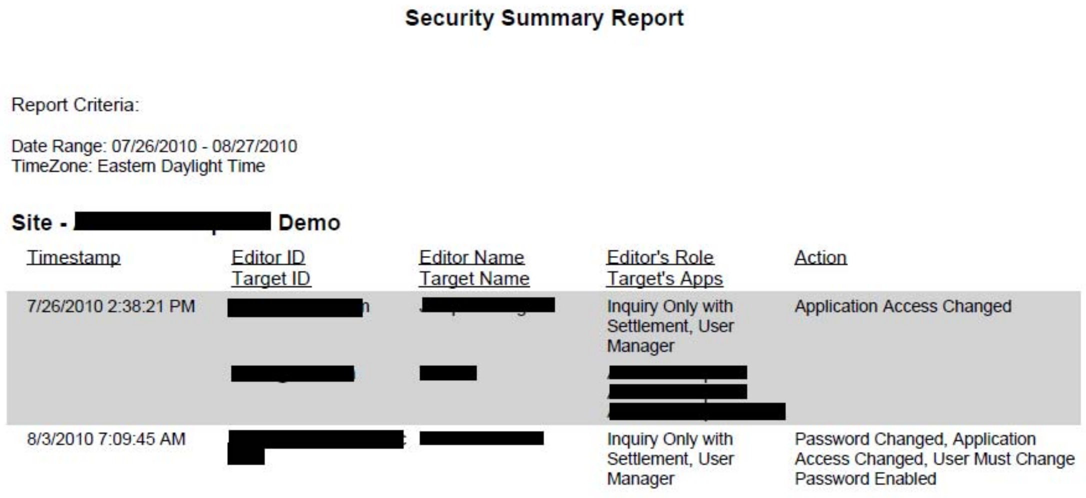
The Contractor shall have a formal documented, published, maintained and disseminated Access Control Policy and Procedures that address purpose, scope, roles, responsibilities and compliancy.

1. The Contractor shall periodically verify the legitimacy of user accounts and access authorizations and timely modify, suspend or remove access for employees who are reassigned, promoted, on a leave of absence, or terminated.

2. The Contractor shall provide User Access Reports in an electronic format that identifies at least the following information:
   a.) User Name
   b.) User Identification Code
   c.) User Department
   d.) Application Name(s)
   e.) Access Rights

3. The Contractor must establish appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. For example, the State staff responsible for assigning user access rights must not have access to any other functionality than access rights management.
4. The information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

PayPoint meets the Access Control requirements detailed in items 1 through 4. PayPoint uses roll-based security and permissions to grant users access to specific activities within the application. PayPoint's authentication allows the customer to delegate specific tasks and roles to unique individuals within the application. Roles can be expanded- or limited-based requirements, as set forth by the State. Roles can be configured to span across the whole Site or Agency, or narrowed to an individual Application level. A screen shot of a Security Summary Report is shown below.



Security Summary Report

Report Criteria:

Date Range: 07/26/2010 - 08/27/2010
TimeZone: Eastern Daylight Time

Site - [redacted] Demo

Timestamp	Editor ID	Editor Name	Editor's Role	Action
	Target ID	Target Name	Target's Apps	
7/26/2010 2:38:21 PM	[redacted]	[redacted]	Inquiry Only with Settlement, User Manager	Application Access Changed
	[redacted]	[redacted]	[redacted]	
8/3/2010 7:09:45 AM	[redacted]	[redacted]	Inquiry Only with Settlement, User Manager	Password Changed, Application Access Changed, User Must Change Password Enabled

Identify hardware or software features that are designed to permit only authorized access to or within the application.
Describe cryptographic methodology used with associated key management processes and procedures.

PayPoint users are assigned a unique User ID and must have a strong password to access the system. All users are assigned a security role, which provides the permissions available to the user and determines what information is displayed and available.

The PayPoint solution uses the terminology of Agency to represent User Department. All reporting can be run at an agency level.

B.) **Identification and Authentication**

Identification and authentication is a technical measure that prevents unauthorized people or unauthorized processes from entering an IT system. The system must be able to identify and differentiate users.

Identification is the means by which a user provides a claimed identity to the system.

The Contractor shall have a formal documented, published, maintained and disseminated Identification and Authentication Policy and Procedures that address purpose, scope, roles, responsibilities and compliancy.

First Data Government Solutions assigns each user of PayPoint a User ID that is an e-mail address, a strong password (at least 8-characters in length), a role that determines what information is displayed, and the available applications. These policies can be seen by the Michigan users that are defined in PayPoint, today.

C.) **Authentication**

Authentication is the means of establishing the validity of a user's claimed identify to the system.

All users including an application or system must have a unique identifier and authenticator (e.g., password, etc.). Passwords are a primary means to control access to a system. The information system must allow users to select and employ strong passwords to prevent compromise of personal, confidential or sensitive information.

The Contractor shall have a formal documented, published, maintained and disseminated Password Policy and Procedures that address purpose, scope, roles, responsibilities and compliancy.

The PayPoint password policy is defined in the PayPoint User Guide. Passwords must be at least 8 characters long and must contain letters and at least one number and may contain special characters.

It is highly recommended that passwords selected be strong passwords, containing numbers, letters and special characters.

System and server passwords follow First Data's password policy which requires strong passwords and scheduled password changes.

D.) **Password Requirements**

The Contractor's password rules will be equivalent to PCI DSS password requirements. If the PCI password requirements change, the Contractor is expected to make changes to their password rules to remain in compliance with PCI DSS standards.

PayPoint is a PCI DSS certified solution. Changes to PCI requirements will be evaluated and managed to enable PayPoint to keep its PCI DSS certified status.

E.) **Security Awareness and Training**

The Contractor shall ensure that individuals with significant information system security roles and responsibilities have appropriate system security training and all users (including program and project managers) are exposed to basic information system security awareness materials before authorizing access to the State of Michigan's information and information system. The information system security training plan must be documented and monitored.

a.) The Contractor shall develop, disseminate and periodically review/update: (i) a formal documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Proper training on the PayPoint solution is essential in providing effective management and smooth product operation. First Data Government Solutions provides training and the PayPoint User Guide (Attachment F) to help effectively manage and inform the State's resources.

F.) Audit Trails

The Contractor must (i) create, protect, and retain information system audit log records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

The Contractor shall observe the following guidelines regarding system auditing:

1. Audit record should contain the following:
   - date and time of the event
   - subject identity
   - type of event
   - how data changed
   - where the event occurred
   - outcome of the event

2. System alerts if audit log generation fails

   First Data uses multiple methods of alerts for the PayPoint system. These include alerts through the use of Computer Associates' UniCenter product, support staff paging, and custom monitoring tools.

3. System protects audit information from unauthorized access

   FDGS protects audit information from unauthorized access through the use of encryption and password protection. PayPoint posting files are encrypted and delivered to a secure FTP location. Access to the administrative site is restricted by passwords and user security roles.

4. Audit record should be reviewed by individuals with a "need to know" on a regular basis

5. Audit logs are retained for sufficient period of time.

PayPoint meets the auditing and logging requirements detailed in items 1 through 5. Audit trails are available through multiple interfaces within the PayPoint solution. For users who have logged into the system and are modifying user or application information, this information is captured and detailed in the Security Summary Report. Further details are captured within the internal PayPoint logging components, and are available to FDGS' customer support staff.

G.) System and Communications Protection

System and communications, if not properly protected, may result in a compromise of all connected systems and the data they store, process, or transmit. The Contractor shall restrict the ability of users to launch various types of denial of service attacks, e.g., viruses, worms, Trojans, etc.

1. The Contractor must have a formal documented, system and communication protection policy and formal, documented procedures to facilitate the implementation of the system. The policies and procedures shall be consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance.

Our data centers use a series of protective methods to ensure the PayPoint solution is not impacted by external attacks. These methods include the use of multiple firewalls, updated anti-virus and monitoring software, and a network operation center staff who monitors the network for such attacks.

The FDGS PayPoint implementation team follows a defined process for boarding an application in the system. Additionally, the technical support staff adheres to internal procedures for escalation and notification of any data center issues.

H.) **Integrity Control**

The Contractor shall provide integrity controls to protect the operating system, application, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

Integrity to the system is controlled through the series of processes and procedures set in place to ensure the functionality to PayPoint is not altered.

A Fire-call ID is required to make modifications to the production environment. The Firecall ID requires management approval. An Impact Record or Problem ticket is needed prior to assigning the Firecall ID so the reason for gaining access can be clearly defined, planned for, and monitored. A Firecall ID is an ID that has access to make changes to the production environment. No individual user has this access.

FDGS limits the access to the data center to individuals whose roles and responsibilities are for the day-to-day management and maintenance of the system. In some instances, individuals with specific expertise need to access the servers. In these circumstances, a Firecall ID is issued to provide temporary access. The Firecall ID is issued only for a specific time and duration. After the selected time needed to access the server is finished, the connectivity to the system is terminated and the request is closed.

I.) **Change Control**

1. The Contractor shall make only changes authorized and approved by the Contract Administrator or designee, maintain strict control over access to program source libraries; separate development, testing and operational environments to enforce an adequate segregation of duties between developers, testers and operations staff; monitor changes to the information system; and conduct a security impact analysis to determine the effects of the changes.

2. The Contractor shall have a formal documented, published, maintained and disseminated change control policy that addresses purpose, scope, roles, responsibilities, and compliance; and formal documented procedures to facilitate the implementation of the change control policy and associated change controls .

First Data Government Solutions has a formal Change Control process that adheres to all specifications in this requirement. We will provide a formal change control policy that addresses all the needs of the State.

J.) **Network Security**

The Contractor is responsible for the security of and access to the State's information. Unsecured operating practices, which expose other connected State networks to malicious security violations, are not acceptable. The Contractor and its sub-Contractor:

1. Must follow the State of Michigan, Department of Information Technology's Firewall Access Policy provisions if those servers require data or transactions that must pass through the State's secure firewall perimeter. This Policy will be available to the Contractor upon award of the contract, after completing and submitting form DIT0049, Non Disclosure Agreement to the Project Manager or designee.

2. Must coordinate with the Department of Information Technology, to enter the proper pointers into the State Domain Name System (DNS) for identifying and locating their Intranet and Internet servers.

3. Must have documented network security policies and procedures that address purpose, scope, roles and responsibilities.

As the incumbent solution, PayPoint meets this requirement and FDGS will to work with the State of Michigan to continue to provide a secure solution.

First Data has an Information Security group strictly dedicated to monitoring and proactively addressing any security threats. The Information Security team follows strict procedures and policies on how servers are monitored, patched, and accessed.

K.) **Web Application Security**

The Contractor shall establish adequate security controls for web application(s) to provide a high level of security to protect confidentiality of data transmitted over the public internet. The controls include, but are not limited to:

a.) authentication
b.) authorization and access control
c.) web application and server configuration (e.g., patch management, deletion of unnecessary services, separation of the operating system and the web server)
d.) session management (e.g., randomly generated unique session IDs, session encryption, time-out setting for inactive session)
e.) input validation (e.g., avoid shell commands, system calls, and malicious codes),
f.) encryption (e.g., protect personal, confidential or sensitive information, encryption keys, passwords, shared secret),
g.) audit logs (e.g., all authentication and authorization events, logging in, logging out, failed logins).

PayPoint meets the web application security requirements detailed in items a through g. VPN, Frame Relay, SSH, SSL, and data encryption are all in place and utilized when transmitting data from point to point in the current application. At no point is the data unsecured in transit.

Addressing item e: First Data performs data validation and input verification to make sure that PayPoint solution is not susceptible to external commands, and malicious code. This is accomplished by performing tests and scans on the system, covering items such as buffer overflow, SQL injections, right of entry processes, and security assessment scans.

Addressing item f: All PCI data (credit and debit card numbers) is encrypted using server-level encryption keys. These keys are locked down and only two employees in First Data have access to the keys. Each environment utilizes different keys and the keys are stored in a lockdown area of the server. In addition to the PCI data, we also encrypt other sensitive data (i.e. bank account number, SSN, FEIN, Driver's License, and passwords). Passwords are stored using a one-way hash. Production server level encryption is 128 AES.

The PayPoint websites (Administration and Consumer Payments) and API calls (Web Services and HTTP) utilize 2048 bit SSL certificates.

Addressing item g: Detailed logs such as failed logins and authorization events are captured in FDGS' Operational Logs. These logs are used by the FDGS support team for monitoring and issue resolution, and are not part of the standard reports.

D. SYSTEM PERFORMANCE AND TECHNICAL REQUIREMENTS

D1. **High Availability:** The Contractor must provide a system that is available 7 days a week, 24 hours per day. The Contractor will meet the Service Level Objective of 99.9% system availability. This equates to less than 0.75 (point 75) hours of outage per calendar month, subject to the exclusions set forth in the exclusions below.

Outages caused by any of the following will be excluded for purposes of determining service level:

a.) Periods of scheduled or emergency maintenance activities or a scheduled outage;
b.) Problems caused by systems administration, commands, or file transfers performed by the State's representatives, other activities the State directs;

c.) Denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and the Contractor's other Contractors), and other force majeure events;

d.) Lack of availability or untimely response by the State to incidents that require the State's participation for problem source identification and/or resolution; and

e.) The State's breach of its obligations under this Statement of Work.

When the accumulated monthly outage exceeds 0.75 (point 75) hours of outage per calendar month, the Contractor is subject to Monetary Assessments as defined in section **Article 1, Appendix M**. An outage to any major system component (E-Check processing, Credit Card processing, Administrative Site availability, Search capability, Make Payment, Reports, etc.) is considered an outage of the entire system.

PayPoint is available 24-hours a day, seven (7)-days a week. First Data Government Solutions has a service level objective of 99.9% system availability. We acknowledge the Monetary Assessments as defined in Article 1, Appendix M for outages that occur under the control of First Data Government Solutions. An outage to any major system component (E-Check processing, Credit Card processing, Administrative Site availability, Search capability, Make Payment, Reports, etc.) is considered an outage of the entire system.

D2. **System Maintenance:** The maintenance window designated for the Contractor to perform system maintenance is from 2:00 a.m. – 6:00 a.m. ET on each Sunday. The Contractor must notify and provide details to the Project Manager or designee fourteen (14) business days in advance when system maintenance will be performed. Details must include the real and potential impact on the system and State processing. Prior to performing system maintenance on the production environment, the Contractor will make every attempt to perform the same maintenance on the UAT environment to allow state agencies an opportunity to perform testing to ensure the maintenance does not have any negative impact on their application.

First Data Government Solutions performs PayPoint system maintenance on Thursdays from 2:00 a.m. to 5:00 a.m. ET, for updates that do not require system outages. For updates that require system down time, the maintenance window is on Sundays between 2:00 a.m. and 6:00 a.m. ET. We can explore a new maintenance window, if the State desires. The business contact provides notification via email to the State 14-business days in advance of the maintenance date. The exception is for a system hot fix that impacts the functionality of the product, which is moved into production as quickly as it can be scheduled.

A.) **Revert to Last Best Version:** When the Contractor maintenance includes implementation of a new software version of any component, there must a procedure in place to revert to the last best version of that component when the upgrade is unacceptable.

First Data Government Solutions follows a procedure established by the Data Center Operations Team to revert back to the last best version if an upgrade becomes problematic. The Configuration Management Team rolls back the code package and restores to the previous version of PayPoint in both the Denver and Omaha data centers.

B.) **Emergency Maintenance:** When the Contractor performs emergency maintenance, there must be full disclosure to the State. Hot Fixes or Break Fixes are considered emergency maintenance. The Contractor shall attempt to schedule emergency maintenance during the regular maintenance window (see D2.). If the maintenance cannot be done during the regular maintenance window, the Contractor will perform the maintenance after normal business hours (8:00 a.m. – 5:00 p.m. ET) when possible and when possible will provide maintenance notes five business days prior to the scheduled maintenance date that explain the system changes being made. When possible the Contractor will perform the maintenance on the UAT environment prior to the scheduled maintenance date so agencies can test the changes prior to live roll out. The maintenance must not proceed until there is agreement between the Contractor and the State on how maintenance shall proceed including but not limited to the utilization of the Contractor's backup site.

First Data Government Solutions provides all information to the State when performing emergency maintenance. We provide the patch or hot fix names, as well as the technical details for the patch. We do not proceed without agreement from the State. The exception is in cases of high-risk security issues and critical performance issues; in which case, changes need to be made before receiving approval from the State.

D3. **TSYS Processing Connectivity:** The Contractor must use a connectivity solution that obtains the lowest authorization cost with the State's credit card acquirer, Fifth Third Processing Solutions. The current Contractor is utilizing a Frame Relay connection to TYSY. The Contractor is responsible for all costs associated with installation and ongoing maintenance of the connection.

First Data Government Solutions has installed and uses a Frame Relay connection to TSYS. We will continue to be responsible for the costs associated with the network connection.

A.) **Server-level Logs:** The Contractor must have the ability to maintain an electronic server-level log of all transactions to and from its credit card processor.

First Data Government Solutions maintains Server-level Logs for 14-days. The logs contain transaction history to and from your/our credit card processor.

D4. **System Response Time:** Based on the activity level described in the contract, the server complex dedicated to the payment system will provide an average daily response time of three (3) seconds or less from the point at which the inquiry hits the server complex to the point at which the server complex responds with the requested web page. This performance and responsiveness is based on the following assumptions:

- The response time excludes any ISP backbone-related availability or performance latency problems in the connectivity between the Contractor and the State. The calculation of metrics related to the server complex's ability to support the daily hit rate will be based upon response times internal to the hosting facility.
- The Contractor will use the appropriate tools to monitor server-hit rates, concurrent user sessions and response time within the hosting environment.

  Since response time is, to a large degree, a function of application architecture, the State will work with the Contractor to optimize the application to assist in meeting the State's expected customer response time.
- This response time objective is subject to a validation by both Contractor and the State. The tool used to establish payment response time is the *Payment Response Time Report* as described in section 1.302.
- Daily response time is defined as a 24 hour period beginning at 12:00 p.m. ET and ending at 11:59 p.m. ET.

In the event the server complex is unable to successfully support the above specification and internal response time performance levels for the initial thirty (30) day period, the Contractor is responsible for re-engineering and upgrading the server complex to meet these performance requirements at no cost to the State. After the initial 30 day period the Contractor will be subject to the monetary assessments detailed in Article 1, Appendix N, System Response Time, Service Level Agreement.

The PayPoint system has a response time on average of less than three (3) seconds. The processor's architecture is another important factor to consider when you analyze response time. Whether you're processing a credit card authorization, eCheck, or PIN-based or PINless debit transaction, the PayPoint system sends a request message to these processor entities and waits for a response message. Once PayPoint receives a response message, we immediately update the database and get a response message back out to the State. Typically, we don't have issues with processor's performance; however, processor performance can impact the speed of a response message to the State. First Data Government Solutions acknowledges the States requirement that the PayPoint system has a system-wide daily average response time of less than three (3) seconds. First Data Government Solutions has negotiated with the State to define a mutually acceptable monetary assessment matrix. First Data Government Solutions' goal is to have a process that is easy to measure and quantify while maintaining current transaction pricing.

D5. **Implementation Testing:** The Contractor will submit a test plan to the Project Manager or designee that encompasses all systems, processes, and functionality. The test plan will include testing telecommunications lines and connectivity. The State may develop its own test plan to supplement the Contractor's plan. Upon completion of testing the Project Manager or designee will require a signature sign-off from the Contractor, Department of Information Technology (DIT) Project Manager, and other principal test participants.

Currently over 300+ payment programs from 15 different State departments are set-up to process payments through the existing system. The average monthly processing volume for the last twelve months is about 260,000 transactions. Overall, transactions for like periods are increasing monthly with PayPoint processing about 339,000 transactions in July 2010 for over $49,000,000.

The State has already validated the features and functionality of the PayPoint system, the Frame Relay connection to TSYS Processing, and the VPN Connection between the State and our Denver and Omaha data centers.

If, in the future, significant changes dictate the need for a test plan, First Data Government Solutions' will work with the State to define scope and provide the test plans necessary to complete additional Implementation testing.

By choosing First Data Government Solutions, the State relieves itself of the risks associated with converting to a new product and the burden of fully testing a new system and the telecommunication links. The State saves a significant amount of time and money using the PayPoint system.

D6. **Disaster Recovery / Back Up Site:**

a.) The Contractor must have a Disaster Recovery Plan that includes a primary and back up site to provide processing continuity. The back up site must be physically separated from the primary site by a distance of at least 10 miles. The back up site must be a functionally complete replica of the primary site, utilizing identical software and hardware settings and values, and will have performance equal to the primary site. The historical customer data must be identical to the primary site.

b.) When the Contractor changes site locations it must be transparent to State applications. Planned Disaster Recovery rollovers must be communicated to the State with a thirty day (30) day notice. The Contractor is expected to test rolling to its Disaster Recovery site a minimum of once annually.

c.) The Contractor shall monitor all changes in site events to ensure outcome is as expected. State applications will be monitored to ensure all types of applications are functioning, such as WEB, manual key entry, and interfaces.

d.) Contractor will have a fall back plan in the event that a change in site location causes problems for processing, such as inability for WEB applications to function, etc.

e.) The roll over from the primary to the back up site must be completed in one hour or less from the time the primary site fails or for a scheduled roll.

Also see Section 2.203

First Data Government Solutions has a primary and back-up data center that PayPoint operates in today. The Primary data center is located in Denver Colorado. The backup data center is located in Omaha Nebraska. First Data Government Solutions has a comprehensive disaster recovery and business continuity plan in place that enables us to quickly switch between these sites with minimal to no loss of data. If a disaster does occur, the decision is made quickly to transfer processing to Omaha. The Operations team rolls the DNS to the new site and we're operational. The databases are continuously replicated between the two sites to prevent loss of data and the telecommunication links to TSYS and other processors are installed and operational in Omaha.

Addressing item b: FDGS will perform annual testing of the disaster recovery site. This will be accomplished by performing stress and functional tests. These tests will ensure that the solution is capable and available for a roll in case of a disaster.

Addressing item e: The time needed to roll from the primary site to the backup location may last from 1 to 2 hours. Upon detection of an issue or outage, FDGS will perform an assessment of the issue to see if the problem may be corrected within an acceptable time, or if the solution needs to be rolled to the backup site. This decision time is not included in the roll duration.

D7. **Redundant Hardware / Software:** The Contractor is required to maintain adequate back up procedures and equipment in case of system failures to meet availability and response time requirements.

First Data Government Solutions has built redundancy into every layer of the architecture in both Denver and Omaha data centers. Monitoring systems are in place to detect problems and allow the support staff to expediently correct the issue or remove the impacted server from the content switch.

D8. **Application Program Interface (API):** The Contractor must provide APIs to facilitate its payment processing functionality. The list of data requirements is defined in **Appendix D - API Data Requirements**. The Contractor must provide a variety of methods for accessing their services. The APIs shall include but not be limited to:

a.) Web Services utilizing Extensible Markup Language (XML), Simple Object Access Protocol (a.k.a. SOAP), Web Services Description Language (WSDL)
b.) Secure HTTP
c.) A generic web page that may be invoked from the Contractor's system by a State application that is used solely for making an electronic payment. The page must allow the State application to specify the appearance of some of its attributes including but not limited to the title of the page, page header, page footer, and confirmation text when a successful payment is made.
d.) A customizable generic Web and IVR hosted solution as described in requirement B14.
e.) A batch interface for transfer of multiple transactions from a State application to the Contractor in a secure manner. The State application will submit the batch of transactions to the Contractor and the Contractor will immediately process the transactions and generate a response file that contains the results for the processed transactions. The Contractor will generally provide the response file in 10 minutes or less, depending on the number of transactions contained in the batch. The Contractor will transmit (push) the response file back to the State application.

PayPoint provides multiple integration methods for the State of Michigan and meets requirements a through e. The State may interact directly with the PayPoint gateway through Web service or HTTPS API calls. The State may also interact with the gateway by providing batch payments through an XML import. Additionally, PayPoint provides a Consumer Payments interface that allows the State to create a branded and customizable Web site using a Web-based template interface. The integration methods are detailed in the PayPoint Merchant Integration Guide . This includes API definitions and specifications.

D9. **Virtual Private Network:** The Contractor must provide Virtual Private Network (VPN) tunnels between the State and its primary and secondary sites. The tunnel at each site must be redundant and must be capable of automated failover to ensure uninterrupted connectivity with the State. Switching between the Contractor's primary and secondary sites must be developed jointly with the telecommunication experts of the Contractor and the State and must comply with State of Michigan Policies, Standards and Procedures as defined in the document titled *Vendor Gateway-to-Gateway VPN Service* located in **Appendix K**.

First Data Government Solutions currently provides the VPN connection between the State, our primary site in Denver, and the secondary site in Omaha.

Provisioning – First Data Government Solutions uses the Internet, so it's not necessary to provision dedicated circuits. However, on an individual basis, we can support VPN connections. We have done this for the State of Michigan in the past.

Protocol – First Data Government Solutions creates an IPSEC 3DES tunnel.

Failover – In both our primary data center in Denver, and our secondary data center in Omaha, we have redundant routers. Should a router within either facility fail, the secondary router at that facility will automatically take control. Once the failed router recovers it will then resume its role as the primary router.

D10. **Erroneous Transactions:** Erroneous transactions are those transactions that are successfully processed by the Contractor's system without a response being received by the agency application and customer. This causes the customer to reinitiate the transaction and may result in the customer's account being charged more than once. It may also result in the failure of agency legacy systems to be properly updated for a successful transaction causing reconciliation problems. Some erroneous transactions could be caused by inconsistencies in the time-out values of system hardware/software.

The Contractor Must:
a.) Have software tools in place to detect, trace, and prevent erroneous transactions.
b.) The product must not commit the object of the transaction for settlement or further processing when an erroneous transaction is detected.

The PayPoint application has a configurable, duplicate payment check to limit erroneous transactions. The State can control the checks by configuring the duration, in minutes, where the system will accept a duplicate payment.

The transaction parameters detect and prevent the erroneous transaction by validating the application identifier, the date/time stamp, the dollar amount, the last four (4) digits of the account, and the custom reference field (if the custom reference field is used in the duplicate payment configuration).

PayPoint will only send successfully authorized transactions for settlement.

D11. **Processing Logs:** The Contractor system must maintain a log of transaction activity from the time a transaction is received until the time a response is sent to the application. Log data must be provided to the State upon request to assist with problem resolution. Logs must be retained for 14 days.

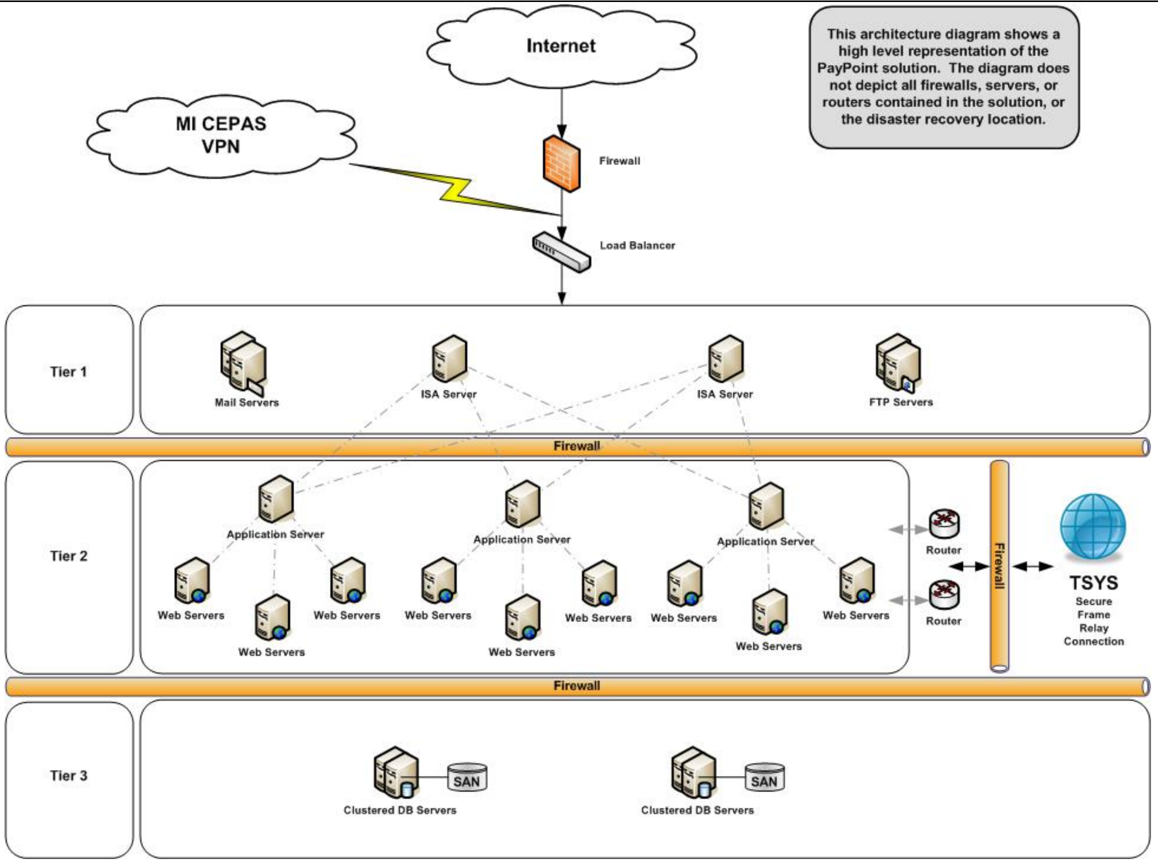
First Data Government Solutions maintains a transaction activity log and can provide to the State upon request. PayPoint retains detailed logs for 14 days but maintains audit data for two years on-line and off-line for seven additional years.

D12. **System Upgrades / Changes / New Releases:** The Contractor will:
a.) Notify the Contract Compliance Inspector or designee at least 60 days in advance of when system changes (hardware/software) are planned.
b.) Provide detailed documentation that describes the changes at least 30 days prior to implementation. The documentation must describe the existing process, the new process, what changed, and the reason for making the change.
c.) Place a testable version of the changes in the Test Environment at least 30 days prior to implementation to allow for agency application testing.

First Data Government Solutions will provide a 60-day notice for PayPoint Releases and Hardware upgrades. The notification is sent to the State via email that includes: the Client Release Notes, Integration Guide, User Guide, and details for a hardware upgrade. A 60-day notification may not be possible for third party vendors (i.e. Microsoft patches). We provide Client Release Notes for PayPoint Releases and hardware upgrade documentation 30-days prior to implementation. A 30-day period may not be possible for third party vendors (i.e. Microsoft patches). A testable version of PayPoint Releases and planned hardware maintenance are available 30-days prior to implementation. The exception is a hotfix to address a production issue.

D13. **Network Architecture:** The Contractor must:
Supply a comprehensive network diagram and supporting narrative with the proposal. Included will be diagrams and details on how the system processes payments to Vital including any software or Third Party vendors used.

The First Data Government Solutions' PayPoint environment is a proven solution and currently processing payment transactions for the State of Michigan through this architecture. A credit card transaction request is passed from the internet user through the first set of routers, and firewalls. The transaction goes through the load balancing content switch to the ISA/web servers in Tier 1. The ISA servers send requests to the Application servers through another set of firewalls in Tier 2. The Application servers process the business rules and communicate to the web servers, the database servers located in Tier 3, or to TSYS. Payment transactions to TSYS occur over a secure frame relay connection dedicated to the current Michigan applications. Approvals or declines are then sent back to First Data from TSYS and relayed back to the internet user.



This architecture diagram shows a high level representation of the PayPoint solution. The diagram does not depict all firewalls, servers, or routers contained in the solution, or the disaster recovery location.

A larger view of the network architecture can be found in Attachment E – Network Architecture.

D14. **Test Environments:** The Contractor will:

a.) Provide access to fully functioning test environments that are a replica of the production environment.
b.) Ensure transactions processed in the Application Development Test environment will not be processed for settlement.
c.) Ensure test results for each testing application must be separate from other application test results.

d.) Provide a separate feedback file that will be generated for transactions processed in the test environment.

e.) Provide multiple test credit card numbers (for all cards- Visa/MC, and Discover) and test bank account numbers to facilitate transaction testing.

First Data Government Solutions provides a User Acceptance Testing (UAT) environment that matches the production environment from a PayPoint perspective. The exception is that 30-days prior to a new PayPoint release, the UAT environment will contain the updated release and will be out of sync with the production environment. The UAT region meets the requirements (a) through (e).

A.) **Testing Environments:** The Contractor must make available two individual testing environments for the State's use. These will be referred to as the Applications Development Testing (ADT) environment and a User Acceptance Testing (UAT) environment.

First Data Government Solutions has two testing environments Quality Assurance (QA) and User Acceptance Testing (UAT). All PayPoint Releases are tested in the QA region by internal resources prior to being moved to UAT. The UAT environment is for external acceptance testing of the PayPoint Release, as well as front-end application testing.

B.) **Application Development Testing Environment:** This environment will be used if necessary by developers to develop and perform reiterative testing of computer code prior to releasing to UAT. It must replicate the Contractor Production environment while supporting all functions and applications defined in production. This environment must be independent of all other testing environments and accessible to only those authorized to conduct testing of a State application. The environment must be available 24x7x365 except for previously identified maintenance windows.

The QA environment matches production, with the exception of the new PayPoint release being tested prior to moving to UAT and production. Client acceptance testing will not be performed on the QA environment.

C.) **User Acceptance Testing (UAT) Environment:** This environment will be used by the State for testing of products promoted from application development testing environment into the UAT environment. It must replicate the Contractor Production environment while supporting all functions and applications defined in production and support end to end testing of credit card authorization, ACH and credit card settlement, and refunds prior to an application being migrated to production. Contractor must provide credit card numbers and e-check account numbers for testing in UAT. This environment must be independent of all other testing environments and accessible to only those authorized to conduct UAT testing of a State application. The environment must be available 24x7x365 except for previously identified maintenance windows. The UAT environment must produce a daily UAT Feedback File (see D15 below) that contains the previous days test transaction detail for transactions processed in the UAT environment.

First Data Government Solutions provides a User Acceptance Testing (UAT) environment that matches the production environment from a PayPoint perspective. The exception is the 30-days prior to a new PayPoint release going into the production environment. The UAT region meets all above requirements.

D.) **Repeatable Test Cases in Application Development:** The Contractor must supply a set of at least 6 repeatable test cases that validates the API is properly integrated into an application in the Application Development Test domain. Every function of the Contractor's product must be in the set of test cases. The test cases must be evaluated using pass or fail, yes or no logic.

First Data Government Solutions provides repeatable test scenarios in the PayPoint Merchant Integration Guide .

D15. **<u>Feedback File</u>:** The Contractor will supply a daily feedback file that contains details of the previous day's transactions. This file will be used to update agency legacy systems and as a reconciliation tool. The following tasks relate to the Feedback File:

A.) **<u>Feedback File Contents:</u>** The anticipated contents of the feedback file are defined in **Appendix E - Feedback File Data Elements**.

a.) The file shall be in a straight or delimited ASCII format.
b.) The feedback file will not contain sensitive information such as credit card numbers, account numbers, or Social Security Numbers in their complete unaltered form.
c.) All sensitive information must be truncated.
d.) The dollar value of the transactions in the feedback file must equal the dollar value of the day's transactions in the settlement batches for each application.
e.) Refund transactions included in the feedback file must contain enough information to allow for linking the refund back to the original transaction.
f.) At the discretion of the State, the file must be one file, sub-divided and sorted by agency application or a zip file containing separate files for each agency application.
g.) To compensate for unexpected service interruptions and common Federal and State holidays, the daily feedback file must be available for five (5) or more calendar days after creation. It must be available in archive for a minimum of 60 calendar days.

First Data Government Solutions provides a feedback file in the form of a daily Posting File. The Posting File does not contain sensitive data and truncates information such as credit card numbers. The Posting File is acceptable for use with payment reconciliation and can be generated for the site level or application level. The feedback files (Posting File) will be available for five (5) or more calendar days and are available upon the State's request. We archive feedback files for a minimum of 60 calendar days. First Data Government Solutions meets requirements (a) through (g).

B.) **<u>Feedback File Retrieval:</u>** The Contractor shall:

a.) Make the file available for pick up by 6:00 a.m. ET.
b.) Ensure pick up shall be accomplished using Secure Shell (a.k.a. SSH), a secure FTP method.
c.) Maintain the secure FTP server and the State will maintain the secure FTP client.
d.) Ensure contents of the feedback file are encrypted at 128 bits or better during transfer from the Contractor to the State.
e.) Inform the State designated contact if the file is unavailable at the agreed time.

First Data Government Solutions meets the Feedback File retrieval requirements. The Feedback File is available daily at approximately 5:30 a.m. ET on a secure FTP Server. In order to access the SFTP server, the State is provided with a unique User ID and Password. The State needs to use a Secure FTP method to pick up the file from the FTP Server. The Feedback is encrypted with PKWare before placing on the FTP Server. First Data Government Solutions contacts the State via email or telephone to inform them that the Feedback file is not available at the agreed time.

D16. **<u>Data Retention</u>:** Transaction data must be retained for a minimum of 24 months on-line. Audit data which includes, but is not limited to, adding, deleting and modifying user accounts must be retained for a minimum of 7 years.

First Data Government Solutions retains audit and payment information for 24 months on–line, and is stored off-line for a period of five (5) years, for a total retention span of seven (7) years.

a.) The Contractor must remain in compliance with Payment Card Industry Data Security Standards (PCIDSS) as long as the contractor is storing data for the State.

First Data Government Solutions is in compliance with Payment Card Industry Standards (PCI) and renew our compliance on a yearly basis.

D17. **Transition Assistance:**

a.) To assist with transition of State customers with registered and scheduled accounts, the Contractor will facilitate transfer of a file in XML format to a destination identified by the Project Manager or designee that contains all information related to the customer's enrolled and/or scheduled accounts. The file will contain full credit card numbers, bank account numbers, enrollment IDs, Agency Application IDs, and any other information collected from the customer. A secure process will be utilized to transfer the file. The file will be transferred at an agreed upon time. It is anticipated this will be prior to expiration of the contract and will be part of the migration plan to the new Contractor. If necessary, a second file will be transferred to migrate registrations that have been created since the first file transfer. Timing of the transfer of this file will need to be determined but is expected to be near the completion of the migration to the new Contractor.

b.) The Contractor will continue to securely store State of Michigan payment data for a period of six (6) months following expiration of the contract. Audit log data must still be retained for 7 years. The State will retain all existing payment functionality and be capable of accessing the data through existing methods during this time period. The Contractor will continue to provide the daily feedback file during this period. The State will retain the capability to process refunds for transactions that were processed on the Contractor's system. The Contractor will invoice the State monthly for any refund transactions processed. The per item charge will be based on the monthly pricing tier the volume of transactions falls under. During this period, user access will be limited.

c.) At the end of the six (6) month period, with State of Michigan approval, the Contractor will destroy all stored State of Michigan data and documents that contain sensitive or confidential information. The Contractor will also disable all State of Michigan user access to their system. The Contractor will provide written affirmation on the destruction of sensitive and confidential information to the Project Manager or designee upon destruction of the data. Also see section 2.218.

First Data Government Solutions provides an XML file of registrations with all information stored in PayPoint. The PKWare Encrypted XML file is placed on the Secure FTP Server. The State picks up the XML file using a User ID and Password. The State uses a Secure FTP product to pick-up the file on the Secure FTP Server. First Data Government Solutions coordinates with the State for a date and time to have the XML file available. We securely store the State's payment data for six (6) months by storing the information in PayPoint. The State is able to access the data using the PayPoint Administration Site. First Data Government Solutions provides a daily feedback file by placing the file on the Secure FTP Server. At the end of the six (6)-month period, with the State's approval, we do an automated purge of all transaction data stored in the PayPoint Databases. The business contact deletes the State's users from the PayPoint System. The business contact provides, to the State, a written affirmation via email on the destruction of sensitive and confidential information.

D18. **Operational Internal Controls:** The Contractor shall ensure that manual and automated systems have sufficient internal controls, including approval processes, to minimize the risk of error. Examples of such controls include:

a. Ensuring when moving from test to production that only the intended State applications are affected.
b. Ensuring that technology infrastructure is well documented.
c. Ensuring that checklists or similar controls are utilized when performing upgrades, system changes, or maintenance.
d. Ensuring that disaster recovery or redundant sites are configured in the same manner as the primary site.
e. Ensuring when changes are made or when an outage occurs that all types of connections are working, such as WEB, Manual Entry Screens, Interfaced IVR processes, etc.
f. Continuously monitoring the system to quickly identify unplanned system outages, slow response times, and other processing errors. Immediately alert support staff when problems are detected.

First Data Government Solutions has a two-step verification process in place for configuring an application. A business contact adds or changes the configuration per the State's request. A second business contact verifies that information input into the configuration is correct. A business contact provides screen shots of the configuration, adds or changes are sent to the State via email in a password protected zip file. First Data Government Solutions is in the process of automating the process, which will be available in a future release.

First Data Government Solutions currently has a dedicated Configuration Management group whose responsibilities it is to migrate new code into QA, UAT, and production environments. All of these code moves have an audit trail and require approvals prior to the code being moved. A weekly change control review meeting between the Chief Technology Office and the Global Technology Solutions teams discuss code moves.

First Data Government Solutions primary data center is in Denver, Colorado and the disaster recovery data center is in Omaha, Nebraska. Applications are rolled to the DR site by manually rolling the DNS.

Confidential and Sensitive information that needs to be stored is encrypted in the database, and masked when displayed to all users of the application. Data is replicated in real-time to the DR facility

First Data follows operational procedures with performing updates or system changes to the PayPoint solution.

Addressing item b: Infrastructure documentation is updated when modifications are made.

Addressing item c: FDGS follows installation checklists when updating the system.

Addressing item d: The disaster recovery site is updated and configured in the same manner as the primary location.

Addressing item e: Regression testing is part of the update and installation plans to ensure that the system retains all functionality.

Addressing item f. FDGS has a client support staff that monitors the solution and receives alerts for outages and slow response time.

D19. **Mapping and Translation:** If the contractor is not currently providing this service to the State of Michigan, the Contractor must develop the translation process to map the current API structure and functions being used by state applications to the Contractor's API structure and functions.

The contractor is responsible for all costs associated with the translation process.

As the incumbent vendor and the source of the current API structure, our solution meets this requirement today.

E. CONTRACTOR SUPPORT

E1. **Dedicated Business and Technical Contacts:**

a.) The Contractor must provide dedicated business and technical contacts for the term of the contract. Contacts must be available between 8:00 a.m. and 5:00 p.m. ET. Each contact or contact group shall have suitable back up(s) that has similar knowledge and abilities. The Contractor will provide a contact list containing phone numbers and email addresses for the designated contacts and back ups. The business contacts will possess thorough knowledge of the Contractor's system functionality and processing capabilities in order to act as a resource for business related questions and issues. During regular business hours (8:00 a.m. – 5:00 p.m. ET) system problems will be reported to the business contact or contact group.

b.) The technical contact will support the State's information technology staff. The technical contact will possess thorough knowledge of the Contractor's technical processes, application integration issues, programming parameters, telecommunication issues and other technical issues in order to act as a resource and central point-of-contact for technical questions, problems, and issues.

c.) In order to document issues and problems, the contacts shall maintain an issues tracking or support ticket log. The log will contain dates, problem description, resolution, and other details related to the issue. The log will be made available to the State periodically as requested.

First Data Government Solutions currently provides a primary business contact and a primary technical contact to the State. The contacts are available between 8:00 a.m. and 5:00 p.m. ET. The contacts have a Business Operations Group that has business and technical knowledge, and ability to address the State's questions or concerns.

As the incumbent, we provide dedicated business and technical Help Desk contacts today. In the event we would need to change personnel at the time of the award or in the future, we will work with the State to assign mutually acceptable replacements while maintaining business continuity through the transition.

First Data Government Solutions logs business or technical issues or problems through our support ticketing system and tracking spreadsheets, as appropriate, and is willing to review the items on a monthly basis or as needed if a major issue is taking place.

E2. **24 x 7 Support:** The Contractor must provide 24 hour per day, 7 day a week support. The Contractor will provide a toll-free phone number and pager number to contact the Contractor after-hours support staff. System problems discovered after regular business hours will be reported to the Contractor's after-hours support staff. The Contractor must have tools and staff in place to monitor that the system is up and processing as expected. If the Contractor's system experiences unscheduled downtime or other processing issues, the support staff will immediately notify the designated State contact(s).

First Data Government Solutions provides support 24 hours per day, seven (7)-days a week. A toll-free number is provided to access our support personnel. We have attached the PayPoint Help Desk MI CEPAS Escalation Process document, Appendix O, that provides the State with contact information and phone numbers.

First Data Government Solutions monitors the system to validate that transactions are processing as expected. If there is an outage, we contact the State with the information via email during business hours, and with an email and phone call to the designated State contacts after hours.

E3. **Severity Codes:** The Contractor's support staff will respond to problems in accordance to Severity Codes assigned to the problem by State staff. The Severity Codes and expected response times are detailed below:

- Severity 1 – means a problem that has critical business impact on the State. The service is not usable. The Contractor response time is 30 minutes or less.
- Severity 2 – means a problem that has a major business impact on the State. Important function or service is not available. The Contractor response time is 2 hours or less.
- Severity 3 – means a problem that has a minor business impact on the State. The service is not seriously affected. The Contractor response time is 4 hours or less.
- Severity 4 – means a problem that has no business impact on the State (for example, a question). The Contractor response time is one day or less.

Responding to problems means acknowledging receipt of the problem notification and actively working to resolve the issue with a goal of rectifying the problem within the designated timeframe. It is recognized that not all issues can be resolved within the designated timeframe. The Contractor will periodically update State staff as to the progress being made and an estimated time the problem will be resolved.

First Data Government Solutions recognizes and follows the above Severity Codes. The Severity Codes are First Data's unique codes provided to the State. First Data Government Solutions agrees to provide periodic updates to the State when issues cannot be resolved within designated time frames, and follows established escalation procedure to make sure the relationship management team is kept apprised of issues that are not meeting response or resolution expectations. An updated escalation and response time plan is provided to the State in Appendix O, PayPoint Help Desk MI CEPAS Escalation Process.

E4. **System Business Documentation:** The Contractor must provide the State with detailed documentation describing the Contractor's entire system, including processes performed by sub-contractors or other business partners. Business documentation must include, but is not limited to:

a.) Accessing the system.
b.) Pictures of system screens and detailed instructions on how to use them.
c.) Description of system components.
d.) Codes and parameters used.
e.) Reporting functionality.
f.) Security.
g.) Instructions for set up of agency applications.
h.) Frequently Asked Questions.
i.) Descriptions of upgrades

First Data Government Solutions provides the above mentioned documentation today.

The PayPoint User Guide includes details on how to use the PayPoint Administration Site. The User Guide provides information on how a User Accesses the system and searches for payments, runs reports, monitors settlement, and Frequently Asked Questions.

A PayPoint Merchant Integration Guide with details on how to develop an API, codes and parameters, description of system components, file layouts, etc. is provided.

We provide a PayPoint Application Form that allows the State to determine the configuration details for the applications. The PayPoint application provides instructions on how to fill out the form and submit it to First Data Government Solutions.

Client Release Notes are provided for each release of PayPoint. A new Release includes upgrades to PayPoint. The Client Release Notes provides detailed information on the upgrades by providing how it works today, what has changed, and Special Instructions.

E5. **System Technical Documentation:** The technical documentation must describe the system in detail to foster complete technical understanding of the Contractor's entire product in all its environments and must include:

a.) **Data Dictionary:** A complete data dictionary must be included describing every data item used in the Contractor's system.

b.) **Definitions:** Special terminology used in the Contractor's documentation must be defined in a glossary. For example, the term CVV2 is explained as Card Verification Value 2 for Visa.

c.) **Naming Conventions:** Naming conventions used in the Contractor's system must be thoroughly discussed.

d.) **Minimum and Recommended Server Configuration:** The Contractor's documentation must specify the minimum and recommended server configuration for implementation and deployment of its system.

e.) **Required Software Add-ons:** Required software add-ons that enable implementation and deployment of the Contractor's system must be thoroughly discussed. For example, if a secure FTP server is required for communication to the system, the documentation tells the details of what is expected of the State. This includes but is not limited to products sold or distributed by the Contractor or other software providers.

f.) **Internet Browser Specifications:** Compatibility with specific Internet browsers is discussed thoroughly in the Contractor's documentation.

g.) **Availability:** The Contractor's technical documentation is available on-demand in an electronic form and media through its web site or other means acceptable to the State.

h.) **Updates:** When the Contractor plans an update to its system new documentation is available thirty (30) or more days prior to the release and implementation of the update. The new documentation is comprised of two parts. The first is a description of the update and the changes that it affects on the Contractor and State systems. The second is a complete revision of the system documentation manual or user guides.

i.) **Single Versions:** Contractor documentation is controlled so that there is a single current version at any given time. Documentation is clearly marked with version numbers and effective begin and end dates.

j.) **Telecommunication Configuration:** Contractor documentation clearly explains the telecommunication specification and protocols required for implementation and deployment of its system by the State.

k.) **Proprietary Nuances:** The Contractor documentation fully discusses any technical proprietary nuances essential to the implementation and deployment of its system by the State. For example, if data downloads from the Contractor site requires a special version or commercial brand of an FTP server, this is disclosed and discussed.

l.) **Describes Functions:** Every electronic payment function of the Contractor's system is described in detail. Using the instructions in the documentation, the State developers will be instructed in detail how to build applications to utilize the Contractor's system.

m.) **Provides Examples:** The Contractor documentation provides computer programming examples. The examples guide State developers in the effective use of its system.

n.) **Testing Explained:** The Contractor documentation thoroughly explains how a State developer utilizes the Contractor's test cases in order to test State application development.

o.) **Web Service:** The Contractor documentation clearly and thoroughly explains its implementation of Web Services including Simple Object Access Protocol (a.k.a. SOAP), Extensible Markup Language (a.k.a. XML), and Web Services Description Language (a.k.a. WSDL).

p.) **HTTPS:** The Contractor documentation clearly and thoroughly explains its implementation of Secure Hyper Text Transfer Protocol (a.k.a. HTTPS).

q.) **Web Service and HTTPS URL:** The Contractor documentation clearly names the URL addresses for accessing all its technical environments. The Initial Test, System Test and Acceptance and Production environments are completely discussed.

r.) **Web Service WSDL:** The Contractor's Web Service WSDL is available on-demand in an electronic form and media through its web site or other means acceptable to the State.

s.) **Implementation Project Guidelines:** The Contractor documentation includes a section on technical project management that guides State project managers in the initiation, planning, execution, control and closeout of State development efforts.

t.) **File Layouts:** The Contractor's documentation includes a clear, concise and separate file layout for all files exchanged between the State and the Contractor.

u.) **Organizational Authorization and Approval Forms:** Any forms required for the executions of development efforts are included in the documentation with explicit directions on their use.

v.) **Frequently Asked Questions:** Common questions asked by other users of the Contractor's system.

As the incumbent vendor, our solution meets this requirement today. First Data Government Solutions provides the State with a PayPoint User Guide with details on how to use the PayPoint Administration Site. The User Guide provides information on how a User Accesses the system and searches for payments, runs reports, monitors settlement, and Frequently Asked Questions.

A PayPoint Merchant Integration Guide with details on how to develop an API, codes and parameters, description of system components, file layouts, etc., is provided

We provide a PayPoint Application Form that allows the State to determine the configuration details for the applications

The PayPoint application provides instructions on how to fill out the form and submit it to First Data Government Solutions.

Client Release Notes are provided for each release of PayPoint. A new Release includes upgrades to PayPoint. The Client Release Notes provides detailed information on upgrades by providing how it works today, what has changed, and Special Instructions. In the event there is technical data needed outside of the referenced documents, First Data Government Solutions will provide any non-confidential data needed to enable the State to successfully foster complete technical understanding of the Contractor's entire product in all of its environments.

E6. **Best Practices:** The Contractor will provide a document with a comprehensive discussion of technical best practices to assist agencies in integrating with the Contractor's system.

First Data Government Solutions will conduct a best practice discussion with the State, as needed. This is normally passed on to the Agencies from the State. Best practice data is part of the user guide and merchant integration guide that can be downloaded from the PayPoint site. If additional data is needed, First Data Government Solutions will work with the State to understand the requirement and provide the appropriate amount of additional detail.

E7. **Training:** The Contractor will provide detailed and comprehensive training that covers all aspects of the functionality of the Contractor's system. Training will include handouts and other documents as required. Initially the Contractor will provide a training session(s) to train the Receipts Processing CEPAS Agency Liaisons and management (see section 1.202, State Staff, Roles, and Responsibilities). The Contractor will then provide multiple training sessions to initially train agency users. Once initial training has been accomplished, the State will assume responsibility for subsequent training of basic system functionality.

The Contractor may be required to provide training for extensive system changes/upgrades at the discretion of the state's Project Manager or designee.

As the incumbent vendor, our solution meets this requirement today. First Data Government Solutions has provided the State with training. This training has enabled State staff to provide training to new Agencies. If changes to the PayPoint system dictate additional training, First Data Government Solutions will work with and train the State on the new functionality. The State will be responsible for passing the training down to the Agencies.

E8. **Demonstration Web Site and Training Material:** The Contractor will provide access to a Demonstration Web Site or inter-active software and training materials for purposes of demonstrating the Contractor's system functionality to State agencies.

As the incumbent vendor, our solution meets this requirement. First Data Government Solutions has a demonstration User Acceptance Testing Web site the State uses for training purposes today.

E9. **CEPAS Incident Reports:** A CEPAS Incident Report is a State form used to document severe system problems that affect State customers or State agency reconciliation processes and requires attention and resolution by the Contractor. CEPAS Incident Reports are assigned a unique Incident Report Number in the format of YYMMDD representing the date the incident occurred. See a copy of the CEPAS Incident Report form in **Appendix F - CEPAS Incident Report**.

a.) Once the problem is resolved, the Contractor will document its response and action taken by completing Part 3 of the form.

b.) The Contractor will maintain and make available a document to summarize the status of all Incident Reports issued by the State. This "Incident Report Summary" will be in the form of a table or spreadsheet and contain relevant information such as Incident Report Number, Date of Incident, Summary of the Problem, Contractor response, Resolution Date, Status (Open, Closed), etc.

c.) The Contractor will respond to incident reports within 10 business days.

d.) The Contractor business contact will email the updated Incident Reports and Incident Report Summary to the State.

First Data Government Solutions meets this requirement today.

First Data Government Solutions updates the State's incident reports and the Incident Report Matrix and makes them available to the State within 10 business days. The business contact emails the updated Incident Reports and Incident Report Matrix to the State and places them in eRoom.

E10. **New Account Set-Up:** The Contractor must complete set-up of new credit card and E-Check accounts within 5 business days of request from the State.

As the incumbent vendor, our solution meets this requirement. First Data Government Solutions completes the set-up of a new Credit Card application within five (5) business days of the request from the State.

The set-up of a new eCheck application is completed within 10 business days of the request from the State.

First Data Government Solutions processes a two-step verification for configuring an application. A business contact adds or changes the configuration, per the State's request. A second business contact verifies that information put into the configuration is correct. Screen shots of the configuration additions or changes are provided to the State via email in a password-protected .zip file. We are in the process of creating a Web interface to review, upload, and verify new accounts. Templates will be available in the future to reduce repetitive input and labor.

F. BANKING

F1. **ACH Application Deposit Identification:** At agency application set up for ACH debit programs, the CEPAS Agency Liaison will provide a unique identifier to identify agency deposits. The unique identifier will assist agencies in identifying daily deposits from the Contractor's system to bank account statements.

First Data Government Solutions provides a unique 10-digit Company ID, which is used to identify the Agency from which the credit or debit to the account is drawn. Companies can use this to set-up debit filters with their FI to only allow debits from this Company ID, unless they approve any others. The second field in the NACHA File that will show up on their bank statement is the Company Entry Description. This is a 10-character field that is set-up in the merchant master record under the Subscriber Periodic Statement Description field.

F2. **Posting of Agency ACH Deposits / Returns:** At agency application set up for ACH debit programs, the CEPAS Agency Liaison will provide the bank account information for the Contractor to deposit agencies daily transactions. The total dollar amount of the daily settlement batch for the agency application will be deposited by initiating an ACH credit to the specified applications bank accounts. Any return items received by the Contractor for the applications will be posted individually to the applications accounts.

First Data Government Solutions provides a daily deposit to the application by initiating an ACH credit to the specified Merchant bank accounts.

Returns are posted as a total amount to the application, and are not individually broken out on the merchant statement. Individual return records are broken out separately on the PayPoint Posting File.

FDGS misunderstood the question and does post returns individually to the applications account.

F3. **Company Name and Entry Description:** At agency application set up for ACH debit programs, the CEPAS Agency Liaison will provide the agency name and short description to be used to populate the Company Name and Company Entry Description of the ACH Batch Header Record. The Company Name allows 16 alphanumeric characters and the Company Entry Description allows 10 alphanumeric characters. This information will appear on the customers' bank statements to identify the source of the withdrawal.

First Data Government Solutions supports the Company Name and Company Entry Description that appear on the customers' bank statement that identifies the source of the debit.

F4. **Timing of ACH Deposits:** The Contractor will transfer the daily file of ACH debit settlement batches to its ODFI for inclusion in the first ACH window following settlement cut off (11:59 p.m.). If the State loses interest on ACH transactions because of late settlement of transactions, the Contractor may be assessed damages. The damages will be assessed based on a calculation of the lost interest earnings on the value of the ACH transactions settled late times the monthly earnings credit rate earned by the State at Bank of America and the number of days delayed in settling the transactions. If the State's customers incur late penalties or interest charges as a result of failure of the Contractor's system, those penalties may also apply (e.g. taxes paid late).

Files are sent at approx. 10:00 AM ET and 7:00 PM ET each day. Michigan is set up with same day processing with a cut-off time of 5:00 PM ET. This means that all transactions that TeleCheck has an accept tag for, that were processed from 5:00 PM ET the day before until 5:00 PM ET current day, are processed by the Settlement engine. The ACH file is then created and transmitted to the ODFI for processing into the ACH Network. Our cut-off time with the ODFI's is 8:00 PM ET.

F5. **Credit Card Deposits:** The State's credit card acquirer facilitates deposit of credit card funds generated through the Contractor's system. The Contractor must settle transactions daily to TSYS in order for TSYS to provide details to the State's credit card acquirer.

As the incumbent vendor, our solution meets this requirement. First Data Government Solutions settles transactions to TSYS seven (7) days a week.

G. IMPLEMENTATION

G1. **Migration and Implementation:**
The migration of State applications and implementation of the Contractor's system must be completed within twelve (12) months of Contract Effective Date. The Contractor must provide a detailed implementation project plan that includes a preliminary schedule for migrating agency applications to the Contractor's system.

The State is currently using the PayPoint system, provided by First Data Government Solutions; therefore, there is not a migration effort associated with this proposal. We continue to support the implementation plans as defined and managed by Treasury. Over the past 6-½ years, our partnership has delivered an enterprise payment system to the State and has successfully implemented over 300 applications. By choosing First Data Government Solutions, the State would not need an initial migration and implementation plan and schedule.

The contractor will submit a finalized project plan after the Contract Effective Date.

G2. **Conversion Time:**
Departments must be converted to the new Contract prior to the expiration of the current contract. The current contract expires November 30, 2011 and the expected conversion time is 12 months. The Contractor must provide a draft implementation schedule that includes sufficient time for all conversion and testing activities. The Project Manager or designee will work with the Contractor to produce an implementation schedule that meets the needs of the State.

The State is currently using the PayPoint system provided by First Data Government Solutions; therefore, there is no conversion effort associated with the First Data Government Solutions' proposal. We continue to support the implementation plans defined and managed by Treasury. By choosing First Data, the State relieves itself of the risks associated with a conversion effort to a new product and saves time and money associated with designing, constructing, testing, training, and implementing a new system.

G3. **Agency Application Implementation**: The Contractor must be able to implement new agency applications during conversion of existing applications. More complex agency applications must be implemented by a date deemed acceptable by the state's Project Manager or designee.

The First Data Government Solutions' support team continues to work with Treasury to implement new Agency applications, according to the implementation plan defined and managed by Treasury. By choosing First Data, the State can focus its time and energy on new Agency applications, especially the more complex implementations.

G4. **Testing:** The Contractor will perform end-to-end testing of each agency application to ensure all functionality is working properly. Testing will include settlement of funds. The Contractor and an agency representative assigned to the testing effort will be required to sign off to verify that testing was satisfactorily completed.

The State is currently using the PayPoint solution provided by First Data Government Solutions. Over 300 applications have been successfully deployed. Since PayPoint is currently hosting the State's applications, there will be no conversion effort needed and testing on existing applications will not be required. For this reason, too, new applications developed and implemented by the State will experience additional benefits through quicker implementation and testing processes.

H. **SOFTWARE MODIFICATION**

a) Supplier will provide Software Modification on a fixed-price or Time and Material ("T&M") basis as defined in a mutually agreed-upon Change Request. The Modification Rates defined in this proposal will be used for all Software Modification provided either on a fixed-price or T&M basis.

b) Supplier and MDTMB will use the Change Management process as established in the State standard project management methodology. No Software Modification work will be performed until a mutually agreed-upon Change Request has been executed by both Supplier and MDTMB.

c) The Change Management process may be modified as mutually agreed by Supplier and MDTMB.

d) The Acceptance Criteria for each Change Request will be defined in the mutually agreed-upon Change Request.

<u>1.200 Roles and Responsibilities</u>

1.201 CONTRACTOR STAFF, ROLES, AND RESPONSIBILITIES

The project team will consist of a primary project manager from both Contractor and the State of Michigan who will have joint responsibility for meeting deadlines and keeping the project on track within their respective organizations. The project team will also consist of additional personnel who will be instrumental in the implementation and ongoing operation of the Contractor's solution.

The Contractor's Project Manager will be responsible for notifying the State of Michigan Project Manager of any proposed changes to the Project Plan.

Identify Contractor staff who will be involved, identify by name the individuals, and describe in detail their roles and responsibilities. Identify Key Personnel. If an overall organization chart has been developed, then provide a reference to that chart as well. Note any part-time personnel. Descriptions of roles should be functional and not just by title. Include an organization chart in Article 1, Attachment B.

First Data Government Solutions is a national leader in providing Comprehensive Payment and Authorization solutions for State government. We understand the business and legislative needs in the development and ongoing support of electronic payment solutions; this has allowed us to earn the respect of our state clients. The First Data Government Solutions' team demonstrates our commitment by offering our experienced staff to the State of Michigan

Key Staff Positions

After a thorough analysis of roles and responsibilities, the requirements of CPAS solution, and stated performance requirements, the First Data Government Solutions team formulated the proposed project organization. The team's organization structure provides for managing and supporting ongoing operational needs, and ensures that adherence to project schedules and performance criteria are achieved. Article 1, Attachment B, Key Personnel Organization Chart depicts the proposed organizational structure of the First Data Government Solutions team.

PayPoint® Customer Service Representative, Ronda Earnhart

Ms. Earnhart, is the primary contact for the State of Michigan, and has been supporting First Data payment solutions for over 13 years. Ms Earnhart currently supports the MI CPAS solution, therefore she has a lot of subject matter expertise as it pertains to the CPAS solution.. Ms Earnhart's primary responsibilities are: Client Interaction: Respond to calls or messages from the State of Michigan when they are having problems or require assistance with PayPoint. She is responsible for communicating with the State of Michigan. Following the PayPoint Help Desk MI CEPAS Escalation Process, as shown in Attachment D it is Ms. Earnhart's primary responsibility to resolve problems, implement changes and maintain an effective client relationship.

- Troubleshooting: Interacts with the State of Michigan when there are systems, processor, or processing issue. She either assists client in troubleshooting the problem immediately or begins the process of researching the issue. This involves gathering data, communication directly with the processor or support entity, testing, and other methods of problem identification. Ms. Earnhart is responsible for total resolution of the issue meeting or exceeding the client's expectation.

- Application development/Boarding: Works closely with Project Managers or directly with merchant to board new application. Works directly with Processors and/or the Relationship/Account Managers to insure a complete processing methodology is functioning as expected in a timely manner.
- Provide 24/7 support via a paging process and respond in a timely manner to all emergency pages during off hours and weekends.

PayPoint® Customer Service Manager, Paul Hogland

Mr. Hogland, has been with First Data for 8 years, his primary role is to manage the support team dedicated to the ongoing operational needs for our PayPoint platform. He also serves as the technical lead for the State of Michigan and acts as the liaison between internal and external resources to mitigate, resolve and communicate technical issues. Mr Hogland acts as the key escalation contact for issues that have not been resolved per the PayPoint Help Desk MI CEPAS Escalation Process. He also plans and develops teams to address failing policies and procedures and effectively communicate the information to upper management. Mr. Hoglund oversees negotiations and administration of vendor contracts, consultant contracts and service agreements. He works closely with other departments to resolve issues outside the normal areas of responsibility. He also coordinates long-range operational goals.

Relationship Manager, Jason Clark

Mr. Clark is a Relationship Manager in the Government and Education business unit of First Data. He has been in First Data's for 11 years, focused solely on government implementations and ongoing support of those systems. As the Relationship Manager, Mr. Clark acts as the strategic advisor and ombudsman on the behalf of the client to ensure that the client's needs are met in accordance with our clients' expectations and First Data's standards.

Account Management, Gerhard Milkuhn

Mr. Milkuhn, has been involved in directly and in-directly in the management and oversight of the State of Michigan relationship for the last several years. He has more than 23 years of experience in Technical Client Services. Mr Milkuhn, directs efforts to ensure customer satisfaction on client accounts. He provides leadership and mentoring to several departments and strives to increase quality and reduce operating cost.

Implementation Manager, Brandon Keith

As the incumbent for the State of Michigan CPAS solution, there will not be an immediate need for an implementation manager. However, should the State of Michigan choose to implement a change to their CPAS solution, Mr Keith will be assigned to manage the implementation project to ensure all business needs and requirements are achieved. Mr. Keith has been with First Data Government solutions for 10 years, entirely dedicated to the project/implementation management role, delivering solutions to State/Local government. As the Implementation Manager for change orders for the State of Michigan, he will have the following responsibilities:

- Construct and maintain a working project plan, the meets the State of Michigan's CPAS objectives - the Project Manager will, relying on past experience, design the project plan.
- Plan and coordinate project meetings
- Provide required status reports
- Facilitate the collection of requirements for the implementation and ongoing performance objectives of the CPAS solutions. Provide quality assurance oversight concerning tasks and deliverables
- Coordinate the staffing and roles for the implementation plan
- Structure the project teams and insure each team understands the objectives to be accomplished during this phase
- Monitor and maintain the project plan to ensure target completion dates
- Ensure communication internally and externally

Our team is designed to meet the evolving needs of the State of Michigan. We incorporate strong functional, technical, operational and administrative team members with support provided by corporate executive management when required. We have found this approach to be mutually beneficial and cost effective for our clients. Our team possesses a strong base of technical and functional skills and is experienced and knowledgeable in the State of Michigan's business needs and requirements. Their detailed qualifications are included in the resumes, in Attachment B.

Contractor must provide a list of all subcontractors, including firm name, address, contact person, and a complete description of the work to be contracted. Include descriptive information concerning subcontractor's organization and abilities.

First Data Government Solutions does not use contractors in the development, operations, or support of the PayPoint System.

Single Point Person: After implementation the Contractor must provide a single point person to work with Treasury Receipts Processing staff to assist with agency related problems. Examples would include report problems, general questions, assistance with new agency account applications, reconciliation concerns, and training. The single point of contact will require a back up with similar skills and experience The Contractor must also provide a single point person to work with the State's information technology staff to answer technical questions and provide technical assistance. Questions or concerns must be resolved within one business day (See Section 1.104, E3.). A support desk concept staffed with knowledgeable and experienced staff will also be considered if it can be shown to be more efficient and reliable than a single point of contact.

Lead PayPoint support representative Ronda Earnhart is the single point person assigned to working with the Treasuary Receipts Processing staff to assist with agency related problems.

Paul Hoguland will serve as her backup and is the PayPoint support manager.

First Data Government Solutions uses a support desk concept staffed with knowledgeable and experienced staff to support technical issues. Paul Hoglund normally leads these efforts and has the experienced staff and external resources referenced in Appendix O as escalation points as needed.

1.202 STATE STAFF, ROLES, AND RESPONSIBILITIES

Jointly, the Department of Technology, Management & Budget (DTMB) and the Department of Treasury will oversee the statewide Contract.

Jeanne Irwin is the Department of Technology, Management & Budget Project Manager, assigned to Treasury; her role is to oversee the Contract performance during the term of the Contract and to support/assist the Department of Treasury and provide guidance to the CEPAS Technical Support Contact who supports agency applications technical needs.

Thomas Sharpe, is the Administrator for the Department of Treasury, Receipts Processing Division; Tom will work jointly with Jeanne Irwin to oversee the Contract business performance during the term of the Contract. Receipts Processing Division is the Business Owner of CEPAS.

Susan Stephens is the CEPAS Technical Support Contact. Susan's roles include supporting the Department of Treasury and agency applications with interface questions, telecommunication issues and other technical needs.

Brenda Vincent is the Assistant Administrator of the Receipts Processing Division. Her role is to provide guidance to the Banking and Disbursements Section Manager and assist the Administrator.

Martin Ruiz is the Manager of the Receipts Processing Division, Banking and Disbursements Section. His role is to oversee the statewide contract and provide guidance to the CEPAS Program Manager, ACH Program Manager, Agency Electronic Payment Coordinators and assist the Assistant Administrator.

Amy Kelso is the CEPAS Program Manager. Amy is the dedicated contact for credit card issues with the CEPAS Contractor. Amy's roles include overseeing the Contract performance on a day-to-day basis during the term of the Contract and keeping the project on track. She also is responsible for working with the Contractor to resolve business related issues, working with the Contractor and agencies to set up new merchant accounts, testing applications, training agency staff, analyzing volume and costs, assisting agency staff in resolving problems, and any card related issues.

Dave Hendrix is the CEPAS ACH Program Manager. Dave is the dedicated contact for ACH issues with the CEPAS contractor. Dave's roles include overseeing the Contract performance on a day-to-day basis, addressing any ACH performance issues, working with the Contractor to resolve ACH business related issues, working with the contractor and agencies to set up new ACH accounts, training agency staff, analyzing volume and costs, assisting agency staff in resolving problems, and any ACH related issues.

Kate Lundquist and Nancy Morse are Agency Electronic Payment Coordinators. Each is assigned to a certain group of state agencies. Their roles include setting up new merchant accounts, working with the Contractor to resolve business related issues involving their respective agencies, creating and maintaining accounting profiles, assisting with testing applications, and assisting agency staff in resolving reconcilement problems.

See **Appendix G - DTMB Organization Chart,** and **Appendix H - Treasury Receipts Processing Organization Chart.**

1.203 OTHER ROLES AND RESPONSIBILITIES

The State has a statewide contract with Fifth Third Processing Solutions for processing credit and debit cards. Fifth Third Processing Solutions is the State's acquirer.

All credit/debit card transactions processed through this contract will be processed through TSYS Processing Services.

1.300 Project Plan

1.301 PROJECT PLAN MANAGEMENT

1. **Contract Conversion:** The Contractor will carry out this project under the direction and control of the Michigan Departments of Technology, Management & Budget and Treasury. Once approved by Treasury, the Contractor will work with each department to implement this Contract. The Contractor cannot work directly with a department without Project Manager or designee (Treasury) authorization (See Sections 1.202 and 2.401).

2. **Project Manager:** There will be continuous liaison with the State Project Manager or designee during implementation. The Contractor's Project Manager will meet with the State Project Manager or designee on a biweekly basis, at a minimum, during implementation for the purpose of reviewing progress and providing necessary guidance in solving problems that arise. (See Section 2.401). The Treasury business owner will be included in these updates.

3. **Progress Reports:** During implementation the Contractor will submit brief written biweekly summaries of progress to the Project Manager or designee. The summary will outline the work accomplished during the reporting period; work to be accomplished during the subsequent reporting period; problems, real or anticipated, which should be brought to the attention of the Project Manager; and notification of any significant deviation from previously agreed-upon work plans with a corrective action plan established.

   Additionally, within 30 days after the Effective Date of the Contract resulting from this Statement of Work, the parties shall determine an appropriate set of meetings to be held between representatives of the State and Contractor. The State will review and approve the format of the contractor's progress report. The Contractor shall prepare and circulate an agenda prior to the meeting(s).

4. **Quarterly Meetings:** Subsequent to implementation, the Contractor Team and the Project Manager or designee will meet quarterly, at a minimum. After implementation, the biweekly summary reports will be replaced by Incident Reports as needed. The State will review and approve the format of the contractor's biweekly summary report. Incident Reports will be utilized to document serious system problems and issues and action taken to resolve them. See **Appendix F** for an example of the Incident Report document.

(Also see Section 1.104, E9.). Statistical reports will also be required on an ongoing basis and will be used as management reporting tools.

5. **Project Plan:** The Contractor's proposal will include a proposed Project Plan identified as "Article 1, Attachment C, Project Plan". The Project Plan must include the following:

   a.) The Contractor's project organizational structure.
   b.) The Contractor's staffing table with names and title of personnel assigned to the project. Necessary substitutions due to change of employment status and other unforeseen circumstances may only be made with prior approval of the State.
   c.) The project breakdown showing sub-projects, activities and tasks, and resources required and allocated to each. The project plan must reflect the task lists identified in each appropriate section of this Statement of Work.
   d.) The time-phased plan in the form of a graphic display using Microsoft Project, showing each event, task, milestone, and decision point in your work plan including a time line for migration of agency applications to the Contractor's system.
   e.) The project Plan shall contain an ongoing section of tasks to be completed on an on-going basis, such as SAS 70 reports, statistical reporting, PCI DSS compliance, Disaster Recovery site rollovers, etc.
   f.) Any changes to scope or schedule or budget must follow a Change Management process (Section 1.403), and it must be agreed upon and communicated to the State's Project Manager or designee in writing explaining the reason for the change and the impact.

   As the incumbent, the implementation for the PayPoint custom applications are complete and in production. Upon award, First Data Government Solutions will create a project plan that is mutually agreeable for both parties for the task items that fall outside of a normal implementation.

   Enhancements, paid for by the State under this contract, will include a detailed project plan documenting all tasks necessary to ensure successful project completion. The FDGS Project Manager will work with the State's Project Manager to create a mutually-agreeable project plan for each enhancement. We will follow the directives described above to meet this requirement.

1.302 REPORTS

The State will mutually agree with the contractor on the format of the following reports. The contractor is required to produce actual report formats for the State's review during the requirements validation process.

1. **Ad Hoc Reporting:** The Contractor's system must provide ad-hoc reporting. The reporting system must provide the ability to add or remove fields as needed.

   Through the PayPoint administration Web site the State has the ability to export search results into a CSV file or to generate a report from the PayPoint reporting module. If it is the State's desire to have additional reports created that cannot be created using the PayPoint standard reports or ad-hoc reports, upon award, FDGS will work with the State to determine the requirements for a custom report, and the effort will be scoped accordingly.

2. **Display Fields:** The Reporting must provide the ability to display the following fields:
   a.) Truncated account number (credit/debit/checking or savings).
   b.) Routing Number
   c.) Expiration Date
   d.) Dollar Amount
   e.) Transaction Date and Time
   f.) Convenience fee
   g.) Tax Amount
   h.) Customer Name, address, phone, or email address.
   i.) Contents of comments field
   j.) Approval Code

k.) Confirmation Number
l.) Agency Name
m.) Application Name
n.) Association
o.) Settlement Date
p.) Settlement Batch Amount
q.) Card Type
r.) Payment Status
s.) Column Sub-Totals and Totals for number of transactions and dollar amounts
t.) Other fields as needed

First Data Government Solutions' reporting provides the ability to display all of the State's requested fields. The PayPoint solution offers standard reports and the ability to run ad-hoc (temporary) reports that allow the State to display the fields desired to meet this requirement.

PayPoint contains eight (8) standard reports. If desired, the State may also run a search of the processed transactions from the PayPoint search screen that can be exported to a CSV file and saved locally. The following standard reports are available in PayPoint:

- Transaction Summary
- Transaction Detail
- Payment Type Summary
- Audit Summary
- User Listing
- Security Summary
- Payment Response Time Summary
- E-Check Returns

Transaction Summary - Provides a high-level summary of transactions that took place on a daily basis, grouped by batch number. The batch number is a unique number assigned to payments when they are issued for settlement.

Transaction Detail - Provides payment activity details including; Application, Batch, Transition ID, Customer Name, Account, Input Type, Account Type, Status, Confirmation Number, and Amount. This report also allows you to review recurring transactions.

Payment Type Summary - Breaks down payment type by payment medium, which includes either credit card or e-Check. Within each category, information is detailed by credit card or check type. For example, credit card displays card type, Master Card, Visa, Diners, etc.

Audit Summary - Provides a high-level summary of the transactions that took place on a daily basis, and may be grouped by batch number.

User Listing - This report provides a list of the users and roles within PayPoint, including when they last logged-in to PayPoint.

Security Summary - Provides changes made to PayPoint's security levels. Any changes to the User information is captured and reported here. This report is used for security reviews of the users' access levels.

Payment Response Time Summary - Provides the average time from request to response for the Make Payment and Cancel Payment APIs.

E-Check Returns - Provides summary and detailed information about eCheck Returns

3. **<u>Report Options</u>:** Reporting system must provide the options to report by:
a.) Specified Date Range
b.) Card Type
c.) Summarized Totals
d.) Transaction Details
e.) Settlement Batch (must match batch amount sent to TSYS)
f.) Agency, Agency Application, Association and statewide
g.) Payment Channels

h.) Payment Type

PayPoint Payment Search Criteria includes the following options and combinations:

- Date Range by Payment Save or Post Dates
- Payment Type
- Status
- Confirmation Number
- Account (Last 4 Digits)
- Transaction ID
- Authorization Code
- Payment ID
- Amount
- User ID
- Name
- Reference
- ACH Return Codes (Available with TeleCheck NFTF Only)

Settlement Search Criteria includes the following options and combinations:

- Date Range by Settlement Date(s)
- Settlement ID
- Payment Type
- Status
- Application

For both the Payment and Settlement Searches, detailed payment results can be exported into a .csv file. These can be sorted and managed using Microsoft Excel tools.

The following fields are exported:

- TransactionID
- PaymentID
- AppID
- Transaction Result
- Payment Result
- Payment Timestamp
- Payment Amount
- Reference
- RecurringID
- RegistrationID
- Processor
- Paymt Attempt Amount
- Paymt Processed Amount
- Uses Conv. Fee
- ACH Return Code (Draft or ACH Item-Available using TeleCheck NFTF Only)
- Full Name
- First Name
- Last Name
- Account Number
- Payment Medium
- Account Type Code
- CardType
- Confirmation #
- Payment Type
- Payment Command
- Payment Channel
- Payment Status
- Settlement BatchID
- User ID
- ACH Payment Type (Draft or ACH Item-Available using TeleCheck NFTF Only)

4. **Report Sorting**: System must allow user to sort the report by any specified field in ascending or descending order.

Using the standard reports available in PayPoint, the State has the ability to save reports in the following formats: PDF, CSV, XML, Excel, and HTML. Saving the report file as an Excel file will allow the State to sort any field in ascending or descending order.

5. **Report Templates:** System must provide the ability to create templates for reports that can be run without re-entry of data/field requirements. Templates created must be available for statewide usage. Reports must also be available by agency or association level.

The PayPoint reporting tools allow the State to save reports that are used often so that the report can be used in the future without recreating the criteria within the report.

6. **CEPAS Incident Reports:** The Contractor is required to provide written responses to CEPAS Incident Reports and maintain an Incident Report Summary document. See section 1.104, E9. and Appendix F. Written responses to incident reports are due within 10 business days of the receiving the incident.

   First Data Government Solutions meets this requirement. We will provide the incident reports to the State within ten (10) business days of receiving the incident.

7. **Security Performance Reports:** The Contractor will provide Security Performance Reports monthly to designated State areas (i.e. Treasury Office of Security and Receipts Processing). See Section 1.104.

   PayPoint supports Security Reports. The Security Summary report is available to the State as a standard report. The Security Summary provides changes made to PayPoint's security levels. Any changes to the User information is captured and reported here. This report is used for security reviews of the users' access levels. Upon award, First Data Government Solutions would like to work with the State for more detailed requirements.

8. **SAS 70 and PCI Reports:** The Contractor will supply the Project Manager or designee annual SAS 70 audits and will email quarterly confirmation that Contractor has run PCI scans and will follow First Data and PCI standard procedures for addressing any findings identified by the scans. See Section 1.104.

   First Data Government Solutions understands the requirement and, as the incumbent, provides the State with annual SAS 70 audits and quarterly PCI reports today.

9. **Project Implementation Reports:** During implementation the Contractor will submit brief written biweekly summaries of progress to the Project Manager or designee.

   The State is currently using the PayPoint system provided by First Data Government Solutions; therefore, there is no conversion effort associated with this proposal. We continue to support the implementation plans defined and managed by Treasury. By choosing First Data, the State relieves itself of the risks associated with a conversion effort to a new product and saves time and money associated with designing, constructing, testing, training, and implementing a new system.

10. **Management Reports:** Management Reports are to be provided electronically to the designated Treasury staff by the 10th calendar day of the next month. The Contractor must provide monthly Management Reports including:

    a. A statistical report that lists all applications in production, grouped by State agency, the volume of transaction settled per application, the dollar amount settled per application, including a statewide total for all agency applications. The report should also list the fiscal year total for each application for both transaction volume and dollars settled.
    b. A report that lists all scheduled and unscheduled downtime for the month. The report must include for each occurrence, the date and beginning and ending time the downtime occurred, the total time down, a summarized reason for the downtime, a description of the State applications that were affected by the downtime. The report must include totals for the amount of unscheduled and scheduled downtime for the month.
    c. A report that lists the average response time for each agency application for any timeframe selected by the report user. See Service Level Agreement in Article 1, Appendix N, System Response Time.
    d. An Incident Report Summary report that lists each Incident Report, description of the incident, status (open or closed), and action taken to resolve.

    As the incumbent, First Data Government Solutions currently provides the State with the management reports described above.

11. **Risk Assessment Review:** The Contractor will supply a copy of its annual Risk Assessment Review to the Project Manager or designee. See Section 1.402.

First Data Government Solutions will meet this requirement by performing the methodology described in Section 1.402.

12. **Monthly Invoice:** The Contractor will provide a monthly invoice no later than 10 calendar days of the next month. See Section 1.601, 1. F.

With the most recent PayPoint release, we will meet this requirement by providing the State detailed monthly invoices no later than 10 calendar days after the previous month's end.

13. **Security Reports:** The Contractor will provide access to Security Reports. The reports will be in an electronic format. The reports will identify user access information and user activity within the system.

PayPoint supports Security Reports. The Security Summary report is available to the State as a standard report. The Security Summary provides a report of changes made to PayPoint's security levels. Any changes to User information is captured and reported here. This report is used for security reviews of the users' access levels. Upon award, First Data Government Solutions would like to work with the State for more detailed requirements.

1.400 Project Management

1.401 ISSUE MANAGEMENT

Issues are those things that endanger the project. It includes imminent threats and events that may have already occurred. Issues will be documented by the Project Manager or designee on Incident Reports. Incident Reports will report system problems and issues that affect State customers or State agency reconciliation processes, dates the incident occurred and was discovered, action taken to resolve them, and post incident recommendations.

If the Contractor fails to take action, or the action taken was ineffective in resolving the issue, the Project Manager or designee will schedule a meeting with the Contractor's executive management to discuss the issue and establish a strategy and timeline for resolution.

If the strategy fails and/or timelines are unreasonably delayed, the Project Manager or designee may contact the Department of Technology, Management and Budget, Purchasing Operations to request issuance of a *Complaint to Contractor* to inform the Contractor of the State's dissatisfaction with resolution of the issue.

As the incumbent, the State will have reduced risk of exposure since the PayPoint application has been running in production for several years. When production issues occur, First Data Government Solutions performs the issue management activities, described above, for the State. We will continue to perform those activities to meet the State's requirements.

1.402 RISK MANAGEMENT

Risk management generally involves (1) identification of the risk; (2) assigning a level of priority based on the probability of occurrence and impact to the project, (3) definition of mitigation strategies, and (4) monitoring of risk and mitigation strategy. Risk assessment review shall be conducted at the beginning of the project, as needed when new risk is identified, and at least on an annual basis. These reports will be provided to the Project Manager or designee.

Comprehensive Risk Management

Risk is the possibility of the occurrence of any event that can negatively affect the success of a project. All large, complex technology integration projects are subject to risks because there is an inherent combination of uncertainty and constraints. Not all project risks can be completely eliminated; however, project risks can and must be managed and/or mitigated. To go beyond this initial identification of risks, however, the IVRS Project must view risk management as a facet of quality, using basic techniques of analysis and measurement to ensure that risks are properly identified, classified, and managed.

The First Data Government Solutions approach to risk management includes these key components.

Identify. Before risks can be managed, they must be identified. Identification discovers risks before they become problems that may adversely affect a project. First Data Government Solutions has developed techniques for surfacing risks through the application of a disciplined and systematic process that encourages project personnel to raise concerns and issues for subsequent analysis.

Analyze. Analysis is the conversion of risk data into risk decision-making information. Analysis provides the basis for the Project Manager to work on the "right" risks.

Plan. Planning turns risk information into decisions and actions (both present and future). Planning involves developing actions to address individual risks, prioritizing risk actions, establishing an owner to address each risk, and creating an integrated risk management plan. The plan for a specific risk could take many forms. For example:

- Mitigate the impact of the risk by developing a contingency plan (along with an identified triggering event) should the risk occur.
- Avoid a risk by changing the design or the development process.
- Accept the risk and take no further action, thus accepting the consequences if the risk occurs.
- Study the risk further to acquire more information and better determine the characteristics of the risk to enable decision-making.

Track. Tracking consists of monitoring the status of risks and taking action to mitigate them. Appropriate risk metrics are identified and monitored to enable the evaluation of the status of risks, themselves, and of risk mitigation plans. Tracking serves as the monitoring function of management.

Control. Risk control or abatement corrects for deviations from planned risk actions. Once risk metrics and triggering events have been chosen, there is nothing unique about risk control. Rather, risk control melds into project management and relies on project management processes to control risk action plans, correct for variations from plans, respond to triggering events, and improve risk management processes.

Communicate. Risk communication lies at the center of the model to emphasize both its pervasiveness and its criticality. Without effective communication, the risk management approach cannot be viable. While communication facilitates interaction among the elements of the model, there are higher-level communications to consider as well. To be analyzed and managed correctly, risks must be communicated to and between the appropriate organizational levels and entities. Because communication is pervasive, our approach is to address it as integral to every risk management activity and not as something performed outside of, and as a supplement to, other activities.

Risk Quantification. Quantification involves the analysis of risks and their interactions to determine which risks warrant the highest level of attention.

Objectives	Techniques	Tools
Comprehensive Risk Management: Well defined process for assessing, anticipating, and mitigating project risk areas. The "lessons learned" and best practices developed by our staff over several years of successfully conducting similar projects, enables us to anticipate and incorporate procedures to avoid or minimize areas of risk.	• Identifying and anticipating all components of risk – managerial, political, technical, financial • Developing risk mitigation strategies from project outset • Conducting on-going risk assessments	• Standardized risk assessment templates • Standardized assessment categories • Best practices from prior projects • Continual dialogue with client partners

1.403 CHANGE MANAGEMENT

During the course of this project, the following provides a detailed process to follow if a change to this SOW is required:

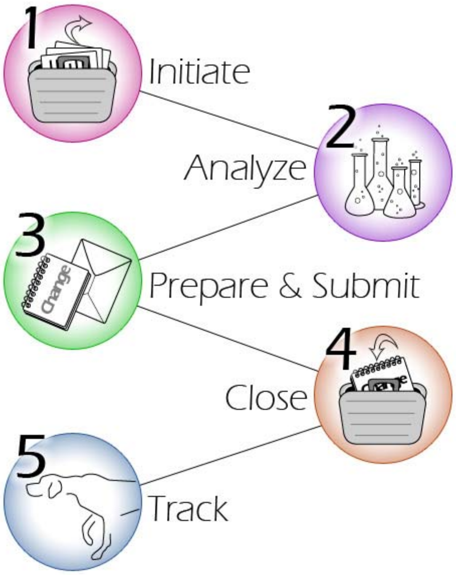
1. The designated Project Manager of the requesting party will review the proposed change and determine whether to submit the request to the other party.
2. The Contractor's Project Manager and the State will review the proposed change and approve it for further investigation or reject it. (The timing of signature by the State Project Manager will be in accordance with the State's Administrative Board or other applicable approval process). The investigation will determine the effect that the implementation of the Project Change Request (PCR) will have on price, schedule, and other terms and conditions of the Agreement.

A written Change Authorization and/or Change Control Request must be signed by both parties to authorize implementation of the investigated changes. Change Authorizations and/or Change Control Requests will be processed through the state's Purchasing Operations Office.

The Contractor will utilize an in-house change management system. Once a change request is identified, it will be thoroughly documented, and assigned a tracking number. Critical information such as involved parties (including approvers, initiators, implementers, and verifiers), relevant dates (open, resolved, implemented, abandoned, etc.), and potential risks are also captured.

If a proposed contract change is approved by the Project Manager, the Project Manager will submit a request for change to the Department of Technology, Management and Budget, Purchasing Operations Buyer, who will make recommendations to the Director of Purchasing Operations regarding ultimate approval/disapproval of change request. If the DTMB Purchasing Operations Director agrees with the proposed modification, and all required approvals are obtained (including State Administrative Board), the Purchasing Operations Buyer will issue an addendum to the Contract, via a Contract Change Notice. **Contractors who provide products or services prior to the issuance of a Contract Change Notice by the DTMB, Purchasing Operations, risk non-payment for the out-of-scope/pricing products and/or services.**

Change Request



Change Management Process Illustration
We have detailed our change management process to enhance the communication between the First Data Government Solutions project team and MI CEPAS Project Manager for all future change requests.

First Data Government Solutions understands and will meet the requirements set forth in this section.

When a change to the application is purposed by the State Project Manager, First Data Government Solutions will work with the State to capture all requirements needed for the purposed change. Once the requirements have been determined, First Data Government Solutions will submit a document ("Change Response or Statement of Work") with a unique identifier, detailing the steps involved needed to implement the change, along with the cost and detailed effort estimates of the requested change.

The State Project Manager or their designee will review the document and proceeds to close the request. In the closing process the State may accept the response, refer the response back to First Data Government Solutions if there are additional facts or approaches that could be considered, reject the response (say, if the cost exceeds the perceived benefit), or withdraw the request. First Data Government Solutions will not begin work on a change request until Contract Change Notice has been issued and executed.

First Data Government Solutions realizes that the State needs to ensure that costs are being controlled for the implementation of change orders. Therefore, First Data Government Solutions proposes to provide with each change order a detailed cost sheet showing the tasks to be completed for the change request, and specifying the amount of effort for each resource required to implement the change.

1.500 Acceptance

1.501 CRITERIA

The following criteria will be used by the State to determine Acceptance of the Services and/or Deliverables provided under this SOW.

The Contractor's system does not experience unscheduled downtime exceeding the 99.9% system availability requirement during the initial 60 day period following implementation.

The State does not lose interest earnings due to delayed ACH settlement during the initial 60 day period following implementation of an ACH application to be determined at time of conversion.

The State receives the lowest applicable interchange rate for credit card authorizations during the initial 60 day processing period.

The State experiences acceptable response times as defined in Section 1.104, D4. during the initial 60 day period following implementation of the Department of State, Renewal by Web application.

If the criteria above are not met, the Contractor will implement a corrective action plan with actions and timelines for the State's review and approval. Once the State Project Manager or designee and Contractor agree that the situation has been resolved, another 60 day period will begin with the expectation that the criteria will be met.

1.502 FINAL ACCEPTANCE

Final Acceptance is when criteria defined in Section 1.501 are met and all requirements of the Contract are met. A requirement validation process will be completed and signed by both the Contractor and State Project Manager or designee.

1.600 Compensation and Payment

1.601 COMPENSATION AND PAYMENT

1. Price Proposal

A.) **Firm Pricing:** All prices will be firm for the duration of the Contract. If the Contract is extended beyond five (5) years, the State and the Contractor may negotiate price increases or decreases. If mutually acceptable rates are not negotiated, the Contract will not be extended.

B.) **Unit Price Contract:** This is a unit price Contract. For unit prices, the State will only pay for actual transactions processed and any fees associated with the Customizable Web & IVR Solution. The Contractor is responsible for all additional costs, overhead, travel, out-of-pocket costs, etc.

For billing purposes, a "transaction" is defined as:

- a settled transaction
- a voided/cancelled transaction
- a refund
- a declined transaction

The following are examples of events not considered billable transactions:

- an authorization
- an NOC
- an ACH return
- communication failures
- errors
- chargebacks
- duplicate transactions attributable to the Contractor
- refunds of duplicate transactions attributable to the Contractor

C.) **Pricing – Appendix A**

Transaction Fee Pricing: The transaction fees include **all** costs for providing the system defined in the Statement of Work including any costs for ODFI services. The State expects volume discounts in the transaction fee pricing based on a monthly review of the transaction volume processed.

Implementation Period Pricing: Transaction fees charged during the 12 month implementation/migration period by the new Contractor will be based on the unit fee for the monthly volume of transactions processed through both the existing CEPAS Contractor and the new Contractor combined. For example, if 100,000 transactions were processed through the new Contractor and 250,000 transactions were processed through the existing Contractor then the unit fee for the price range that includes 350,000 transactions will be the unit price charged. Any fees associated with the Customizable Web and IVR solution will be charged based on the volume of activity processed and pricing in Table 4.

Bank of Hours: This bank of 1000 hours is to be used for customized enhancements that the State may request.

Guaranteed ACH Pricing: Some State agencies may choose to have ACH debit transactions guaranteed by the Contractor. By guaranteeing the transaction the Contractor is assuming the risk of the transaction being returned.

Customizable Web & IVR Solution: The Contractor charges the unit cost for payments made using the Contractor's Customizable Web & IVR Solution and for utilizing different optional components of the Contractors system. All payments will be subject to a per item transaction fee for using the solution plus additional per item fees for utilizing any of the additional functions (Authentication, Registration, IVR). This pricing method is being used to allow the cost of this functionality to be absorbed only by those agencies that require this type of service/functionality.

Monthly Invoice: The Contractor will supply an invoice electronically (i.e. Excel spreadsheet by email) that has one page for each State Department except Courts that lists the period covered, number of transactions processed for each application within that Department, the unit price, and total cost for the application and a separate detailed breakdown of any Customizable Web & IVR Solution fees. At the discretion of the State, some groupings of applications will be reported at the association (merchant chain) level. The page must also contain a total item count and dollar amount for the Department (total of all applications). The invoice must also contain a summary total page that lists an item count and dollar amount for the month for all State Departments except Courts (statewide total). A separate identically formatted invoice will be prepared for the Courts. The Contractor will provide the invoice for the month by no later than 10 calendar days of the following month. The invoice for the Courts will be sent to a designated contact at the Courts. Both invoices will be sent to the designated contacts in the Treasury, Receipts Processing Division.

1.602 HOLDBACK

RESERVED

Article 2, Terms and Conditions

2.000 Contract Structure and Term

2.001 CONTRACT TERM

This Contract is for a period of five (5) years beginning July 1, 2011 through June 30, 2016. All outstanding Purchase Orders must also expire upon the termination (cancellation for any of the reasons listed in **Section 2.150**) of the Contract, unless otherwise extended under the Contract. Absent an early termination for any reason, Purchase Orders issued but not expired, by the end of the Contract's stated term, will remain in effect for the balance of the fiscal year for which they were issued.

2.002 OPTIONS TO RENEW

This Contract may be renewed in writing by mutual agreement of the parties not less than 30 days before its expiration. The Contract may be renewed for up to five (5) additional one (1) year periods.

2.003 LEGAL EFFECT

Contractor shall show acceptance of this Contract by signing two copies of the Contract and returning them to the Contract Administrator. The Contractor shall not proceed with the performance of the work to be done under the Contract, including the purchase of necessary materials, until both parties have signed the Contract to show acceptance of its terms, and the Contractor receives a contract release/purchase order that authorizes and defines specific performance requirements.

Except as otherwise agreed in writing by the parties, the State assumes no liability for costs incurred by Contractor or payment under this Contract, until Contractor is notified in writing that this Contract (or Change Order) has been approved by the State Administrative Board (if required), approved and signed by all the parties, and a Purchase Order against the Contract has been issued.

2.004 ATTACHMENTS & EXHIBITS

All Attachments and Exhibits affixed to any and all Statement(s) of Work, or appended to or referencing this Contract, are incorporated in their entirety and form part of this Contract.

2.005 ORDERING

The State will issue a written Purchase Order, Blanket Purchase Order, Direct Voucher or Procurement Card Order, which must be approved by the Contract Administrator or the Contract Administrator's designee, to order any Services/Deliverables under this Contract. All orders are subject to the terms and conditions of this Contract. No additional terms and conditions contained on either a Purchase Order or Blanket Purchase Order apply unless they are also specifically contained in that Purchase Order or Blanket Purchase Order's accompanying Statement of Work. Exact quantities to be purchased are unknown, however, the Contractor will be required to furnish all such materials and services as may be ordered during the CONTRACT period. Quantities specified, if any, are estimates based on prior purchases, and the State is not obligated to purchase in these or any other quantities.

2.006 ORDER OF PRECEDENCE

The Contract, including any Statements of Work and Exhibits, to the extent not contrary to the Contract, each of which is incorporated for all purposes, constitutes the entire agreement between the parties with respect to the subject matter and supersedes all prior agreements, whether written or oral, with respect to the subject matter and as additional terms and conditions on the purchase order must apply as limited by **Section 2.005.**

In the event of any inconsistency between the terms of the Contract and a Statement of Work, the terms of the Statement of Work will take precedence (as to that Statement of Work only); provided, however, that a Statement of Work may not modify or amend the terms of the Contract, which may be modified or amended only by a formal Contract amendment.

2.007 HEADINGS

Captions and headings used in the Contract are for information and organization purposes. Captions and headings, including inaccurate references, do not, in any way, define or limit the requirements or terms and conditions of the Contract.

2.008 FORM, FUNCTION & UTILITY

If the Contract is for use of more than one State agency and if the Deliverable/Service does not the meet the form, function, and utility required by that State agency, that agency may, subject to State purchasing policies, procure the Deliverable/Service from another source.

2.009 REFORMATION AND SEVERABILITY

Each provision of the Contract is severable from all other provisions of the Contract and, if one or more of the provisions of the Contract is declared invalid, the remaining provisions of the Contract remain in full force and effect.

2.010 Consents and Approvals

Except as expressly provided otherwise in the Contract, if either party requires the consent or approval of the other party for the taking of any action under the Contract, the consent or approval must be in writing and must not be unreasonably withheld or delayed.

2.011 NO WAIVER OF DEFAULT

If a party fails to insist upon strict adherence to any term of the Contract then the party has not waived the right to later insist upon strict adherence to that term, or any other term, of the Contract.

2.012 SURVIVAL

Any provisions of the Contract that impose continuing obligations on the parties, including without limitation the parties' respective warranty, indemnity and confidentiality obligations, survive the expiration or termination of the Contract for any reason. Specific references to survival in the Contract are solely for identification purposes and not meant to limit or prevent the survival of any other section

2.020 Contract Administration

2.021 ISSUING OFFICE

This Contract is issued by the Department of Technology, Management and Budget, Purchasing Operations, the Department of Treasury, and the Department of Information Technology (collectively, including all other relevant State of Michigan departments and agencies, the "State"). Purchasing Operations is the sole point of contact in the State with regard to all procurement and contractual matters relating to the Contract. The Purchasing Operations Contract Administrator for this Contract is:

Laura Gyorkos, Buyer Specialist
Purchasing Operations
Department of Technology, Management and Budget
Mason Bldg, 2nd Floor
PO Box 30026
Lansing, MI 48909
Email: gyorkosl@michigan.gov
Phone: 517-373-1455

2.022 CONTRACT COMPLIANCE INSPECTOR

The Director of Purchasing Operations directs the person named below, or his or her designee, to monitor and coordinate the activities for the Contract on a day-to-day basis during its term. **Monitoring Contract activities does not imply the authority to change, modify, clarify, amend, or otherwise alter the prices, terms, conditions and specifications of the Contract. Purchasing Operations is the only State office authorized to change, modify, amend, alter or clarify the prices, specifications, terms and conditions of this Contract.** The Contract Compliance Inspector for this Contract is:

Mark Lawrence
Department of Technology, Management and Budget
Mason Bldg, 2nd Floor
PO Box 30026
Lansing, MI 48909
Email: LawrenceM1@michigan.gov
Phone: (517) 335-5857

2.023 PROJECT MANAGER

The following individual will oversee the project:

Jeanne Irwin
Department of Technology, Management and Budget
7285 Parsons Dr
Dimondale, MI
Email: irwinj@michigan.gov
Phone: (517) 636-5001

2.024 CHANGE REQUESTS

The State reserves the right to request from time to time any changes to the requirements and specifications of the Contract and the work to be performed by the Contractor under the Contract. During the course of ordinary business, it may become necessary for the State to discontinue certain business practices or create Additional Services/Deliverables. At a minimum, to the extent applicable, the State would like the Contractor to provide a detailed outline of all work to be done, including tasks necessary to accomplish the Services/Deliverables, timeframes, listing of key personnel assigned, estimated hours for each individual per task, and a complete and detailed cost justification.

If the State requests or directs the Contractor to perform any Services/Deliverables that are outside the scope of the Contractor's responsibilities under the Contract ("New Work"), the Contractor must notify the State promptly, and before commencing performance of the requested activities, that it believes the requested activities are New Work. If the Contractor fails to notify the State before commencing performance of the requested activities, any such activities performed before the Contractor gives notice shall be conclusively considered to be in-scope Services/Deliverables, not New Work.

If the State requests or directs the Contractor to perform any services or provide deliverables that are consistent with and similar to the Services/Deliverables being provided by the Contractor under the Contract, but which the Contractor reasonably and in good faith believes are not included within the Statements of Work, then before performing such services or providing such deliverables, the Contractor shall notify the State in writing that it considers the services or deliverables to be an Additional Service/Deliverable for which the Contractor should receive additional compensation. If the Contractor does not so notify the State, the Contractor shall have no right to claim thereafter that it is entitled to additional compensation for performing that service or providing that deliverable. If the Contractor does so notify the State, then such a service or deliverable shall be governed by the Change Request procedure in this Section.

In the event prices or service levels are not acceptable to the State, the Additional Services or New Work shall be subject to competitive bidding based upon the specifications.

(1) Change Request at State Request
If the State should require Contractor to perform New Work, Additional Services or make changes to the Services that would affect the Contract completion schedule or the amount of compensation due Contractor (a "Change"), the State shall submit a written request for Contractor to furnish a proposal for carrying out the requested Change (a "Change Request").

(2) Contractor Recommendation for Change Requests:
Contractor shall be entitled to propose a Change to the State, on its own initiative, should it be of the opinion that this would benefit the Contract.

(3) Upon receipt of a Change Request or on its own initiative, Contractor shall examine the implications of the requested Change on the technical specifications, Contract schedule and price of the Deliverables and Services and shall submit to the State without undue delay a written proposal for carrying out the Change. Contractor's proposal will include any associated changes in the technical specifications, Contract schedule and price and method of pricing of the Services. If the Change is to be performed on a time and materials basis, the Amendment Labor Rates shall apply to the provision of such Services. If Contractor provides a written proposal and should Contractor be of the opinion that a requested Change is not to be recommended, it shall communicate its opinion to the State but shall nevertheless carry out the Change as specified in the written proposal if the State directs it to do so.

(4) By giving Contractor written notice within a reasonable time, the State must be entitled to accept a Contractor proposal for Change, to reject it, or to reach another agreement with Contractor. Should the parties agree on carrying out a Change, a written Contract Change Notice must be prepared and issued under this Contract, describing the Change and its effects on the Services and any affected components of this Contract (a "Contract Change Notice").

(5) No proposed Change must be performed until the proposed Change has been specified in a duly executed Contract Change Notice issued by the Department of Technology, Management and Budget, Purchasing Operations.

(6) If the State requests or directs the Contractor to perform any activities that Contractor believes constitute a Change, the Contractor must notify the State that it believes the requested activities are a Change before beginning to work on the requested activities. If the Contractor fails to notify the State before beginning to work on the requested activities, then the Contractor waives any right to assert any claim for additional compensation or time for performing the requested activities. If the Contractor commences performing work outside the scope of this Contract and then ceases performing that work, the Contractor must, at the request of the State, retract any out-of-scope work that would adversely affect the Contract.

2.025 NOTICES

Any notice given to a party under the Contract must be deemed effective, if addressed to the party as addressed below, upon: (i) delivery, if hand delivered; (ii) receipt of a confirmed transmission by facsimile if a copy of the notice is sent by another means specified in this Section; (iii) the third Business Day after being sent by U.S. mail, postage pre-paid, return receipt requested; or (iv) the next Business Day after being sent by a nationally recognized overnight express courier with a reliable tracking system.

State:
State of Michigan
Purchasing Operations
Attention: Laura Gyorkos
PO Box 30026
530 West Allegan
Lansing, Michigan 48909

Contractor:
Name: Jason Clark
Address: 11311 Cornell Park Drive, Suite 300
Cincinnati, OH 45242

Either party may change its address where notices are to be sent by giving notice according to this Section.

2.026 BINDING COMMITMENTS

Representatives of Contractor must have the authority to make binding commitments on Contractor's behalf within the bounds set forth in the Contract. Contractor may change the representatives from time to time upon written notice.

2.027 RELATIONSHIP OF THE PARTIES

The relationship between the State and Contractor is that of client and independent contractor. No agent, employee, or servant of Contractor or any of its Subcontractors must be or must be deemed to be an employee, agent or servant of the State for any reason. Contractor will be solely and entirely responsible for its acts and the acts of its agents, employees, servants and Subcontractors during the performance of the Contract.

2.028 COVENANT OF GOOD FAITH

Each party must act reasonably and in good faith. Unless stated otherwise in the Contract, the parties will not unreasonably delay, condition or withhold the giving of any consent, decision or approval that is either requested or reasonably required of them in order for the other party to perform its responsibilities under the Contract.

2.029 ASSIGNMENTS

(a) Neither party may assign this Contract, or assign or delegate any of its duties or obligations under the Contract, to another party (whether by operation of law or otherwise), without the prior approval of the other party. The State may, however, assign this Contract to any other State agency, department, or division without the prior approval of the Contractor.
(b) If the Contractor intends to assign this Contract or any of the Contractor's rights or duties under the Contract, the Contractor must notify the State and provide adequate information about the assignee at least 90 days before the proposed assignment or as otherwise provided by law or court order. The State may withhold approval from proposed assignments, subcontracts, or novations if the State determines, in its sole discretion, that the transfer of responsibility would decrease the State's likelihood of receiving performance on the Contract or the State's ability to recover damages.
(c) If the State permits an assignment of the Contractor's right to receive payments, the Contractor is not relieved of its responsibility to perform any of its contractual duties. All payments must continue to be made to one entity.

2.030 General Provisions

2.031 MEDIA RELEASES

News releases (including promotional literature and commercial advertisements) pertaining to the RFP and Contract or project to which it relates shall not be made without prior written State approval, and then only in accordance with the explicit written instructions from the State. No results of the activities associated with the RFP and Contract are to be released without prior written approval of the State and then only to persons designated.

2.032 CONTRACT DISTRIBUTION

Purchasing Operations retains the sole right of Contract distribution to all State agencies and local units of government unless other arrangements are authorized by Purchasing Operations.

2.033 PERMITS

Contractor must obtain and pay any associated costs for all required governmental permits, licenses and approvals for the delivery, installation and performance of the Services. The State must pay for all costs and expenses incurred in obtaining and maintaining any necessary easements or right of way.

2.034 WEBSITE INCORPORATION

The State is not bound by any content on the Contractor’s website, even if the Contractor’s documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the State has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by an authorized representative of the State.

2.035 FUTURE BIDDING PRECLUSION

Contractor acknowledges that, to the extent this Contract involves the creation, research, investigation or generation of a future RFP; it may be precluded from bidding on the subsequent RFP. The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Contractor, or as a Contractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP

2.036 FREEDOM OF INFORMATION

All information in any proposal submitted to the State by Contractor and this Contract is subject to the provisions of the Michigan Freedom of Information Act, 1976 Public Act No. 442, as amended, MCL 15.231, et seq (the “FOIA”).

2.037 DISASTER RECOVERY

Contractor and the State recognize that the State provides essential services in times of natural or man-made disasters. Therefore, except as so mandated by Federal disaster response requirements, Contractor personnel dedicated to providing Services/Deliverables under this Contract will provide the State with priority service for repair and work around in the event of a natural or man-made disaster.

<u>2.040 Financial Provisions</u>

2.041 FIXED PRICES FOR SERVICES/DELIVERABLES

Each Statement of Work or Purchase Order issued under this Contract shall specify (or indicate by reference to the appropriate Contract Exhibit) the firm, fixed prices for all Services/Deliverables, and the associated payment milestones and payment amounts. The State may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor must show verification of measurable progress at the time of requesting progress payments.

2.042 ADJUSTMENTS FOR REDUCTIONS IN SCOPE OF SERVICES/DELIVERABLES

If the scope of the Services/Deliverables under any Statement of Work issued under this Contract is subsequently reduced by the State, the parties shall negotiate an equitable reduction in Contractor’s charges under such Statement of Work commensurate with the reduction in scope.

2.043 SERVICES/DELIVERABLES COVERED

For all Services/Deliverables to be provided by Contractor (and its Subcontractors, if any) under this Contract, the State shall not be obligated to pay any amounts in addition to the charges specified in this Contract.

2.044 INVOICING AND PAYMENT – IN GENERAL

(a) Each Statement of Work issued under this Contract shall list (or indicate by reference to the appropriate Contract Exhibit) the prices for all Services/Deliverables, equipment and commodities to be provided, and the associated payment milestones and payment amounts.

(b) Each Contractor invoice will show details as to charges by Service/Deliverable component and location at a level of detail reasonably necessary to satisfy the State’s accounting and charge-back requirements. Invoices for Services performed on a time and materials basis will show, for each individual, the number of hours of Services performed during the billing period, the billable skill/labor category for such person and the applicable hourly billing rate. Prompt payment by the State is contingent on the Contractor’s invoices showing the amount owed by the State minus any holdback amount to be retained by the State in accordance with **Section 1.064**.

(c) Correct invoices will be due and payable by the State, in accordance with the State’s standard payment procedure as specified in 1984 Public Act No. 279, MCL 17.51 et seq., within 45 days after receipt, provided the State determines that the invoice was properly rendered.

(d1) All invoices should reflect actual work done. Specific details of invoices and payments will be agreed upon between the Contract Administrator and the Contractor after the proposed Contract Agreement has been signed and accepted by both the Contractor and the Director of Purchasing Operations, Department of Management & Budget. This activity will occur only upon the specific written direction from Purchasing Operations.

The specific payment schedule for any Contract(s) entered into, as the State and the Contractor(s) will mutually agree upon. The schedule should show payment amount and should reflect actual work done by the payment dates, less any penalty cost charges accrued by those dates. As a general policy statements shall be forwarded to the designated representative by the 10th day of the following month.

The Government may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor must show verification of measurable progress at the time of requesting progress payments.

2.045 PRO-RATION

To the extent there are any Services that are to be paid for on a monthly basis, the cost of such Services shall be pro-rated for any partial month.

2.046 ANTITRUST ASSIGNMENT

The Contractor assigns to the State any claim for overcharges resulting from antitrust violations to the extent that those violations concern materials or services supplied by third parties to the Contractor, toward fulfillment of this Contract.

2.047 FINAL PAYMENT

The making of final payment by the State to Contractor does not constitute a waiver by either party of any rights or other claims as to the other party’s continuing obligations under the Contract, nor will it constitute a waiver of any claims by one party against the other arising from unsettled claims or failure by a party to comply with this Contract, including claims for Services and Deliverables not reasonably known until after acceptance to be defective or substandard. Contractor’s acceptance of final payment by the State under this Contract shall constitute a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still unsettled.

2.048 ELECTRONIC PAYMENT REQUIREMENT

Electronic transfer of funds is required for payments on State Contracts. Contractors are required to register with the State electronically at http://www.cpexpress.state.mi.us. As stated in Public Act 431 of 1984, all contracts that the State enters into for the purchase of goods and services shall provide that payment will be made by electronic fund transfer (EFT).

2.050 Taxes

2.051 EMPLOYMENT TAXES

Contractors are expected to collect and pay all applicable federal, state, and local employment taxes, including the taxes.

2.052 SALES AND USE TAXES

Contractors are required to be registered and to remit sales and use taxes on taxable sales of tangible personal property or services delivered into the State. Contractors that lack sufficient presence in Michigan to be required to register and pay tax must do so as a volunteer. This requirement extends to: (1) all members of any controlled group as defined in § 1563(a) of the Internal Revenue Code and applicable regulations of which the company is a member, and (2) all organizations under common control as defined in § 414(c) of the Internal Revenue Code and applicable regulations of which the company is a member that make sales at retail for delivery into the State are registered with the State for the collection and remittance of sales and use taxes. In applying treasury regulations defining “two or more trades or businesses under common control” the term “organization” means sole proprietorship, a partnership (as defined in § 701(a) (2) of the Internal Revenue Code), a trust, an estate, a corporation, or a limited liability company.

2.060 Contract Management

2.061 CONTRACTOR PERSONNEL QUALIFICATIONS

All persons assigned by Contractor to the performance of Services under this Contract must be employees of Contractor or its majority-owned (directly or indirectly, at any tier) subsidiaries (or a State-approved Subcontractor) and must be fully qualified to perform the work assigned to them. Contractor must include a similar provision in any subcontract entered into with a Subcontractor. For the purposes of this Contract, independent contractors engaged by Contractor solely in a staff augmentation role must be treated by the State as if they were employees of Contractor for this Contract only; however, the State understands that the relationship between Contractor and Subcontractor is an independent contractor relationship.

2.062 CONTRACTOR KEY PERSONNEL

(a) The Contractor must provide the Contract Compliance Inspector with the names of the Key Personnel.

(b) Key Personnel must be dedicated as defined in the Statement of Work to the Project.

(c) The State will have the right to approve in writing the initial assignment of Key Personnel, as well as any proposed Key Personnel replacements. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, will introduce the individual to the appropriate State representatives, and will provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(d) When practicable and not prohibited by law, Contractor will notify the State at least 30 days prior to any changes in Key Personnel. Contractor will not be required to provide prior notice of changes in Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation or for cause termination of the Key Personnel's employment, but the Contractor will provide notice to the State as soon as practicable once it becomes aware of a change. The Contractor with the State must review any Key Personnel replacements, and appropriate transition planning will be established.

2.063 RE-ASSIGNMENT OF PERSONNEL AT THE STATE'S REQUEST

The State reserves the right to require the removal from the Project of Contractor personnel found by the State, in the exercise of reasonable judgment and after consultation with the Contractor, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request must be based on legitimate, good faith reasons. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed personnel, the State agrees to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any incident with removed personnel results in delay not reasonably anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Service will not be counted for a time as agreed to by the parties.

2.064 CONTRACTOR PERSONNEL LOCATION

All staff assigned by Contractor to work on the Contract will perform their duties either primarily at Contractor's offices and facilities or at State facilities. Without limiting the generality of the foregoing, Key Personnel will, at a minimum, spend at least the amount of time on-site at State facilities as indicated in the applicable Statement of Work. Subject to availability, selected Contractor personnel may be assigned office space to be shared with State personnel.

2.065 CONTRACTOR IDENTIFICATION

Contractor employees must be clearly identifiable while on State property by wearing a State-issued badge, as required. Contractor employees are required to clearly identify themselves and the company they work for whenever making contact with State personnel by telephone or other means.

2.066 COOPERATION WITH THIRD PARTIES

Contractor agrees to cause its personnel and the personnel of any Subcontractors to cooperate with the State and its agents and other contractors including the State's Quality Assurance personnel. As reasonably requested by the State in writing, the Contractor will provide to the State's agents and other contractors reasonable access to Contractor's Project personnel, systems and facilities to the extent the access relates to activities specifically associated with this Contract and will not interfere or jeopardize the safety or operation of the systems or facilities. The State acknowledges that Contractor's time schedule for the Contract is very specific and agrees not to unnecessarily or unreasonably interfere with, delay or otherwise impeded Contractor's performance under this Contract with the requests for access.

2.067 CONTRACT MANAGEMENT RESPONSIBILITIES

Contractor shall be responsible for all acts and omissions of its employees, as well as the acts and omissions of any other personnel furnished by Contractor to perform the Services. Contractor shall have overall responsibility for managing and successfully performing and completing the Services/Deliverables, subject to the overall direction and supervision of the State and with the participation and support of the State as specified in this Contract. Contractor's duties will include monitoring and reporting the State's performance of its participation and support responsibilities (as well as Contractor's own responsibilities) and providing timely notice to the State in Contractor's reasonable opinion if the State's failure to perform its responsibilities in accordance with the Project Plan is likely to delay the timely achievement of any Contract tasks.

The Contractor will provide the Services/Deliverables directly or through its affiliates, subsidiaries, subcontractors or resellers. Regardless of the entity providing the Service/Deliverable, the Contractor will act as a single point of contact coordinating these entities to meet the State's need for Services/Deliverables. Nothing in this Contract, however, shall be construed to authorize or require any party to violate any applicable law or regulation in its performance of this Contract.

2.068 CONTRACTOR RETURN OF STATE EQUIPMENT/RESOURCES

The Contractor must return to the State any State-furnished equipment, facilities and other resources when no longer required for the Contract in the same condition as when provided by the State, reasonable wear and tear excepted.

2.070 Subcontracting by Contractor

2.071 CONTRACTOR FULL RESPONSIBILITY

Contractor shall have full responsibility for the successful performance and completion of all of the Services and Deliverables. The State will consider Contractor to be the sole point of contact with regard to all contractual matters under this Contract, including payment of any and all charges for Services and Deliverables.

2.072 STATE CONSENT TO DELEGATION

Contractor shall not delegate any duties under this Contract to a Subcontractor unless the Department of Technology, Management and Budget, Purchasing Operations has given written consent to such delegation. The State shall have the right of prior written approval of all Subcontractors and to require Contractor to replace any Subcontractors found, in the reasonable judgment of the State, to be unacceptable. The State's request shall be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request shall be based on legitimate, good faith reasons. Replacement Subcontractor(s) for the removed Subcontractor shall be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed Subcontractor, the State will agree to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any such incident with a removed Subcontractor results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLA for the affected Work will not be counted for a time agreed upon by the parties.

2.073 SUBCONTRACTOR BOUND TO CONTRACT

In any subcontracts entered into by Contractor for the performance of the Services, Contractor shall require the Subcontractor, to the extent of the Services to be performed by the Subcontractor, to be bound to Contractor by the terms of this Contract and to assume toward Contractor all of the obligations and responsibilities that Contractor, by this Contract, assumes toward the State. The State reserves the right to receive copies of and review all subcontracts, although Contractor may delete or mask any proprietary information, including pricing, contained in such contracts before providing them to the State. The management of any Subcontractor will be the responsibility of Contractor, and Contractor shall remain responsible for the performance of its Subcontractors to the same extent as if Contractor had not subcontracted such performance. Contractor shall make all payments to Subcontractors or suppliers of Contractor. Except as otherwise agreed in writing by the State and Contractor, the State will not be obligated to direct payments for the Services other than to Contractor. The State's written approval of any Subcontractor engaged by Contractor to perform any obligation under this Contract shall not relieve Contractor of any obligations or performance required under this Contract. A list of the Subcontractors, if any, approved by the State as of the execution of this Contract, together with a copy of the applicable subcontract is attached.

2.074 FLOW DOWN

Except where specifically approved in writing by the State on a case-by-case basis, Contractor shall flow down the obligations in **Sections 2.031, 2.060, 2.100, 2.110, 2.120, 2.130, and 2.200** in all of its agreements with any Subcontractors.

2.075 COMPETITIVE SELECTION

The Contractor shall select subcontractors (including suppliers) on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the Contract.

2.076

For the purposes of this Section 2.070, the defined term "Subcontractor" shall exclude Telecheck; nevertheless, Contractor remains responsible for any obligations or performance required under this Contract.

2.080 State Responsibilities

2.081 EQUIPMENT

The State will provide only the equipment and resources identified in the Statements of Work and other Contract Exhibits.

2.082 FACILITIES

The State must designate space as long as it is available and as provided in the Statement of Work, to house the Contractor's personnel whom the parties agree will perform the Services/Deliverables at State facilities (collectively, the "State Facilities"). The Contractor must have reasonable access to, and unless agreed otherwise by the parties in writing must observe and comply with all rules and regulations relating to each of the State Facilities (including hours of operation) used by the Contractor in the course of providing the Services. Contractor agrees that it will not, without the prior written consent of the State, use any State Facilities or access any State information systems provided for the Contractor's use, or to which the Contractor otherwise gains access in the course of performing the Services, for any purpose other than providing the Services to the State.

2.090 Security

2.091 BACKGROUND CHECKS

Where not prohibited by law, Contractor agrees to reasonably assist the State, in its pursuit to obtain permission from any employee performing services under this Agreement, should the State request to perform a background check on such employee.

2.092 SECURITY BREACH NOTIFICATION

If the Contractor breaches this Section, the Contractor must (i) promptly cure any deficiencies and (ii) comply with any applicable federal and state laws and regulations pertaining to unauthorized disclosures. Contractor and the State will cooperate to mitigate, to the extent practicable, the effects of any breach, intrusion, or unauthorized use or disclosure. Contractor must report to the State in writing any use or disclosure of Confidential Information other than as provided for by the Contract within 10 days of becoming aware of the use or disclosure or the shorter time period as is reasonable under the circumstances.

2.093 PCI DATA SECURITY REQUIREMENTS

Contractors with access to credit/debit card cardholder data must adhere to the Payment Card Industry (PCI) Data Security requirements. Contractor agrees that they are responsible for security of cardholder data in their possession. Contractor agrees that data can ONLY be used for assisting the State in completing a transaction, supporting a loyalty program, supporting the State, providing fraud control services, or for other uses specifically required by law.

Contractor agrees to provide business continuity in the event of a major disruption, disaster or failure.

Unless otherwise prohibited by law, the Contractor will contact the Department of Technology, Management and Budget, Financial Services, CEPAS Program Manager or Receipts Processing Administrator to advise them of any breaches in security where the State’s card data has been compromised within 2 business days after the compromise has been confirmed by the Contractor’s Privacy Office. In the event of a security intrusion, the Contractor agrees to cooperate with Payment Card Association requirements.
Contractor agrees to dispose the State’s sensitive cardholder data in accordance with Contractor’s record retention policies and consistent with Payment Card Industry Requirements. The Contractor will continue to treat cardholder data as confidential upon contract termination.

The Contractor will provide the Department of Technology, Management and Budget, Financial Services and the CEPAS Program Manager documentation showing PCI Data Security certification has been achieved. The Contractor will advise the Department of Technology, Management and Budget, Financial Services and the CEPAS Program Manager of all failures to comply with the PCI Data Security Requirements. Failures include, but are not limited to system scans and self-assessment questionnaires. The Contractor will provide a time line for corrective action.

2.100 Confidentiality

2.101 CONFIDENTIALITY

Contractor and the State each acknowledge that the other possesses and will continue to possess confidential information that has been developed or received by it. As used in this Section, “Confidential Information” of Contractor must mean all non-public proprietary information of Contractor (other than Confidential Information of the State as defined below), which is marked confidential, restricted, proprietary, or with a similar designation. “Confidential Information” of the State must mean any information which is retained in confidence by the State (or otherwise required to be held in confidence by the State under applicable federal, state and local laws and regulations) or which, in the case of tangible materials provided to Contractor by the State under its performance under this Contract, is marked as confidential, proprietary or with a similar designation by the State. “Confidential Information” excludes any information (including this Contract) that is publicly available under the Michigan FOIA.

2.102 PROTECTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION

The State and Contractor will each use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication or dissemination of its own confidential information of like character, but in no event less than reasonable care. Neither Contractor nor the State will (i) make any use of the Confidential Information of the other except as contemplated by this Contract, (ii) acquire any right in or assert any lien against the Confidential Information of the other, or (iii) if requested to do so, refuse for any reason to promptly return the other party's Confidential Information to the other party. Each party will limit disclosure of the other party’s Confidential Information to employees and Subcontractors who must have access to fulfill the purposes of this Contract. Disclosure to, and use by, a Subcontractor is permissible where (A) use of a Subcontractor is authorized under this Contract, (B) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Subcontractor's scope of responsibility, and (C) Contractor obligates the Subcontractor in a written Contract to maintain the State’s Confidential Information in confidence. Any employee of Contractor and any Subcontractor having access or continued access to the State’s Confidential Information shall be subject to a written confidentiality agreement that shall be no less restrictive than the provisions of this section.

Promptly upon termination or cancellation of the Contract for any reason and receipt of a written request from the State, Contractor must certify to the State that Contractor has destroyed all State Confidential Information in the data base and disposed of all other State information in accordance with Contractor's record retention policies and consistent with Payment Card Industry requirements.

2.103 EXCLUSIONS

Notwithstanding the foregoing, the provisions in this Section will not apply to any particular information which the State or Contractor can demonstrate (i) was, at the time of disclosure to it, in the public domain; (ii) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party; (iii) was in the possession of the receiving party at the time of disclosure to it without an obligation of confidentiality; (iv) was received after disclosure to it from a third party who had a lawful right to disclose the information to it without any obligation to restrict its further disclosure; or (v) was independently developed by the receiving party without reference to Confidential Information of the furnishing party. Further, the provisions of this Section will not apply to any particular Confidential Information to the extent the receiving party is required by law to disclose the Confidential Information, provided that the receiving party (i) promptly provides the furnishing party with notice of the legal request, and (ii) assists the furnishing party in resisting or limiting the scope of the disclosure as reasonably requested by the furnishing party.

2.104 NO IMPLIED RIGHTS

Nothing contained in this Section must be construed as obligating a party to disclose any particular Confidential Information to the other party, or as granting to or conferring on a party, expressly or impliedly, any right or license to the Confidential Information of the other party.

2.105 RESPECTIVE OBLIGATIONS

The parties' respective obligations under this Section must survive the termination or expiration of this Contract for any reason.

2.110 Records and Inspections

2.111 INSPECTION OF WORK PERFORMED

The State's authorized representatives must at all reasonable times and with thirty (30) days prior written request, have the right to enter Contractor's premises, where the Services are being performed, and must have access, upon reasonable request, to interim drafts of Deliverables or work-in-progress. Upon thirty (30) Days prior written notice and at all reasonable times, the State's representatives must be allowed to inspect, monitor, or otherwise evaluate the work being performed; provided that such inspections shall be conducted during normal business hours at the State's own expense in a manner that does not disrupt Contractor's business. The State shall abide by all Contractor work rules and security regulations while conducting such inspections.

2.112 EXAMINATION OF RECORDS

For five years after the Contractor provides any work under this Contract (the "Audit Period"), the State may audit the Contractor's reasonable records related to the products or Services provided under this Agreement; provided that the State gives Contractor at least thirty (30) days prior written notice and does not conduct such audits more frequently than once in any one (1) year period. Such audit shall be conducted during normal business hours at the State's own expense in a manner that does not disrupt Contractor's business. The State shall abide by all Contractor work rules and security regulations while conducting such audit.. The State does not have the right to review any information deemed confidential by the Contractor to the extent access would require the confidential information to become publicly available.

2.113 RETENTION OF RECORDS

Contractor must maintain reasonable records pertaining to the products and Services provided to the State under this Contract for the periods required by Contractor's records retention policies

2.114 AUDIT RESOLUTION

If necessary, the Contractor and the State will meet to review each audit report promptly after issuance. The Contractor will respond to each audit report in writing within 30 days from receipt of the report, unless a shorter response time is specified in the report. The Contractor and the State agree to address issues that the parties mutually agree pose a concern or to address any issues which are identified as a material breach that were identified as a result of the audit.

2.115 ERRORS

If the audit demonstrates any errors in the documents provided to the State, then the amount in error must be reflected as a credit or debit on the next invoice and in subsequent invoices until the amount is paid or refunded in full. However, a credit or debit may not be carried for more than four invoices. If a balance remains after four invoices, then the remaining amount will be due as a payment or refund within 45 days of the last quarterly invoice that the balance appeared on or termination of the contract, whichever is earlier.

In addition to other available remedies, the difference between the payment received and the correct payment amount is greater than 10%, then the Contractor must pay all of the reasonable costs of the audit.

2.120 Warranties

2.121 WARRANTIES AND REPRESENTATIONS

The Contractor represents and warrants:

(a) It is capable in all respects of fulfilling and must fulfill all of its obligations under this Contract. The performance of all obligations under this Contract must be provided in a timely, professional, and workman-like manner and must meet the performance and operational standards required under this Contract.

(b) The Contract Appendices, Attachments and Exhibits identify the equipment and software and services necessary for the Deliverable(s) to perform and Services to operate in compliance with the Contract's requirements and other standards of performance.

(c) It is the lawful owner or licensee of any Deliverable licensed or sold to the State by Contractor or developed by Contractor under this Contract, and Contractor has all of the rights necessary to convey to the State the ownership rights or licensed use, as applicable, of any and all Deliverables.

(d) If, under this Contract, Contractor procures any equipment, software or other Deliverable for the State (including equipment, software and other Deliverables manufactured, re-marketed or otherwise sold by Contractor under Contractor's name), then in addition to Contractor's other responsibilities with respect to the items in this Contract, Contractor must assign or otherwise transfer to the State or its designees, or afford the State the benefits of, any manufacturer's warranty for the Deliverable.

(e) The contract signatory has the power and authority, including any necessary corporate authorizations, necessary to enter into this Contract, on behalf of Contractor.

(f) It is qualified and registered to transact business in all locations where required.

(g) Neither the Contractor nor any Affiliates, nor any employee of either, has, must have, or must acquire, any contractual, financial, business, or other interest, direct or indirect, that would conflict in any manner or degree with Contractor's performance of its duties and responsibilities to the State under this Contract or otherwise create an appearance of impropriety with respect to the award or performance of this Agreement. Contractor must notify the State about the nature of the conflict or appearance of impropriety within two days of learning about it.

(h) Neither Contractor nor any Affiliates, nor any employee of either has accepted or must accept anything of value based on an understanding that the actions of the Contractor or Affiliates or employee on behalf of the State would be influenced. Contractor must not attempt to influence any State employee by the direct or indirect offer of anything of value.

(i) Neither Contractor nor any Affiliates, nor any employee of either has paid or agreed to pay any person, other than bona fide employees and consultants working solely for Contractor or the Affiliate, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Contract.

(j) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other bidder; and no attempt was made by Contractor to induce any other person to submit or not submit a proposal for the purpose of restricting competition.

(k) All financial statements, reports, and other information furnished by Contractor to the State as part of its response to the RFP or otherwise in connection with the award of this Contract fairly and accurately represent the business, properties, financial condition, and results of operations of Contractor as of the respective dates, or for the respective periods, covered by the financial statements, reports, other information. Since the respective dates or periods covered by the financial statements, reports, or other information, there have been no material adverse changes in the business, properties, financial condition, or results of operations of Contractor.

(l) All written information furnished to the State by or for the Contractor in connection with this Contract, including its bid, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading.

(m) It is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State or the department within the previous five years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract.

(n) If any of the certifications, representations, or disclosures made in the Contractor's original bid response change after contract award, the Contractor is required to report those changes immediately to the Department of Technology, Management and Budget, Purchasing Operations.

2.122 WARRANTY

Contractor warrants that the Contractor's system will perform in accordance with the specifications in Article 1 – Statement of Work of the Contractor's response to Section 1.104 of the RFP.

EXCEPT AS SPECIFICALLY SET FORTH IN THIS CONTRACT, CONTRACTOR DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH RELATE TO THE SERVICES PROVIDED UNDER THIS CONTRACT. FURTHER, CONTRACTOR DOES NOT WARRANT THAT THE STATE'S USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. THIS CONTRACT IS A SERVICE AGREEMENT, ANY EQUIPMENT PROVIDED TO THE STATE UNDER THIS CONTRACT IS INCIDENTAL TO THE SERVICES PROVIDED, AND THE PROVISIONS OF THE UNIFORM COMMERCIAL CODE DO NOT APPLY TO THIS CONTRACT.

2.123 RESERVED

2.124 RESERVED

2.125 RESERVED

2.126 EQUIPMENT TO BE NEW

If applicable, all equipment provided under this Contract by Contractor shall be new where Contractor has knowledge regarding whether the equipment is new or assembled from new or serviceable used parts that are like new in performance or has the option of selecting one or the other. Equipment that is assembled from new or serviceable used parts that are like new in performance is acceptable where Contractor does not have knowledge or the ability to select one or other, unless specifically agreed otherwise in writing by the State.

2.127 PROHIBITED PRODUCTS

The State will not accept salvage, distressed, outdated or discontinued merchandise. Shipping of such merchandise to any State agency, as a result of an order placed against the Contract, shall be considered default by the Contractor of the terms and conditions of the Contract and may result in cancellation of the Contract by the State. The brand and product number offered for all items shall remain consistent for the term of the Contract, unless Purchasing Operations has approved a change order pursuant to **Section 2.024**.

2.128 CONSEQUENCES FOR BREACH

In addition to any remedies available in law, if the Contractor breaches any of the warranties contained in this section, the breach may be considered as a default in the performance of a material obligation of this Contract.

2.130 Insurance

2.131 LIABILITY INSURANCE

The Contractor must provide proof of the minimum levels of insurance coverage as indicated below. The insurance must protect the State from claims that may arise out of or result from the Contractor's performance of services under the terms of this Contract, whether the services are performed by the Contractor, or by any subcontractor, or by anyone directly or indirectly employed by any of them, or by anyone for whose acts they may be liable.

The Contractor waives all rights against the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents for recovery of damages to the extent these damages are covered by the insurance policies the Contractor is required to maintain under this Contract.

All insurance coverage provided relative to this Contract/Purchase Order is PRIMARY and NON-CONTRIBUTING to any comparable liability insurance (including self-insurances) carried by the State.

The insurance must be written for not less than any minimum coverage specified in this Contract or required by law, whichever is greater.

The insurers selected by Contractor must have an A.M. Best rating of A or better, or as otherwise approved in writing by the State, or if the ratings are no longer available, with a comparable rating from a recognized insurance rating agency. All policies of insurance required in this Contract must be issued by companies that have been approved to do business in the State.
See www.michigan.gov/dleg.

Where specific limits are shown, they are the minimum acceptable limits. If Contractor's policy contains higher limits, the State must be entitled to coverage to the extent of the higher limits.

The Contractor is required to pay for and provide the type and amount of insurance checked ☑ below:

☑ 1. Commercial General Liability with the following minimum coverage:
$2,000,000 General Aggregate Limit other than Products/Completed Operations
$2,000,000 Products/Completed Operations Aggregate Limit
$1,000,000 Personal & Advertising Injury Limit
$1,000,000 Each Occurrence Limit

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents as ADDITIONAL INSUREDS on the Commercial General Liability certificate. The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company.

☑ 2. If a motor vehicle is used to provide services or products under this Contract, the Contractor must have vehicle liability insurance on any auto including owned, hired and non-owned vehicles used in Contractor's business for bodily injury and property damage as required by law.

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents as ADDITIONAL INSUREDS on the vehicle liability certificate. The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company.

☑ 3. Workers' compensation coverage must be provided according to applicable laws governing the employees and employers work activities in the state of the Contractor's domicile. If a self-insurer provides the applicable coverage, proof must be provided of approved self-insured authority by the jurisdiction of domicile. For employees working outside of the state of qualification, Contractor must provide appropriate certificates of insurance proving mandated coverage levels for the jurisdictions where the employees' activities occur.

Any certificates of insurance received must also provide a list of states where the coverage is applicable.

The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company. This provision must not be applicable where prohibited or limited by the laws of the jurisdiction in which the work is to be performed.

☑ 4. Employers liability insurance with the following minimum limits:
$100,000 each accident
$100,000 each employee by disease
$500,000 aggregate disease

☑ 5. Employee Fidelity, including Computer Crimes, insurance naming the State as a loss payee, providing coverage for direct loss to the State and any legal liability of the State arising out of or related to fraudulent or dishonest acts committed by the employees of Contractor or its Subcontractors, acting alone or in collusion with others, in a minimum amount of one million dollars ($1,000,000.00).

☑ 6. Umbrella or Excess Liability Insurance in a minimum amount of ten million dollars ($10,000,000.00), which must apply, at a minimum, to the insurance required in Subsection 1 (Commercial General Liability) above.

☑ 7. Professional Liability (Errors and Omissions) Insurance with the following minimum coverage: three million dollars ($3,000,000.00) each occurrence and three million dollars ($3,000,000.00) annual aggregate.

☑ 8. Fire and Personal Property Insurance covering against any loss or damage to the office space used by Contractor for any reason under this Contract, and the equipment, software and other contents of the office space, including without limitation, those contents used by Contractor to provide the Services to the State, up to its replacement value, where the office space and its contents are under the care, custody and control of Contractor. The policy must cover all risks of direct physical loss or damage, including without limitation, flood and earthquake coverage and coverage for computer hardware and software. The State must be endorsed on the policy as a loss payee as its interests appear.

2.132 SUBCONTRACTOR INSURANCE COVERAGE

Except where the State has approved in writing a Contractor subcontract with other insurance provisions, Contractor must require all of its Subcontractors under this Contract to purchase and maintain the insurance coverage as described in this Section for the Contractor in connection with the performance of work by those Subcontractors. Alternatively, Contractor may include any Subcontractors under Contractor’s insurance on the coverage required in this Section. Subcontractor(s) must fully comply with the insurance coverage required in this Section. Failure of Subcontractor(s) to comply with insurance requirements does not limit Contractor’s liability or responsibility.

2.133 CERTIFICATES OF INSURANCE AND OTHER REQUIREMENTS

Contractor must furnish to DTMB Purchasing Operations, certificate(s) of insurance verifying insurance coverage or providing satisfactory evidence of self-insurance as required in this Section (the “Certificates”). The Certificate must be on the standard “accord” form or equivalent. **The Contract Number or the Purchase Order Number must be shown on the Certificate Of Insurance To Assure Correct Filing.** All Certificate(s) are to be prepared and submitted by the Insurance Provider. Contractor agrees to provide the Director of Purchasing Operations, Department of Technology, Management and Budget, with 30 days prior written notice, except for 10 days for non-payment of premium, of cancellation of any of insurance coverage required in this Section. The notice must include the Contract or Purchase Order number affected. Before the Contract is signed, and not less than 20 days before the insurance expiration date every year thereafter, the Contractor must provide evidence that the State and its agents, officers and employees are listed as additional insured under each commercial general liability and commercial automobile liability policy. In the event the State approves the representation of the State by the insurer’s attorney, the attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.

The Contractor must maintain all required insurance coverage throughout the term of the Contract and any extensions and, in the case of claims-made Commercial General Liability policies, must secure tail coverage for at least three years following the expiration or termination for any reason of this Contract. The minimum limits of coverage specified above are not intended, and must not be construed; to limit any liability or indemnity of Contractor under this Contract to any indemnified party or other persons. Contractor is responsible for all deductibles with regard to the insurance. If the Contractor fails to pay any premium for required insurance as specified in this Contract, or if any insurer cancels or significantly reduces any required insurance as specified in this Contract without the State's written consent, then the State may, after the State has given the Contractor at least 30 days written notice, pay the premium or procure similar insurance coverage from another company or companies. The State may deduct any part of the cost from any payment due the Contractor, or the Contractor must pay that cost upon demand by the State.

2.140 Indemnification

2.141 GENERAL INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from liability, including all claims and losses, and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties), accruing or resulting to any person, firm or corporation that may be injured or damaged by the Contractor in the performance of this Contract and that are attributable to the negligence or tortious acts of the Contractor or any of its subcontractors, or by anyone else for whose acts any of them may be liable.

2.142 CODE INDEMNIFICATION

To the extent permitted by law, the Contractor shall indemnify, defend and hold harmless the State from any claim, loss, or expense arising from Contractor's breach of the No Surreptitious Code Warranty.

2.143 EMPLOYEE INDEMNIFICATION

In any claims against the State of Michigan, its departments, divisions, agencies, sections, commissions, officers, employees and agents, by any employee of the Contractor or any of its subcontractors, the indemnification obligation under the Contract must not be limited in any way by the amount or type of damages, compensation or benefits payable by or for the Contractor or any of its subcontractors under worker's disability compensation acts, disability benefit acts or other employee benefit acts. This indemnification clause is intended to be comprehensive. Any overlap in provisions, or the fact that greater specificity is provided as to some categories of risk, is not intended to limit the scope of indemnification under any other provisions.

2.144 PATENT/COPYRIGHT INFRINGEMENT INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from and against all losses, liabilities, damages (including taxes), and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) incurred in connection with any action or proceeding threatened or brought against the State to the extent that the action or proceeding is based on a claim that any piece of equipment, software, commodity or service supplied by the Contractor or its subcontractors, or the operation of the equipment, software, commodity or service, or the use or reproduction of any documentation provided with the equipment, software, commodity or service infringes any United States patent, copyright, trademark or trade secret of any person or entity, which is enforceable under the laws of the United States.

In addition, should the equipment, software, commodity, or service, or its operation, become or in the State's or Contractor's opinion be likely to become the subject of a claim of infringement, the Contractor must at the Contractor's sole expense (i) procure for the State the right to continue using the equipment, software, commodity or service or, if the option is not reasonably available to the Contractor, (ii) replace or modify to the State's satisfaction the same with equipment, software, commodity or service of equivalent function and performance so that it becomes non-infringing, or, if the option is not reasonably available to Contractor, (iii) accept its return by the State with appropriate credits to the State against the Contractor's charges and reimburse the State for any actual losses or costs incurred as a consequence of the State ceasing its use and returning it.

Notwithstanding the foregoing, the Contractor has no obligation to indemnify or defend the State for, or to pay any costs, damages or attorneys' fees related to, any claim based upon (i) equipment, software, comoodity or services developed based on written specifications of the State; (ii) use of the equipment, software, commodity or service in a configuration other than implemented or approved in writing by the Contractor, including, but not limited to, any modification of the equipment, software, commodity or service by the State; or (iii) the combination, operation, or use of the equipment, software, commodity or service with equipment or software not supplied by the Contractor under this Contract.

2.145 CONTINUATION OF INDEMNIFICATION OBLIGATIONS

The Contractor's duty to indemnify under this Section continues in full force and effect, notwithstanding the expiration or early cancellation of the Contract, with respect to any claims based on facts or conditions that occurred before expiration or cancellation.

2.146 INDEMNIFICATION PROCEDURES

The procedures set forth below must apply to all indemnity obligations under this Contract.

(a) After the State receives notice of the action or proceeding involving a claim for which it will seek indemnification, the State must promptly notify Contractor of the claim in writing and take or assist Contractor in taking, as the case may be, any reasonable action to avoid the imposition of a default judgment against Contractor. No failure to notify the Contractor relieves the Contractor of its indemnification obligations except to the extent that the Contractor can prove damages attributable to the failure. Within 10 days following receipt of written notice from the State relating to any claim, the Contractor must notify the State in writing whether Contractor agrees to assume control of the defense and settlement of that claim (a "Notice of Election"). After notifying Contractor of a claim and before the State receiving Contractor's Notice of Election, the State is entitled to defend against the claim, at the Contractor's expense, and the Contractor will be responsible for any reasonable costs incurred by the State in defending against the claim during that period.

(b) If Contractor delivers a Notice of Election relating to any claim: (i) the State is entitled to participate in the defense of the claim and to employ counsel at its own expense to assist in the handling of the claim and to monitor and advise the State about the status and progress of the defense; (ii) the Contractor must, at the request of the State, demonstrate to the reasonable satisfaction of the State, the Contractor's financial ability to carry out its defense and indemnity obligations under this Contract; (iii) the Contractor must periodically advise the State about the status and progress of the defense and must obtain the prior written approval of the State before entering into any settlement of the claim or ceasing to defend against the claim and (iv) to the extent that any principles of Michigan governmental or public law may be involved or challenged, the State has the right, at its own expense, to control the defense of that portion of the claim involving the principles of Michigan governmental or public law. But the State may retain control of the defense and settlement of a claim by notifying the Contractor in writing within 10 days after the State's receipt of Contractor's information requested by the State under clause (ii) of this paragraph if the State determines that the Contractor has failed to demonstrate to the reasonable satisfaction of the State the Contractor's financial ability to carry out its defense and indemnity obligations under this Section. Any litigation activity on behalf of the State, or any of its subdivisions under this Section, must be coordinated with the Department of Attorney General. In the event the insurer's attorney represents the State under this Section, the insurer's attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.

(c) If Contractor does not deliver a Notice of Election relating to any claim of which it is notified by the State as provided above, the State may defend the claim in the manner as it may deem appropriate, at the cost and expense of Contractor. If it is determined that the claim was one against which Contractor was required to indemnify the State, upon request of the State, Contractor must promptly reimburse the State for all the reasonable costs and expenses.

2.150 Termination/Cancellation

2.151 NOTICE AND RIGHT TO CURE

If the Contractor breaches the contract, and the State in its sole discretion determines that the breach is curable, then the State will provide the Contractor with written notice of the breach and a time period (not less than 30 days) to cure the Breach. The notice of breach and opportunity to cure is inapplicable for successive or repeated breaches or if the State determines in its sole discretion that the breach poses a serious and imminent threat to the health or safety of any person or the imminent loss, damage, or destruction of any real or tangible personal property.

2.152 TERMINATION FOR CAUSE

(a) The State may terminate this contract, for cause, by notifying the Contractor in writing, if the Contractor (i) breaches any of its material duties or obligations under this Contract (including a Chronic Failure to meet any particular SLA), or (ii) fails to cure a breach within the time period specified in the written notice of breach provided by the State

(b) If this Contract is terminated for cause, the Contractor must pay all costs incurred by the State in terminating this Contract, including but not limited to, State administrative costs, reasonable attorneys' fees and court costs, and any reasonable additional costs the State may incur to procure the Services/Deliverables required by this Contract from other sources. Re-procurement costs are not consequential, indirect or incidental damages, and cannot be excluded by any other terms otherwise included in this Contract, provided the costs are not in excess of 50% more than the prices for the Service/Deliverables provided under this Contract.

(c) If the State chooses to partially terminate this Contract for cause, charges payable under this Contract will be equitably adjusted to reflect those Services/Deliverables that are terminated and the State must pay for all Services/Deliverables for which Final Acceptance has been granted provided up to the termination date. Services and related provisions of this Contract that are terminated for cause must cease on the effective date of the termination.

(d) If the State terminates this Contract for cause under this Section, and it is determined, for any reason, that Contractor was not in breach of contract under the provisions of this section, that termination for cause must be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties must be limited to that otherwise provided in this Contract for a termination for convenience.

2.153 TERMINATION FOR CONVENIENCE

The State may terminate this Contract for its convenience, in whole or part, if the State determines that a termination is in the State's best interest. Reasons for the termination must be left to the sole discretion of the State and may include, but not necessarily be limited to (a) the State no longer needs the Services or products specified in the Contract, (b) relocation of office, program changes, changes in laws, rules, or regulations make implementation of the Services no longer practical or feasible, (c) unacceptable prices for Additional Services or New Work requested by the State, or (d) falsification or misrepresentation, by inclusion or non-inclusion, of information material to a response to any RFP issued by the State. The State may terminate this Contract for its convenience, in whole or in part, by giving Contractor written notice at least 30 days before the date of termination. If the State chooses to terminate this Contract in part, the charges payable under this Contract must be equitably adjusted to reflect those Services/Deliverables that are terminated. Services and related provisions of this Contract that are terminated for cause must cease on the effective date of the termination.

2.154 TERMINATION FOR NON-APPROPRIATION

(a) Contractor acknowledges that, if this Contract extends for several fiscal years, continuation of this Contract is subject to appropriation or availability of funds for this Contract. If funds to enable the State to effect continued payment under this Contract are not appropriated or otherwise made available, the State must terminate this Contract and all affected Statements of Work, in whole or in part, at the end of the last period for which funds have been appropriated or otherwise made available by giving written notice of termination to Contractor. The State must give Contractor at least 30 days advance written notice of termination for non-appropriation or unavailability (or the time as is available if the State receives notice of the final decision less than 30 days before the funding cutoff).

(b) If funding for the Contract is reduced by law, or funds to pay Contractor for the agreed-to level of the Services or production of Deliverables to be provided by Contractor are not appropriated or otherwise unavailable, the State may, upon 30 days written notice to Contractor, reduce the level of the Services or the change the production of Deliverables in the manner and for the periods of time as the State may elect. The charges payable under this Contract will be equitably adjusted to reflect any equipment, services or commodities not provided by reason of the reduction.

(c) If the State terminates this Contract, eliminates certain Deliverables, or reduces the level of Services to be provided by Contractor under this Section, the State must pay Contractor for all Work-in-Process performed through the effective date of the termination or reduction in level, as the case may be and as determined by the State, to the extent funds are available. This Section will not preclude Contractor from reducing or stopping Services/Deliverables or raising against the State in a court of competent jurisdiction, any claim for a shortfall in payment for Services performed or Deliverables finally accepted before the effective date of termination.

2.155 TERMINATION FOR CRIMINAL CONVICTION

The State may terminate this Contract immediately and without further liability or penalty in the event Contractor, an officer of Contractor, or an owner of a 25% or greater share of Contractor is convicted of a criminal offense related to a State, public or private Contract or subcontract.

2.156 TERMINATION FOR APPROVALS RESCINDED

The State may terminate this Contract if any final administrative or judicial decision or adjudication disapproves a previously approved request for purchase of personal services under Constitution 1963, Article 11, § 5, and Civil Service Rule 7-1. In that case, the State will pay the Contractor for only the work completed to that point under the Contract. Termination may be in whole or in part and may be immediate as of the date of the written notice to Contractor or may be effective as of the date stated in the written notice.

2.157 RIGHTS AND OBLIGATIONS UPON TERMINATION

(a) If the State terminates this Contract for any reason, the Contractor must (a) stop all work as specified in the notice of termination, (b) take any action that may be necessary, or that the State may direct, for preservation and protection of Deliverables or other property derived or resulting from this Contract that may be in Contractor's possession, (c) return all materials and property provided directly or indirectly to Contractor by any entity, agent or employee of the State, (d) transfer title in, and deliver to, the State, unless otherwise directed, all Deliverables intended to be transferred to the State at the termination of the Contract and which are resulting from the Contract (which must be provided to the State on an "As-Is" basis except to the extent the amounts paid by the State in respect of the items included compensation to Contractor for the provision of warranty services in respect of the materials), and (e) take any action to mitigate and limit any potential damages, or requests for Contractor adjustment or termination settlement costs, to the maximum practical extent, including terminating or limiting as otherwise applicable those subcontracts and outstanding orders for material and supplies resulting from the terminated Contract.

(b) If the State terminates this Contract before its expiration for its own convenience, the State must pay Contractor for all charges due for Services provided before the date of termination and, if applicable, as a separate item of payment under this Contract, for Work In Process, on a percentage of completion basis at the level of completion determined by the State. All completed or partially completed Deliverables prepared by Contractor under this Contract, at the option of the State, becomes the State's property, and Contractor is entitled to receive equitable fair compensation for the Deliverables. Regardless of the basis for the termination, the State is not obligated to pay, or otherwise compensate, Contractor for any lost expected future profits, costs or expenses incurred with respect to Services not actually performed for the State.

(c) Upon a good faith termination, the State may assume, at its option, any subcontracts and agreements for services and deliverables provided under this Contract, and may further pursue completion of the Services/Deliverables under this Contract by replacement contract or otherwise as the State may in its sole judgment deem expedient.

2.158 RESERVATION OF RIGHTS

Any termination of this Contract or any Statement of Work issued under it by a party must be with full reservation of, and without prejudice to, any rights or remedies otherwise available to the party with respect to any claims arising before or as a result of the termination.

2.160 Termination by Contractor

2.161 TERMINATION BY CONTRACTOR

If the State breaches the Contract, and the Contractor in its sole discretion determines that the breach is curable, then the Contractor will provide the State with written notice of the breach and a time period (not less than 30 days) to cure the breach. The Notice of Breach and opportunity to cure is inapplicable for successive and repeated breaches.

The Contractor may terminate this Contract if the State (i) materially breaches its obligation to pay the Contractor undisputed amounts due and owing under this Contract, (ii) breaches its other obligations under this Contract to an extent that makes it impossible or commercially impractical for the Contractor to perform the Services, or (iii) does not cure the breach within the time period specified in a written notice of breach. But the Contractor must discharge its obligations under **Section 2.160** before it terminates the Contract.

2.170 Transition Responsibilities

2.171 CONTRACTOR TRANSITION RESPONSIBILITIES

If the State terminates this contract, for convenience or cause, or if the Contract is otherwise dissolved, voided, rescinded, nullified, expires or rendered unenforceable, the Contractor agrees to comply with direction provided by the State to assist in the orderly transition of equipment, services, software, leases, etc. to the State or a third party designated by the State. If this Contract expires or terminates, the Contractor agrees to make all reasonable efforts to effect an orderly transition of services within a reasonable period of time that in no event will exceed one hundred eighty (180) days. These efforts must include, but are not limited to, those listed in **Sections 2.141, 2.142, 2.143, 2.144, and 2.145.**

2.172 CONTRACTOR PERSONNEL TRANSITION

The Contractor must work with the State, or a specified third party, to develop a transition plan setting forth the specific tasks and schedule to be accomplished by the parties, to effect an orderly transition. The Contractor must allow as many personnel as practicable to remain on the job to help the State, or a specified third party, maintain the continuity and consistency of the services required by this Contract. In addition, during or following the transition period, in the event the State requires the Services of the Contractor’s subcontractors or vendors, as necessary to meet its needs, Contractor agrees to reasonably, and with good-faith, work with the State to use the Services of Contractor’s subcontractors or vendors. Contractor will notify all of Contractor’s subcontractors of procedures to be followed during transition.

2.173 CONTRACTOR INFORMATION TRANSITION

Contractor will provide transition assistance as a billable item; using the hourly rate in Article 1, Attachment A. Contractor will draft a Statement of Work outlining the project purpose, scope, and cost associated with the migration.

2.174 RESERVED

2.175 TRANSITION PAYMENTS

If the transition results from a termination for any reason, the termination provisions of this Contract must govern reimbursement. If the transition results from expiration, the Contractor will be reimbursed for all reasonable transition costs (i.e. costs incurred within the agreed period after contract expiration that result from transition operations) at the rates agreed upon by the State. The Contractor will prepare an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

2.176 STATE TRANSITION RESPONSIBILITIES

In the event that this Contract is terminated, dissolved, voided, rescinded, nullified, or otherwise rendered unenforceable, the State agrees to reconcile all accounts between the State and the Contractor, complete any pending post-project reviews and perform any others obligations upon which the State and the Contractor agree.

(a) Reconciling all accounts between the State and the Contractor;
(b) Completing any pending post-project reviews.

2.180 Stop Work

2.181 STOP WORK ORDERS

The State may, at any time, by written stop work order to Contractor, require that Contractor stop all, or any part, of the work called for by the Contract for a period of up to 90 calendar days after the stop work order is delivered to Contractor, and for any further period to which the parties may agree. The stop work order must be identified as a stop work order and must indicate that it is issued under this **Section 2.150**. Upon receipt of the stop work order, Contractor must immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the stop work order during the period of work stoppage. Within the period of the stop work order, the State must either: (a) cancel the stop work order; or (b) terminate the work covered by the stop work order as provided in **Section 2.130**.

2.182 CANCELLATION OR EXPIRATION OF STOP WORK ORDER

The Contractor must resume work if the State cancels a Stop Work Order or if it expires. The parties will agree upon an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract must be modified, in writing, accordingly, if: (a) the stop work order results in an increase in the time required for, or in Contractor's costs properly allocable to, the performance of any part of the Contract; and (b) Contractor asserts its right to an equitable adjustment within 30 calendar days after the end of the period of work stoppage; provided that, if the State decides the facts justify the action, the State may receive and act upon a Contractor proposal submitted at any time before final payment under the Contract. Any adjustment will conform to the requirements of **Section 2.024**.

2.183 ALLOWANCE OF CONTRACTOR COSTS

If the stop work order is not canceled and the work covered by the stop work order is terminated for reasons other than material breach, the termination must be deemed to be a termination for convenience under **Section 2.153**, and the State will pay reasonable costs resulting from the stop work order in arriving at the termination settlement. For the avoidance of doubt, the State is not liable to Contractor for loss of profits because of a stop work order issued under this Section**.**

2.190 Dispute Resolution

2.191 IN GENERAL

Any claim, counterclaim, or dispute between the State and Contractor arising out of or relating to the Contract or any Statement of Work must be resolved as follows. For all Contractor claims seeking an increase in the amounts payable to Contractor under the Contract, or the time for Contractor's performance, Contractor must submit a letter, together with all data supporting the claims, executed by Contractor's Contract Administrator or the Contract Administrator's designee certifying that (a) the claim is made in good faith, (b) the amount claimed accurately reflects the adjustments in the amounts payable to Contractor or the time for Contractor's performance for which Contractor believes the State is liable and covers all costs of every type to which Contractor is entitled from the occurrence of the claimed event, and (c) the claim and the supporting data are current and complete to Contractor's best knowledge and belief.

2.192 INFORMAL DISPUTE RESOLUTION

(a) All disputes between the parties must be resolved under the Contract Management procedures in this Contract. If the parties are unable to resolve any disputes after compliance with the processes, the parties must meet with the Director of Purchasing Operations, DTMB, or designee, for the purpose of attempting to resolve the dispute without the need for formal legal proceedings, as follows:

(1) The representatives of Contractor and the State must meet as often as the parties reasonably deem necessary to gather and furnish to each other all information with respect to the matter in issue which the parties believe to be appropriate and germane in connection with its resolution. The representatives must discuss the problem and negotiate in good faith in an effort to resolve the dispute without the necessity of any formal proceeding.

(2) During the course of negotiations, all reasonable requests made by one party to another for non-privileged information reasonably related to the Contract will be honored in order that each of the parties may be fully advised of the other's position.
(3) The specific format for the discussions will be left to the discretion of the designated State and Contractor representatives, but may include the preparation of agreed upon statements of fact or written statements of position.
(4) Following the completion of this process within 60 calendar days, the Director of Purchasing Operations, DTMB, or designee, must issue a written opinion regarding the issue(s) in dispute within 30 calendar days. The opinion regarding the dispute must be considered the State's final action and the exhaustion of administrative remedies.
(b) This Section will not be construed to prevent either party from instituting, and a party is authorized to institute, formal proceedings earlier to avoid the expiration of any applicable limitations period, to preserve a superior position with respect to other creditors, or under Section 2.193.
(c) The State will not mediate disputes between the Contractor and any other entity, except state agencies, concerning responsibility for performance of work under the Contract.

2.193 INJUNCTIVE RELIEF

The only circumstance in which disputes between the State and Contractor will not be subject to the provisions of **Section 2.192** is where a party makes a good faith determination that a breach of the terms of the Contract by the other party is the that the damages to the party resulting from the breach will be so immediate, so large or severe and so incapable of adequate redress after the fact that a temporary restraining order or other immediate injunctive relief is the only adequate remedy.

2.194 CONTINUED PERFORMANCE

Each party agrees to continue performing its obligations under the Contract while a dispute is being resolved except to the extent the issue in dispute precludes performance (dispute over payment must not be deemed to preclude performance) and without limiting either party's right to terminate the Contract as provided in **Section 2.150**, as the case may be.

<u>2.200 Federal and State Contract Requirements</u>

2.201 NONDISCRIMINATION

In the performance of the Contract, Contractor agrees not to discriminate against any employee or applicant for employment, with respect to his or her hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of race, color, religion, national origin, ancestry, age, sex, height, weight, and marital status, physical or mental disability. Contractor further agrees that every subcontract entered into for the performance of this Contract or any purchase order resulting from this Contract will contain a provision requiring non-discrimination in employment, as specified here, binding upon each Subcontractor. This covenant is required under the Elliot Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, et seq., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., and any breach of this provision may be regarded as a material breach of the Contract.

2.202 UNFAIR LABOR PRACTICES

Under 1980 PA 278, MCL 423.321, et seq., the State must not award a Contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled under section 2 of the Act. This information is compiled by the United States National Labor Relations Board. A Contractor of the State, in relation to the Contract, must not enter into a contract with a Subcontractor, manufacturer, or supplier whose name appears in this register. Under section 4 of 1980 PA 278, MCL 423.324, the State may void any Contract if, after award of the Contract, the name of Contractor as an employer or the name of the Subcontractor, manufacturer or supplier of Contractor appears in the register.

2.203 WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT

In performing Services for the State, the Contractor must comply with the Department of Civil Services Rule 2-20 regarding Workplace Safety and Rule 1-8.3 regarding Discriminatory Harassment. In addition, the Contractor must comply with Civil Service regulations and any applicable agency rules provided to the Contractor. For Civil Service Rules, see http://www.mi.gov/mdcs/0,1607,7-147-6877---,00.html.

2.204 PREVAILING WAGE

The rates of wages and fringe benefits to be paid each class of individuals employed by the Contractor, its subcontractors, their subcontractors, and all persons involved with the performance of this Contract in privity of contract with the Contractor shall not be less than the wage rates and fringe benefits established by the Michigan Department of Labor and Economic Development, Wage and Hour Bureau, schedule of occupational classification and wage rates and fringe benefits for the local where the work is to be performed. The term Contractor shall include all general contractors, prime contractors, project managers, trade contractors, and all of their contractors or subcontractors and persons in privity of contract with them.

The Contractor, its subcontractors, their subcontractors and all persons involved with the performance of this contract in privity of contract with the Contractor shall keep posted on the work site, in a conspicuous place, a copy of all wage rates and fringe benefits as prescribed in the contract. You must also post, in a conspicuous place, the address and telephone number of the Michigan Department of Labor and Economic Development, the office responsible for enforcement of the wage rates and fringe benefits. You shall keep an accurate record showing the name and occupation of the actual wage and benefits paid to each individual employed in connection with this contract. This record shall be available to the State upon request for reasonable inspection.

If any trade is omitted from the list of wage rates and fringe benefits to be paid to each class of individuals by the Contractor, it is understood that the trades omitted shall also be paid not less than the wage rate and fringe benefits prevailing in the local where the work is to be performed.

2.210 Governing Law

2.211 GOVERNING LAW

The Contract must in all respects be governed by, and construed according to, the substantive laws of the State of Michigan without regard to any Michigan choice of law rules that would apply the substantive law of any other jurisdiction to the extent not inconsistent with, or pre-empted by federal law.

2.212 COMPLIANCE WITH LAWS

Contractor shall comply with all applicable state, federal and local laws and ordinances in providing the Services/Deliverables.

2.213 JURISDICTION

Any dispute arising from the Contract must be resolved in the State of Michigan. With respect to any claim between the parties, Contractor consents to venue in Ingham County, Michigan, and irrevocably waives any objections it may have to the jurisdiction on the grounds of lack of personal jurisdiction of the court or the laying of venue of the court or on the basis of forum non conveniens or otherwise. Contractor agrees to appoint agents in the State of Michigan to receive service of process.

2.220 Limitation of Liability

2.221 LIMITATION OF LIABILITY

Neither the Contractor nor the State is liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages. This limitation of liability does not apply to claims for infringement of United States patent, copyright, trademark or trade secrets; to claims for personal injury or damage to property caused by the gross negligence or willful misconduct of the Contractor; to claims covered by other specific provisions of this Contract calling for liquidated damages; or to court costs or attorney’s fees awarded by a court in addition to damages after litigation based on this Contract.

The Contractor’s liability for damages to the State is limited to $4,500,000.00. The foregoing limitation of liability does not apply to claims for infringement of United States patent, copyright, trademarks or trade secrets; to claims for personal injury or damage to property caused by the gross negligence or willful misconduct of the Contractor; or to court costs or attorney’s fees awarded by a court in addition to damages after litigation based on this Contract.

The State's liability for damages to the Contractor is limited to the value of the Contract.

2.230 Disclosure Responsibilities

2.231 DISCLOSURE OF LITIGATION

Contractor must disclose any material criminal litigation, investigations or proceedings involving the Contractor (and each Subcontractor) or any of its officers or directors or any litigation, investigations or proceedings under the Sarbanes-Oxley Act. In addition, each Contractor (and each Subcontractor) must notify the State of any material civil litigation, arbitration or proceeding which arises during the term of the Contract and extensions, to which Contractor (or, to the extent Contractor is aware, any Subcontractor) is a party, and which involves: (i) disputes that might reasonably be expected to adversely affect the viability or financial stability of Contractor or any Subcontractor; or (ii) a claim or written allegation of fraud against Contractor or, to the extent Contractor is aware, any Subcontractor by a governmental or public entity arising out of their business dealings with governmental or public entities. The Contractor must disclose in writing to the Contract Administrator any litigation, investigation, arbitration or other proceeding (collectively, "Proceeding") within 30 days of its occurrence. Details of settlements that are prevented from disclosure by the terms of the settlement may be annotated. Information provided to the State from Contractor's publicly filed documents referencing its material litigation will be deemed to satisfy the requirements of this Section.

If any Proceeding disclosed to the State under this Section, or of which the State otherwise becomes aware, during the term of this Contract would cause a reasonable party to be concerned about:

(a) the ability of Contractor (or a Subcontractor) to continue to perform this Contract according to its terms and conditions, or

(b) whether Contractor (or a Subcontractor) in performing Services for the State is engaged in conduct which is similar in nature to conduct alleged in the Proceeding, which conduct would constitute a breach of this Contract or a violation of Michigan law, regulations or public policy, then the Contractor must provide the State all reasonable assurances requested by the State to demonstrate that:

(1) Contractor and its Subcontractors will be able to continue to perform this Contract and any Statements of Work according to its terms and conditions, and

(2) Contractor and its Subcontractors have not and will not engage in conduct in performing the Services which is similar in nature to the conduct alleged in the Proceeding.

(c) Contractor must make the following notifications in writing:

(1) Within 30 days of Contractor becoming aware that a change in its ownership or officers has occurred, or is certain to occur, or a change that could result in changes in the valuation of its capitalized assets in the accounting records, Contractor must notify DTMB Purchasing Operations.

(2) Contractor must also notify DTMB Purchasing Operations within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership or officers.

(3) Contractor must also notify DTMB Purchase Operations within 30 days whenever changes to company affiliations occur.

2.232 RESERVED

2.233 BANKRUPTCY

The State may, without prejudice to any other right or remedy, terminate this Contract, in whole or in part, and, at its option, may take possession of the "Work in Process" and finish the Works in Process by whatever appropriate method the State may deem expedient if:

(a) the Contractor files for protection under the bankruptcy laws;

(b) an involuntary petition is filed against the Contractor and not removed within 30 days;

(c the Contractor becomes insolvent or if a receiver is appointed due to the Contractor's insolvency;

(d) the Contractor makes a general assignment for the benefit of creditors; or

(e) the Contractor or its affiliates are unable to provide reasonable assurances that the Contractor or its affiliates can deliver the services under this Contract.

Contractor will fix appropriate notices or labels on the Work in Process to indicate ownership by the State. To the extent reasonably possible, materials and Work in Process must be stored separately from other stock and marked conspicuously with labels indicating ownership by the State.

2.240 Performance

2.241 TIME OF PERFORMANCE

(a) Contractor must use commercially reasonable efforts to provide the resources necessary to complete all Services and Deliverables according to the time schedules contained in the Statements of Work and other Exhibits governing the work, and with professional quality.

(b) Without limiting the generality of **Section 2.241,** Contractor must notify the State in a timely manner upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion of any Deliverables/Services on the scheduled due dates in the latest State-approved delivery schedule and must inform the State of the projected actual delivery date.

(c) If the Contractor believes that a delay in performance by the State has caused or will cause the Contractor to be unable to perform its obligations according to specified Contract time periods, the Contractor must notify the State in a timely manner and must use commercially reasonable efforts to perform its obligations according to the Contract time periods notwithstanding the State's failure. Contractor will not be in default for a delay in performance to the extent the delay is caused by the State.

2.242 SERVICE LEVEL AGREEMENT (SLA)

(a) SLAs will be completed with the following operational considerations:

(1) SLAs will not be calculated for individual Incidents where any event of Excusable Failure has been determined; Incident means any interruption in Services.

(2) SLAs will not be calculated for individual Incidents where loss of service is planned and where the State has received prior notification or coordination.

(3) SLAs will not apply if the applicable Incident could have been prevented through planning proposed by Contractor and not implemented at the request of the State. To invoke this consideration, complete documentation relevant to the denied planning proposal must be presented to substantiate the proposal.

(4) Time period measurements will be based on the time Incidents are received by the Contractor and the time that the State receives notification of resolution based on 24x7x365 time period, except that the time period measurement will be suspended based on the following:

(i) Time period(s) will not apply where Contractor does not have access to a physical State Location and where access to the State Location is necessary for problem identification and resolution.

(ii) Time period(s) will not apply where Contractor needs to obtain timely and accurate information or appropriate feedback and is unable to obtain timely and accurate information or appropriate feedback from the State.

(b) Chronic Failure for any Service(s) will be defined as three unscheduled outage(s) or interruption(s) on any individual Service for the same reason or cause or if the same reason or cause was reasonably discoverable in the first instance over a rolling 30 day period. Chronic Failure will result in the State's option to terminate the effected individual Service(s) and procure them from a different Contractor for the chronic location(s) with Contractor to pay the difference in charges for up to three additional months. The termination of the Service will not affect any tiered pricing levels.

(c) Root Cause Analysis will be performed on any Business Critical outage(s) or outage(s) on Services when requested by the Contract Administrator. Contractor will provide its analysis within two weeks of outage(s) and provide a recommendation for resolution.

(d) All decimals must be rounded to two decimal places with five and greater rounding up and four and less rounding down unless otherwise specified.

See Article 1, Appendices M and N

2.243 LIQUIDATED DAMAGES

The parties acknowledge that late or improper processing of payments as described in Article 1, Statement of Work (SOW) will cause loss and damage to the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result. Therefore, Contractor and the State agree that if there is late or improper processing of payments as described in the SOW and the State does not elect to exercise its rights under **Section 2.141**, the State is entitled to collect liquidated damages for each occurrence in the amount of up to $5,000.00 and an additional $100.00 per day for each day Contractor fails to remedy the late or improper processing of payments as described in the SOW, subject to section 2.221 Limitation of Liability.

No liquidated damages will be charged for late or improper processing of payments that results in monetary assessments being assessed in accordance with the Service Level Agreements described in Article 1, Appendix M, Downtime or Article 1, Appendix N, System Response Time.

2.244 EXCUSABLE FAILURE

Neither party will be liable for any default, damage or delay in the performance of its obligations under the Contract to the extent the default, damage or delay is caused by government regulations or requirements (executive, legislative, judicial, military or otherwise), power failure, electrical surges or current fluctuations, lightning, earthquake, war, water or other forces of nature or acts of God, delays or failures of transportation, equipment shortages, suppliers' failures, or acts or omissions of common carriers, fire; riots, civil disorders; strikes or other labor disputes, embargoes; injunctions (provided the injunction was not issued as a result of any fault or negligence of the party seeking to have its default or delay excused); or any other cause beyond the reasonable control of a party; provided the non-performing party and its Subcontractors are without fault in causing the default or delay, and the default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of alternate sources, workaround plans or other means, including disaster recovery plans.

If a party does not perform its contractual obligations for any of the reasons listed above, the non-performing party will be excused from any further performance of its affected obligation(s) for as long as the circumstances prevail. But the party must use commercially reasonable efforts to recommence performance whenever and to whatever extent possible without delay. A party must promptly notify the other party in writing immediately after the excusable failure occurs, and also when it abates or ends.

If any of the above-enumerated circumstances substantially prevent, hinder, or delay the Contractor's performance of the Services/provision of Deliverables for more than 10 Business Days, and the State determines that performance is not likely to be resumed within a period of time that is satisfactory to the State in its reasonable discretion, then at the State's option: (a) the State may procure the affected Services/Deliverables from an alternate source, and the State is not be liable for payment for the unperformed Services/ Deliverables not provided under the Contract for so long as the delay in performance continues; (b) the State may terminate any portion of the Contract so affected and the charges payable will be equitably adjusted to reflect those Services/Deliverables terminated; or (c) the State may terminate the affected Statement of Work without liability to Contractor as of a date specified by the State in a written notice of termination to the Contractor, except to the extent that the State must pay for Services/Deliverables provided through the date of termination.

The Contractor will not have the right to any additional payments from the State as a result of any Excusable Failure occurrence or to payments for Services not rendered/Deliverables not provided as a result of the Excusable Failure condition. Defaults or delays in performance by Contractor which are caused by acts or omissions of its Subcontractors will not relieve Contractor of its obligations under the Contract except to the extent that a Subcontractor is itself subject to an Excusable Failure condition described above and Contractor cannot reasonably circumvent the effect of the Subcontractor's default or delay in performance through the use of alternate sources, workaround plans or other means.

2.250 Approval of Deliverables

2.251 DELIVERY OF DELIVERABLES

A list of the Deliverables to be prepared and delivered by Contractor including, for each Deliverable, the scheduled delivery date and a designation of whether the Deliverable is a document ("Written Deliverable") or a Custom Software Deliverable is attached, if applicable. All Deliverables shall be completed and delivered for State review and written approval and, where applicable, installed in accordance with the State-approved delivery schedule and any other applicable terms and conditions of this Contract.

Prior to delivering any Deliverable to the State, Contractor will first perform all required quality assurance activities, and, in the case of Custom Software Deliverables, System Testing to verify that the Deliverable is complete and in conformance with its specifications. Before delivering a Deliverable to the State, Contractor shall certify to the State that (1) it has performed such quality assurance activities, (2) it has performed any applicable testing, (3) it has corrected all material deficiencies discovered during such quality assurance activities and testing, (4) the Deliverable is in a suitable state of readiness for the State's review and approval, and (5) the Deliverable/Service has all Critical Security patches/updates applied.

2.252 CONTRACTOR SYSTEM TESTING

Contractor will be responsible for System Testing each Custom Software Deliverable in Contractor's development environment prior to turning over the Custom Software Deliverable to the State for User Acceptance Testing and approval. Contractor's System Testing shall include the following, at a minimum, plus any other testing required by CMM Level 3 or Contractor's system development methodology:

Contractor will be responsible for performing Unit Testing and incremental Integration Testing of the components of each Custom Software Deliverable.

Contractor's System Testing will also include Integration Testing of each Custom Software Deliverable to ensure proper inter-operation with all prior software Deliverables, interfaces and other components that are intended to inter-operate with such Custom Software Deliverable, and will include Regression Testing, volume and stress testing to ensure that the Custom Software Deliverables are able to meet the State's projected growth in the number and size of transactions to be processed by the Application and number of users, as such projections are set forth in the applicable Statement of Work.

Contractor's System Testing will also include Business Function Testing and Technical Testing of each Application in a simulated production environment. Business Function Testing will include testing of full work streams that flow through the Application as the Application will be incorporated within the State's computing environment. The State shall participate in and provide support for the Business Function Testing to the extent reasonably requested by Contractor. Within ten (10) days before the commencement of Business Function Testing pursuant to this Section, Contractor shall provide the State for State review and written approval Contractor's test plan for Business Function Testing.

Within five (5) Business Days following the completion of System Testing pursuant to this **Section**, Contractor shall provide to the State a testing matrix establishing that testing for each condition identified in the System Testing plans has been conducted and successfully concluded. To the extent that testing occurs on State premises, the State shall be entitled to observe or otherwise participate in testing under this Section as the State may elect.

2.253 APPROVAL OF DELIVERABLES, IN GENERAL

All Deliverables (Written Deliverables and Custom Software Deliverables) require formal written approval by the State, in accordance with the following procedures. Formal approval by the State requires that the Deliverable be confirmed in writing by the State to meet its specifications, which, in the case of Custom Software Deliverables, will include the successful completion of State User Acceptance Testing, to be led by the State with the support and assistance of Contractor. The parties acknowledge that the approval process set forth herein will be facilitated by ongoing consultation between the parties, visibility of interim and intermediate Deliverables and collaboration on key decisions.

The State's obligation to comply with any State Review Period is conditioned on the timely delivery of Deliverables being reviewed. If Contractor fails to provide a Deliverable to the State in a timely manner, the State will nevertheless use commercially reasonable efforts to complete its review or testing within the applicable State Review Period.

Before commencement of its review or testing of a Deliverable, the State may inspect the Deliverable to confirm that all components of the Deliverable (e.g., software, associated documentation, and other materials) have been delivered. If the State determines that the Deliverable is incomplete, the State may refuse delivery of the Deliverable without performing any further inspection or testing of the Deliverable. Otherwise, the review period will be deemed to have started on the day the State receives the Deliverable and the applicable certification by Contractor in accordance with this Section.

The State will approve in writing a Deliverable upon confirming that it conforms to and, in the case of a Custom Software Deliverable, performs in accordance with, its specifications without material deficiency. The State may, but shall not be required to, conditionally approve in writing a Deliverable that contains material deficiencies if the State elects to permit Contractor to rectify them post-approval. In any case, Contractor will be responsible for working diligently to correct within a reasonable time at Contractor's expense all deficiencies in the Deliverable that remain outstanding at the time of State approval.

If, after three (3) opportunities (the original and two repeat efforts), Contractor is unable to correct all deficiencies preventing State approval of a Deliverable, the State may: (i) demand that Contractor cure the failure and give Contractor additional time to cure the failure at the sole expense of Contractor; or (ii) keep this Contract in force and do, either itself or through other parties, whatever Contractor has failed to do, in which event Contractor shall bear any excess expenditure incurred by the State in so doing beyond the contract price for such Deliverable and will pay the State an additional sum equal to ten percent (10%) of such excess expenditure to cover the State's general expenses without the need to furnish proof in substantiation of such general expenses; or (iii) terminate this Contract for default, either in whole or in part by notice to Contractor (and without the need to afford Contractor any further opportunity to cure). Notwithstanding the foregoing, the State shall not use, as a basis for exercising its termination rights under this Section, deficiencies discovered in a repeat State Review Period that could reasonably have been discovered during a prior State Review Period.

The State, at any time and in its own discretion, may halt the UAT or approval process if such process reveals deficiencies in or problems with a Deliverable in a sufficient quantity or of a sufficient severity as to make the continuation of such process unproductive or unworkable. In such case, the State may return the applicable Deliverable to Contractor for correction and re-delivery prior to resuming the review or UAT process and, in that event, Contractor will correct the deficiencies in such Deliverable in accordance with the Contract, as the case may be.

Approval in writing of a Deliverable by the State shall be provisional; that is, such approval shall not preclude the State from later identifying deficiencies in, and declining to accept, a subsequent Deliverable based on or which incorporates or inter-operates with an approved Deliverable, to the extent that the results of subsequent review or testing indicate the existence of deficiencies in the subsequent Deliverable, or if the Application of which the subsequent Deliverable is a component otherwise fails to be accepted pursuant to **Section 2.080**.

2.254 PROCESS FOR APPROVAL OF WRITTEN DELIVERABLES

The State Review Period for Written Deliverables will be the number of days set forth in the applicable Statement of Work following delivery of the final version of the Written Deliverable (failing which the State Review Period, by default, shall be five (5) Business Days for Written Deliverables of one hundred (100) pages or less and ten (10) Business Days for Written Deliverables of more than one hundred (100) pages). The duration of the State Review Periods will be doubled if the State has not had an opportunity to review an interim draft of the Written Deliverable prior to its submission to the State. The State agrees to notify Contractor in writing by the end of the State Review Period either stating that the Written Deliverable is approved in the form delivered by Contractor or describing any deficiencies that must be corrected prior to approval of the Written Deliverable (or at the State's election, subsequent to approval of the Written Deliverable). If the State delivers to Contractor a notice of deficiencies, Contractor will correct the described deficiencies and within five (5) Business Days resubmit the Deliverable in a form that shows all revisions made to the original version delivered to the State. Contractor's correction efforts will be made at no additional charge. Upon receipt of a corrected Written Deliverable from Contractor, the State will have a reasonable additional period of time, not to exceed the length of the original State Review Period, to review the corrected Written Deliverable to confirm that the identified deficiencies have been corrected.

2.255 PROCESS FOR APPROVAL OF CUSTOM SOFTWARE DELIVERABLES

The State will conduct UAT of each Custom Software Deliverable in accordance with the following procedures to determine whether it meets the criteria for State approval – i.e., whether it conforms to and performs in accordance with its specifications without material deficiencies.

Within thirty (30) days (or such other number of days as the parties may agree to in writing) prior to Contractor's delivery of any Custom Software Deliverable to the State for approval, Contractor shall provide to the State a set of proposed test plans, including test cases, scripts, data and expected outcomes, for the State's use (which the State may supplement in its own discretion) in conducting UAT of the Custom Software Deliverable. Contractor, upon request by the State, shall provide the State with reasonable assistance and support during the UAT process.

For the Custom Software Deliverables listed in an attachment, the State Review Period for conducting UAT will be as indicated in the attachment. For any other Custom Software Deliverables not listed in an attachment, the State Review Period shall be the number of days agreed in writing by the parties (failing which it shall be forty-five (45) days by default). The State Review Period for each Custom Software Deliverable will begin when Contractor has delivered the Custom Software Deliverable to the State accompanied by the certification required by this **Section** and the State's inspection of the Deliverable has confirmed that all components of it have been delivered.

The State's UAT will consist of executing test scripts from the proposed testing submitted by Contractor, but may also include any additional testing deemed appropriate by the State. If the State determines during the UAT that the Custom Software Deliverable contains any deficiencies, the State will notify Contractor of the deficiency by making an entry in an incident reporting system available to both Contractor and the State. Contractor will modify promptly the Custom Software Deliverable to correct the reported deficiencies, conduct appropriate System Testing (including, where applicable, Regression Testing) to confirm the proper correction of the deficiencies and re-deliver the corrected version to the State for re-testing in UAT. Contractor will coordinate the re-delivery of corrected versions of Custom Software Deliverables with the State so as not to disrupt the State's UAT process. The State will promptly re-test the corrected version of the Software Deliverable after receiving it from Contractor.

Within three (3) business days after the end of the State Review Period, the State will give Contractor a written notice indicating the State's approval or rejection of the Custom Software Deliverable according to the criteria and process set out in this **Section**.

2.256 FINAL ACCEPTANCE

"Final Acceptance" shall be considered to occur when the Custom Software Deliverable to be delivered has been approved by the State and has been operating in production without any material deficiency for fourteen (14) consecutive days. If the State elects to defer putting a Custom Software Deliverable into live production for its own reasons, not based on concerns about outstanding material deficiencies in the Deliverable, the State shall nevertheless grant Final Acceptance of the Project.

2.260 Ownership

A. Except as otherwise set forth in this Section, as between Contractor and the State, Contractor owns all right, title, and interest in and to any inventions (patentable or otherwise), discoveries, improvements or copyrightable works (collectively, "New Intellectual Property") that Contractor creates in connection with its performance of services hereunder as well as the Contractor's system and all of Contractor's pre-existing (prior to the effective date) proprietary information ("Pre-existing Intellectual Property"), methodologies, software, materials, concepts, or project tools ("Methodologies") used by Contractor to create the New Intellectual Property. The State shall provide all reasonable assistance requested by Contractor in its protection of the Intellectual Property. The term "Intellectual Property" shall mean and include Contractor's Pre-existing Intellectual Property, New Intellectual Property, Methodologies and the Contractor's system.

B. Notwithstanding Contractor's ownership of the Intellectual Property, the State retains ownership of any and all of its pre-existing (prior to the effective date) intellectual property rights, and any third-party which has provided software products to the State retains all rights in its software products.

C. Effective upon completion of the services and payment by the State of the corresponding fees, Contractor hereby grants to the State a limited, non-exclusive, non-transferable, non-assignable license to use the Contractor's system on the equipment specified in this Contract and related end-user materials in machinereadable form for internal use only. The State shall not decompile, reverse assemble or otherwise reverse engineer the Contractor's system or use the contractor's system for third party transactions, commercial time-sharing or service bureau use.

D. Notwithstanding Section C above, the States rights in and obligations with respect to any Third-Party Software, whether or not obtained with the assistance of Contractor, shall be determined in accordance with the agreements between such software vendors and the State. The State agrees to be bound by the terms and restrictions of any software license included with any Third-Party Software and to execute a required end-user agreement with the execution of this Contract.

E. Use of Marks and Publicity. Neither party will use any trademark, service mark, trade name nor other proprietary designation (collectively, "Marks") owned, licensed or registered by the other party without prior written consent; provided, however, Contractor may use the State's name in publicity indicating that the State and Contractor have entered into a contractual relationship, as well as customer lists or other advertising identifying the customers of the Contractor. Neither party will use or reference the other's Marks in any manner that disparages or portrays the other in a negative light. Neither party may alter, modify, or change the other's Marks in any way. A breach of the terms of this Contract related to the use of a party's Marks will cause irreparable harm such that the non-breaching party will not have an adequate remedy at law and, in addition to any other rights or remedies available at law or in equity, will be entitled to seek injunctive relief against the breaching party (without posting a bond or other security).

F. Patent Acknowledgements and Disclaimers. .The State acknowledges that it has been informed that the Contractor's affiliates own, control or license from third parties, certain patents or patent applications ("Contractor IP"), which may apply to the service that Contractor provides the State, including without limitation, the patent applications and patents owned or controlled by Ronald A. Katz Technology Licensing L.P. ("RAKTL"), and licensed to Contractor's affiliates ("RAKTL Patents"). If Contractor performs or provides the State with each and every element, step or component of an allegedly infringing combination, system or process, the Contractor IP will cover the State with regard to the owned patents or patent application, the RAKTL Patents, and certain other licensed patents and patent applications for that combination, system or process. The State acknowledges and agrees that with regard to all other combinations, systems or processes or portions of combinations, systems or processes assembled, used, operated or offered by the State ("Other Combinations") which may use, incorporate or implicate one or more of the services that Contractor provides the State, the Contractor IP may not cover the State, including without limitation, with respect to the RAKTL Patents. Notwithstanding any provision in this Contract to the contrary, Contractor shall not be obligated to indemnify the State with respect to any claims concerning Other Combinations. The State will need to separately evaluate their position with regard to third party rights concerning Other Combinations. Except as expressly provided above, the State acknowledges and agrees that it does not obtain any implied license or other rights under the Contractor IP, including without limitation, with regard to the RAKTL Patents, and Contractor and its affiliates hereby expressly disclaim any such implied license or other rights. For the avoidance of doubt, the State acknowledges that it has been informed that an affiliate of Contractor has a limited, minority, non-controlling, equity interest in RAKTL.

G. The State is the owner of all data made available by the State to the Contractor or its agents, Subcontractors or representatives under the Contract. The Contractor will not use the State's data for any purpose other than providing the Services, nor will any part of the State's data be disclosed, sold, assigned, leased or otherwise disposed of to the general public or to specific third parties or commercially exploited by or on behalf of the Contractor. No employees of the Contractor, other than those on a strictly need-to-know basis, have access to the State's data. Contractor will not possess or assert any lien or other right against the State's data. Without limiting the generality of this Section, the Contractor must only use personally identifiable information as strictly necessary to provide the Services and must disclose the information only to its employees who have a strict need-to-know the information. The Contractor must comply at all times with all laws and regulations applicable to the personally identifiable information.

H. The Contractor is the owner of all data made available by the Contractor to the State under this Contract. The State will not use the Contractor's data for any purpose other than those set forth under this Contract, nor will any part of the Contractors's data be disclosed, sold, assigned, leased or otherwise disposed of to the general public or to specific third parties or commercially exploited by or on behalf of the Steve. No employees of the State, other than those on a strictly need-to-know basis, have access to the Contractor's data. The State will not possess or assert any lien or other right against the Contractor's data. The State must comply at all times with all laws and regulations applicable to the personally identifiable information.

2.270 State Standards

2.271 EXISTING TECHNOLOGY STANDARDS

Contractor shall abide by all State of Michigan applicable laws and regulations. Contractor shall maintain and implement written policies and procedures regarding data privacy and data security, including but not limited to the safeguarding of customer data designed to comply with the Federal Interagency Guidelines Establishing Information Security Standards. The Contractor's officers and employees are bound by the policies and procedures of Contractor.

2.272 ACCEPTABLE USE POLICY

To the extent that Contractor has access to the State computer system, Contractor must comply with the State's Acceptable Use Policy, see http://www.michigan.gov/ditservice. All Contractor employees will comply with the State's Acceptable Use Policy before accessing the State system. The State reserves the right to terminate Contractor's access to the State system if a violation occurs.

2.273 SYSTEMS CHANGES

Contractor is not responsible for and not authorized to make changes to any State systems without written authorization from the Project Manager. Any changes Contractor makes to State systems with the State's approval must be done according to applicable State procedures, including security, access and configuration management procedures.

2.280 Extended Purchasing

2.281 RESERVED

2.282 STATE EMPLOYEE PURCHASES

Reserved.

2.290 Environmental Provision

2.291 ENVIRONMENTAL PROVISION

Energy Efficiency Purchasing Policy: The State seeks wherever possible to purchase energy efficient products. This includes giving preference to U.S. Environmental Protection Agency (EPA) certified 'Energy Star' products for any category of products for which EPA has established Energy Star certification. For other purchases, the State may include energy efficiency as one of the priority factors to consider when choosing among comparable products.

Environmental Purchasing Policy: The State of Michigan is committed to encouraging the use of products and services that impact the environment less than competing products. The State is accomplishing this by including environmental considerations in purchasing decisions, while remaining fiscally responsible, to promote practices that improve worker health, conserve natural resources, and prevent pollution. Environmental components that are to be considered include: recycled content and recyclables; energy efficiency; and the presence of undesirable materials in the products, especially those toxic chemicals which are persistent and bioaccumulative. The Contractor should be able to supply products containing recycled and environmentally preferable materials that meet performance requirements and is encouraged to offer such products throughout the duration of this Contract. Information on any relevant third party certification (such as Green Seal, Energy Star, etc.) should also be provided.

Hazardous Materials: For the purposes of this Section, "Hazardous Materials" is a generic term used to describe asbestos, ACBMs, PCBs, petroleum products, construction materials including paint thinners, solvents, gasoline, oil, and any other material the manufacture, use, treatment, storage, transportation or disposal of which is regulated by the federal, state or local laws governing the protection of the public health, natural resources or the environment. This includes, but is not limited to, materials the as batteries and circuit packs, and other materials that are regulated as (1) "Hazardous Materials" under the Hazardous Materials Transportation Act, (2) "chemical hazards" under the Occupational Safety and Health Administration standards, (3) "chemical substances or mixtures" under the Toxic Substances Control Act, (4) "pesticides" under the Federal Insecticide Fungicide and Rodenticide Act, and (5) "hazardous wastes" as defined or listed under the Resource Conservation and Recovery Act.

(a) The Contractor must use, handle, store, dispose of, process, transport and transfer any material considered a Hazardous Material according to all federal, State and local laws. The State must provide a safe and suitable environment for performance of Contractor's Work. Before the commencement of Work, the State must advise the Contractor of the presence at the work site of any Hazardous Material to the extent that the State is aware of the Hazardous Material. If the Contractor encounters material reasonably believed to be a Hazardous Material and which may present a substantial danger, the Contractor must immediately stop all affected Work, notify the State in writing about the conditions encountered, and take appropriate health and safety precautions.

(b) Upon receipt of a written notice, the State will investigate the conditions. If (a) the material is a Hazardous Material that may present a substantial danger, and (b) the Hazardous Material was not brought to the site by the Contractor, or does not result in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Materials, the State must order a suspension of Work in writing. The State must proceed to have the Hazardous Material removed or rendered harmless. In the alternative, the State must terminate the affected Work for the State's convenience.

(c) Once the Hazardous Material has been removed or rendered harmless by the State, the Contractor must resume Work as directed in writing by the State. Any determination by the Michigan Department of Community Health or the Michigan Department of Environmental Quality that the Hazardous Material has either been removed or rendered harmless is binding upon the State and Contractor for the purposes of resuming the Work. If any incident with Hazardous Material results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Work will not be counted in a time as mutually agreed by the parties.

(d) If the Hazardous Material was brought to the site by the Contractor, or results in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Material, or from any other act or omission within the control of the Contractor, the Contractor must bear its proportionate share of the delay and costs involved in cleaning up the site and removing and rendering harmless the Hazardous Material according to Applicable Laws to the condition approved by applicable regulatory agency(ies).

Labeling: Michigan has a Consumer Products Rule pertaining to labeling of certain products containing volatile organic compounds. For specific details visit http://www.michigan.gov/deq/0,1607,7-135-3310_4108-173523--,00.html

Refrigeration and Air Conditioning: The Contractor shall comply with the applicable requirements of Sections 608 and 609 of the Clean Air Act (42 U.S.C. 7671g and 7671h) as each or both apply to this contract.

Environmental Performance: Waste Reduction Program - Contractor shall establish a program to promote cost-effective waste reduction in all operations and facilities covered by this contract. The Contractor's programs shall comply with applicable Federal, State, and local requirements, specifically including Section 6002 of the Resource Conservation and Recovery Act (42 U.S.C. 6962, et seq.).

2.300 Deliverables

2.301 SOFTWARE

A list of the items of software the State is required to purchase for execution the Contract is attached. The list includes all software required to complete the Contract and make the Deliverables operable; if any additional software is required in order for the Deliverables to meet the requirements of this Contract, such software shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Statement of Work or Contract Change Notice). The attachment also identifies certain items of software to be provided by the State.

2.302 HARDWARE

A list of the items of hardware the State is required to purchase for execution the Contract is attached. The list includes all hardware required to complete the Contract and make the Deliverables operable; if any additional hardware is required in order for the Deliverables to meet the requirements of this Contract, such hardware shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Contract Change Notice). The attachment also identifies certain items of hardware to be provided by the State.

2.303 EQUIPMENT TO BE NEW

If applicable, all equipment provided under this Contract by Contractor shall be new where Contractor has knowledge regarding whether the equipment is new or assembled from new or serviceable used parts that are like new in performance or has the option of selecting one or the other. Equipment that is assembled from new or serviceable used parts that are like new in performance is acceptable where Contractor does not have knowledge or the ability to select one or other, unless specifically agreed otherwise in writing by the State.

2.304 EQUIPMENT TO BE NEW AND PROHIBITED PRODUCTS

The State will not accept salvage, distressed, outdated or discontinued merchandise. Shipping of such merchandise to any State agency, as a result of an order placed against the Contract, shall be considered default by the Contractor of the terms and conditions of the Contract and may result in cancellation of the Contract by the State. The brand and product number offered for all items shall remain consistent for the term of the Contract, unless Purchasing Operations has approved a change order pursuant to **Section 2.024.**

2.310 Software Warranties

2.311 RESERVED

2.312 NO SURREPTITIOUS CODE WARRANTY

The Contractor represents and warrants that no copy of licensed Software provided to the State contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this Contract as the “No Surreptitious Code Warranty.”

As used in this Contract, “Self-Help Code” means any back door, time bomb, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee’s computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

As used in this Contract, “Unauthorized Code” means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code. Unauthorized Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee’s computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

In addition, Contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the State.

2.313 CALENDAR WARRANTY

The Contractor represents and warrants that all software for which the Contractor either sells or licenses to the State of Michigan and used by the State prior to, during or after the calendar year 2000, includes or shall include, at no added cost to the State, design and performance so the State shall not experience software abnormality and/or the generation of incorrect results from the software, due to date oriented processing, in the operation of the business of the State of Michigan.

The software design, to insure calendar year rollover compatibility, shall include, but is not limited to: data structures (databases, data files, etc.) that provide 4-digit date century; stored data that contain date century recognition, including, but not limited to, data stored in databases and hardware device internal system dates; calculations and program logic (e.g., sort algorithms, calendar generation, event recognition, and all processing actions that use or produce date values) that accommodates same century and multi-century formulas and date values; interfaces that supply data to and receive data from other systems or organizations that prevent non-compliant dates and data from entering any State system; user interfaces (i.e., screens, reports, etc.) that accurately show 4 digit years; and assurance that the year 2000 shall be correctly treated as a leap year within all calculation and calendar logic.

2.314 THIRD-PARTY SOFTWARE WARRANTY

The Contractor represents and warrants that it will disclose the use or incorporation of any third-party software into the Deliverables. At the time of Delivery, the Contractor shall provide in writing the name and use of any Third-party Software, including information regarding the Contractor's authorization to include and utilize such software. The notice shall include a copy of any ownership agreement or license that authorizes the Contractor to use the Third-party Software.

2.315 PHYSICAL MEDIA WARRANTY

Contractor represents and warrants that each licensed copy of the Software provided by the Contractor is free from physical defects in the media that tangibly embodies the copy. This warranty does not apply to defects discovered more than (30) thirty days after that date of Final Acceptance of the Software by the State. This warranty does not apply to defects arising from acts of Excusable Failure. If the Contractor breaches this warranty, then the State shall be entitled to replacement of the non-compliant copy by Contractor, at Contractor's expense (including shipping and handling).

2.320 Reserved

2.330 Reserved

2.400 Other Provisions

2.411 FORCED LABOR, CONVICT LABOR, OR INDENTURED SERVITUDE MADE MATERIALS

The contractor represents and certifies that, to the best of its knowledge and belief no foreign (outside of the U.S.) made equipment, materials, or supplies, will be furnished to the State under any resulting Contract, that have been produced in whole or in part by forced labor, convict labor, or indentured servitude.

_________ (Initial)

2.421 KNOWLEDGE OF CHILD LABOR FOR LISTED END PRODUCTS

(a) "Forced or indentured child labor" means all work or service:

(i) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(ii) Performed by any person under the age of 18 under a contract the enforcement of which can be accomplished by process or penalties.

(b) *Listed end products*. The following end product(s) being acquired under this solicitation is (are) included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, identified by their country of origin. There is a reasonable basis to believe that listed end products from the listed countries of origin may have been mined, produced, or manufactured by forced or indentured child labor.

Listed End Product	Listed Country of Origin

(c) *Certification*. The State will not make award to a Bidder unless the Bidder, by checking the appropriate block, certifies to one of the following:

( ) The Bidder will not supply any end product listed in paragraph (b) of this provision that was mined, produced, or manufactured in a corresponding country as listed for that end product.

( ) The Bidder may supply an end product listed in paragraph (b) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The Bidder certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture the end product. On the basis of those efforts, the Bidder certifies that it is not aware of any the use of child labor.

________ (Initial)

Appendix A
Pricing
(Excel Spreadsheet)

Article 1, Attachment A

Price Proposal

Bidders to complete the yellow highlighted fields

Table 1 - Transaction Fees (For Base Contract Term - 5 years)

Range of Monthly Transactions	Unit Fee	X Estimated Monthly Volume	Total Estimated Cost
0 - 150,000	$ 0.15	150,000	$ 22,500.00
150, 001 - 250,000	$ 0.14	250,000	$ 35,000.00
250,001 - 300,000	$ 0.13	300,000	$ 39,000.00
300,001 - 350,000	$ 0.13	350,000	$ 45,500.00
350,001 - 400,000	$ 0.12	400,000	$ 48,000.00
400,001 - 450,000	$ 0.11	450,000	$ 51,745.50
450,001 - 500,000	$ 0.10	500,000	$ 52,495.00
500,001 - 550,000	$ 0.10	550,000	$ 57,744.50
550,001 - 600,000	$ 0.09	600,000	$ 56,994.00
600,001 - 650,000	$ 0.09	650,000	$ 61,743.50
650,001 - 700,000	$ 0.08	700,000	$ 56,000.00
700,001 - 750,000	$ 0.08	750,000	$ 60,000.00
Total Volume and Cost for all Ranges		5,650,000	$ 586,722.50

Table 1 - Weighted Average (Monthly Cost)

Total Cost for all Ranges from Table 1	Divided by Total Estimated Monthly Volume from Table 1	Weighted Avg. Rate Per Item	Estimated Unit Fee Value Weighted Avg. x 350,000 Items x 60 months
$ 586,722.50	5,650,000	$ 0.10	$ 2,180,738.50

Table 2 - Bank of Hours for Customized Enhancements - 5 Year Cost

Rate per Hour	Number of Hours	Total Cost
$ 120.00	1,000	$ 120,000.00

Table 3 - Guaranteed ACH Debit Pricing - 5 Year Cost
(Choose one pricing method- Unknown if when/will use)

Pricing Method	Cost	Estimated Volume	Estimated Cost
Unit Fee **or**	$ -	25,000	$ -
Percentage (of Amount)	2.15%	$ 3,500,000	$ 75,250.00
		Total Cost	$ 75,250.00

Table 4 - Customizable Web & IVR Solution (Monthly Cost)			
Solution Component	**Cost**	**Est Monthly Volume**	**Estimated Cost**
Transaction Fee	$ 0.07	2,000	$ 140.00
Additional Fee - Authentication	$ -	200	$ -
Additional Fee - Registration	$ -	600	$ -
Additional Fee - IVR	$ 0.10	700	$ 70.00
		Total Cost	$ 210.00

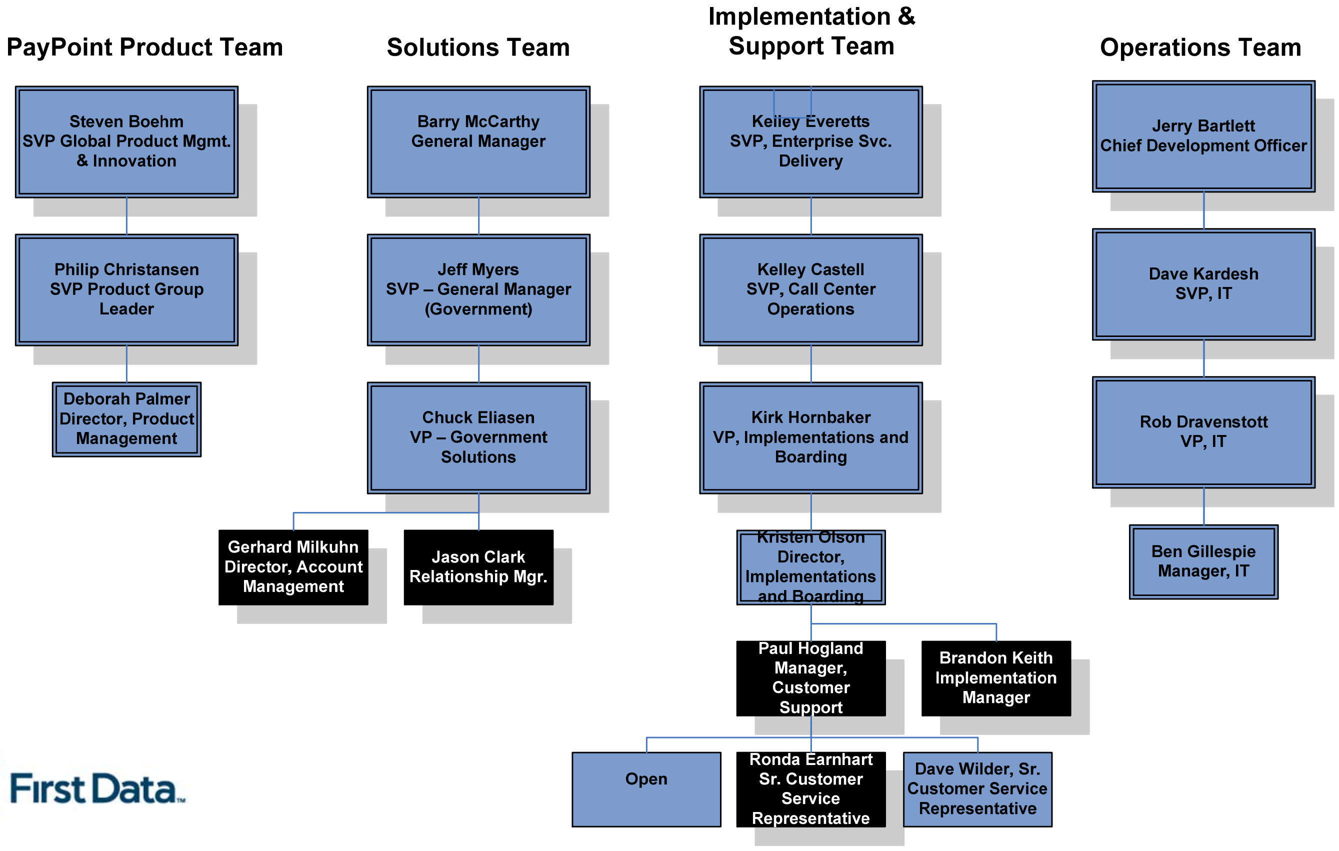
Table 5 - Bid Award Basis (Five Base Years)	
Table 1 - Estimated Unit fee value using weighted average	$ 2,180,738.50
Table 2 - Bank of Hours	$ 120,000.00
Table 3 - Estimated Guaranteed Cost	$ 75,250.00
Table 4 - Customizable Web & IVR Solution	$ 12,600.00
Total	$ 2,388,588.50

Table 6 - Estimated Contract Value (Five Base Years)			
Component	**Unit Fee**	**Estimated Volume/Use**	**Total Estimated Cost**
Per Item Fees - Year 1	$ 0.13	3,932,004	$ 511,160.52
Per Item Fees - Year 2	$ 0.12	4,325,204	$ 519,024.48
Per Item Fees - Year 3	$ 0.12	4,757,725	$ 570,927.00
Per Item Fees - Year 4	$ 0.11	5,233,497	$ 601,799.82
Per Item Fees - Year 5	$ 0.10	5,756,847	$ 604,411.37
Bank of Hours (5 year cost)	$ 120.00	1,000	$ 120,000.00
Guaranteed ACH Fees (5 year cost)	Total Cost from Table 3		$ 75,250.00
Customizable Web & IVR (5 year cost)	Total Cost from Table 4 x 60 Months		$ 12,600.00
Total Estimated Contract Value			**$ 3,015,173.19**

Appendix B
FDGS Organization Chart

Article 1, Attachment B,

First Data Organization Chart for Michigan CPAS



PayPoint Product Team

- Steven Boehm, SVP Global Product Mgmt. & Innovation
- Philip Christansen, SVP Product Group Leader
- Deborah Palmer, Director, Product Management

Solutions Team

- Barry McCarthy, General Manager
- Jeff Myers, SVP – General Manager (Government)
- Chuck Eliasen, VP – Government Solutions
- Gerhard Milkuhn, Director, Account Management
- Jason Clark, Relationship Mgr.

Implementation & Support Team

- Kelley Everetts, SVP, Enterprise Svc. Delivery
- Kelley Castell, SVP, Call Center Operations
- Kirk Hornbaker, VP, Implementations and Boarding
- Kristen Olson, Director, Implementations and Boarding
- Paul Hogland, Manager, Customer Support
- Brandon Keith, Implementation Manager
- Open
- Ronda Earnhart, Sr. Customer Service Representative
- Dave Wilder, Sr. Customer Service Representative

Operations Team

- Jerry Bartlett, Chief Development Officer
- Dave Kardesh, SVP, IT
- Rob Dravenstott, VP, IT
- Ben Gillespie, Manager, IT

First Data.

Appendix C
Key Entry Payment Screen Fields

Y = Required
O = Optional

Item Number	Business Data Item	Definition	Credit Card	ACH	API Response
1	Application Identifier	Assigned identifier to distinguish applications within the State enterprise. One State Agency may have many applications	Y	Y	
2	Payment Medium	The type of payment: Credit Card, ACH, or PINless Debit	Y	Y	
3	Payment Channel	The channel the payment is received through: Web, IVR, Walk in, Voice, Fax, Mail, Bulk	Y	Y	
4	Payer First Name	Payer's first name. ACH requires, but optional for credit card.	O	Y	
5	Payer Middle Initial	Middle initial of a payer.	O	O	
6	Payer Last Name	Last name of a payer. ACH requires, but optional for credit card.	O	Y	
7	Billing Address	The customer billing address.	O	O	
8	Payer Primary Phone Number	The primary phone number for a Payer.	O	O	
9	Payer Email Address	Payer's email address	O	O	
10	Shipping Address	The customer shipping address	O	O	
11	Payment Total Amount	The payment amount plus fees and other charges.	Y	Y	
12	Payment Tax Amount	The amount of tax in a transaction.	O	O	
13	Comments Field	A free form text field that may be used by an application to attach information specific to its operations. Especially useful as a payment feedback tool. Available for payment and registration transactions.	O	O	
14	Payment Date	Allows for post dating on ACH payments. Defaults to current date.		O	
15	Name On Account	Name on payer's bank account.		Y	
16	Name As It Appears On Card	Name that appears on payer's credit card.	Y		
17	Card Number	Credit card or debit card number.	Y		
18	Expiration Date	The expiration date of a card. Typically made of month and year.	Y		
19	Verification Code	The three or four digit verification code used by Visa (CVV2), MasterCard (CVC2), and American Express (CID). Typically on the back of cards.	O		
20	Swipe Card Button	Allows payer's credit to be swiped to auto fill card number, etc.	O		
21	Purchase Identifier	An identifier associated with a purchase by the State application.	O		
22	Bank Account Type	Savings or Checking. Used for ACH payments.		Y	
23	Bank Account Number	The Savings or Checking account used in an ACH transaction to satisfy the payment. (Truncated in Contractors system)		Y	
24	Bank Routing Number	The ACH routing number for the bank at which the Account Number resides.		Y	
25	Authorization Medium	Channel used by the payer to provide authorization for an		Y	

		ACH payment. Used to select appropriate SEC code.			
26	Bank Name	The name of the bank at which Bank Account Number resides.		O	
27	Bank State	The state where the bank resides.		O	
28	Drivers License Number	The payer's driver license number. (Truncated in Contractors system)		O	
29	Drivers License State	State where the drivers license is issued.		O	
30	Social Security Number	The payer's social security number. (Truncated in Contractors system)		O	
31	Business Name	Name of a registered business.		O	
32	Federal Tax Number	FEIN of a business.		O	
33	Confirmation Number	A unique identifier generated by the electronic payment vendor that is associated to successful payment and registration transactions.			Y
34	Result Message Text	A text string that describes the result of a call to the vendor's electronic payment engine.			Y
35	Return Code	A code value returned to the State application after a transaction with the vendor's electronic payment engine. The return code values are global within the set of defined transactions; for example, the code for "success" is always the same regardless of what transaction is used.			Y

Appendix D
API Data Requirements

Item Number	Business Data Item	Definition	API Required	API Optional	API Response
1	Application Identifier	Assigned identifier to distinguish applications within the State enterprise. One State Agency may have many applications	Yes		
2	Payment Channel	Describes the means used to make a payment. The State currently tracks IVR, web, walk-in, voice, fax, mail, scheduled, and unknown.	Yes		
3	Password	A unique password assigned to each application.	Yes		
4	Source Identification	Source identification of originating request. Often used to store IP addresses.		Yes	
5	Payment Method	Payment methods currently used are credit card, commercial credit card, ACH, Business ACH.	Yes		
6	Billing Address	The customer billing address.		Yes	
7	Shipping Address	The customer shipping address.		Yes	
8	Card Number	Credit card or debit card number.	Yes		
9	Credit Card Type	The brand of card used in a transaction. The State supports four types, Visa, MasterCard, American Express, and Discover.		Yes	Yes
10	Card Acquired Status	This tells how the card number is collected from the payer. The values are present, not present, and swiped.	Yes		
11	Verification Code	The three or four digit verification code used by Visa (CVV2), MasterCard (CVC2), and American Express (CID) and Discover (CID).		Yes	
12	E-commerce Goods	A flag that indicates if a transactions falls under the e-commerce goods specification as defined by the credit card associations.		Yes	
13	Expiration Date	The expiration date of a card.	Yes		
14	Purchase Identifier	An identifier associated with a purchase by the State application.		Yes	
15	Track Data	The data collected electronically when a card is swiped.		Yes	
16	User IP Address	The Internet Protocol address of the user submitting a request to the vendor's electronic payment product.		Yes	
17	Bank Account Type	Savings or Checking. Used for ACH payments.	Yes		
18	Bank Account Number	The Savings or Checking account used in ACH transactions to satisfy the payment.	Yes		
19	Bank Name	The name of the bank at which Bank Account Number resides.		Yes	
20	Bank Routing Number	The ACH routing number for the bank at which the Account Number resides.	Yes		
21	Bank State	The state where the bank resides.		Yes	
22	Drivers License Number	The payer's driver license number.		Yes	
23	Drivers License State	State where the drivers license is issued.		Yes	
24	Social Security Number	The payer's social security number.		Yes	
25	Pre-note Status	The status of an ACH pre-note performed for a enrolled account. The State tracks the values of unknown, success, created, failed, and waiting.		Yes	

26	Authorization Medium	Authorization Medium will contain the method by which the authorization was obtained. Values include Web, IVR, Walk in, Voice, Fax, and Mail. Used to determine the correct NACHA SEC code.	Yes		
27	Business Name	Name of a business customer.		Yes	
28	Federal Tax Number	FEIN of a business.		Yes	
29	Recurring Indicator	Used to indicate a single or recurring payment.		Yes	
30	Payer First Name	Payer's first name.	Yes		
31	Payer Full Name	Full name of a payer. May be required for address verification.	Yes		
32	Payer Last Name	Last name of a payer.	Yes		
33	Payer Middle Initial	Middle initial of a payer.		Yes	
34	Payer Primary Phone Number	The primary phone number for a Payer.		Yes	
35	Payer Secondary Phone Number	The secondary phone number for a Payer.		Yes	
36	Payer Email Address	Payer’s email address		Yes	
37	Payer Street Address Line One	First line in a payer’s address. May be required for credit card address verification.	Yes	Yes	
38	Payer Street Address Line Two	Second line in a payer’s address. May be required for credit card address verification.	Yes	Yes	
39	Payer City	City in which Street Address Line One resides. May be required for credit card address verification.	Yes		
40	Payer State	State in which Payer City resides. May be required for credit card address verification.	Yes	Yes	
41	Payer Zip Code	Zip code in which payer address resides. May be required for credit card address verification.	Yes	Yes	
42	Country Code	Default to US. Required for international addresses.	Yes	Yes	
43	Convenience Fee	A fee that is added to the sale amount for providing a convenience to the customer.		Yes	
44	Registration Identifier	A unique number assigned to a registered account. Assignment made by the Contractor system.		Yes	
45	Group Identifier	A State Agency may use this to group payments by application.		Yes	
46	Payment Amount	Dollars and cents of a payment.	Yes		
47	Comments Field	A free-form text field that may be used by an application to attach information specific to its operations. Especially useful as a payment feedback tool. Available for all payments and enrolled transactions.		Yes	
48	Payment Date	Allows for post dating of ACH payments.		Yes	
49	Payment Tax Amount	The amount of tax in a commercial credit card transaction.		Yes	
50	Confirmation Number	A unique identifier generated by the electronic payment Contractor that is associated to all payments (declined or approved) and enrolled transactions.			Yes
51	Result Message Text	A text string that describes the result of a call to the Contractor's electronic payment engine.			Yes

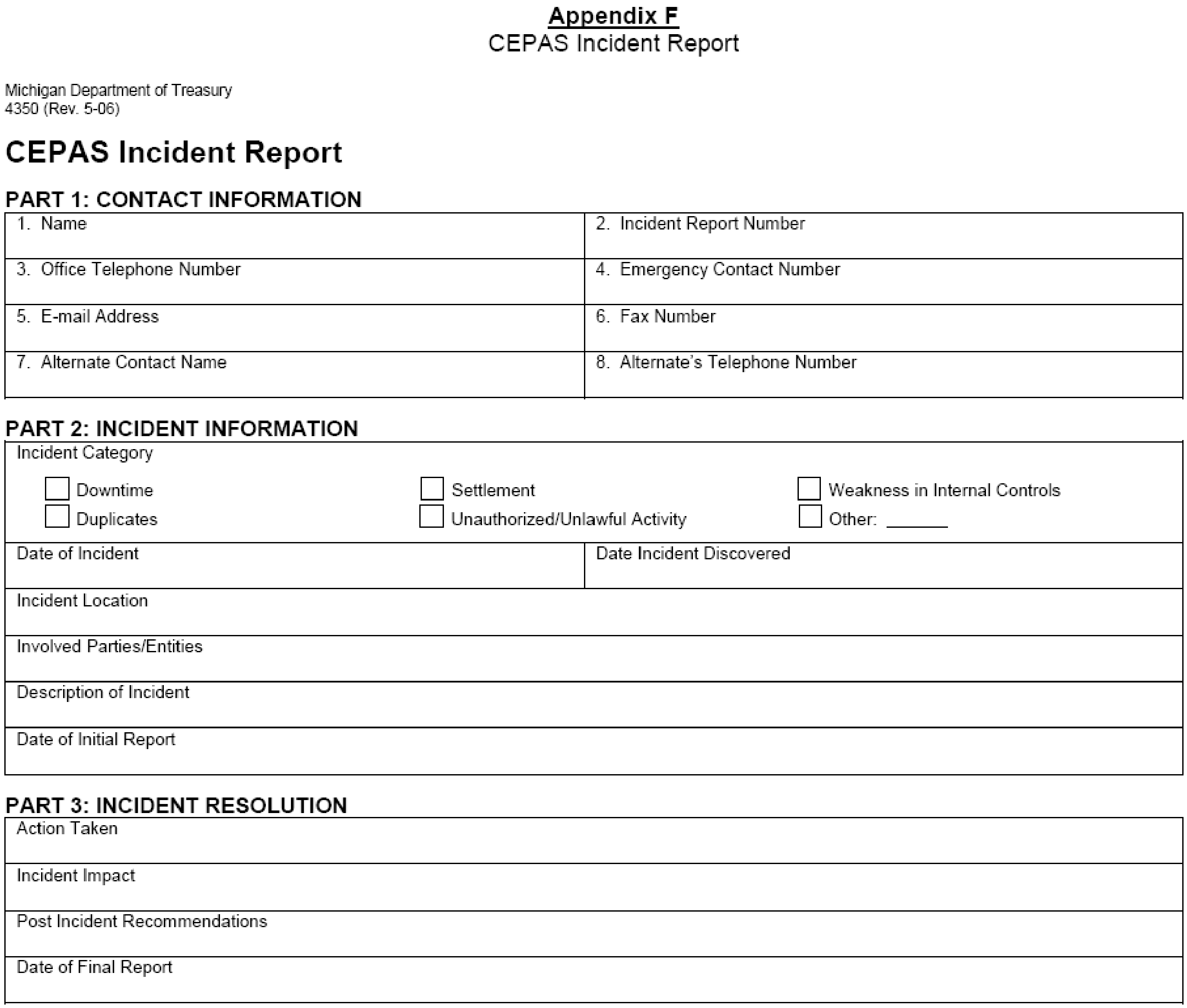
52	Return Code	A code value returned to the State application after a transaction with the Contractor's electronic payment engine. The return code values are global within the set of defined transactions; for example, the code for "approved" is always the same regardless of what transaction is used.			Yes
53	Settlement Date	The date the Contractor will submit a payment or refund for settlement.			Yes
54	Payment Total Amount	The payment amount plus fees and other charges.			Yes
55	Credit Card Authorization Code	When a successful credit card payment is made, this is the unique authorization number generated by the credit card processor.			Yes
56	Refund Request Amount	An amount of payment money that will be refunded to a payer. Associated to a specific transaction, it must be less than or equal to the original payment amount. (See Payment Amount)	Yes		
57	Convenience Fee Refund Amount	An amount of convenience fee money that will be refunded to a payer. Associated to a specific transaction, it must be less than or equal to the original convenience fee amount. (See Convenience Fee)	Yes		
58	Registration Action	The registration action request to the Contractor electronic engine. Values must include Create, Update, and Delete	Yes		
59	Registration Terms Agreed To	An indicator that the enrollee has agreed to the terms of account registration.	Yes		
60	Look up Reference	Applicable to Create and Update only. Used to reference one or more registrations to a single unique identifier.		Yes	
61	Scheduled Payment Action	The scheduled payment action request to the vendor electronic engine. Values must include Create, Update, and Delete	Yes		
62	Scheduled Payment Identifier	Unique identifier returned to the requesting application when a successful create action is executed.			Yes
63	Scheduled Payment Begin Date	The date on which the first scheduled payment begins. Required to define a scheduled payment.	Yes		
64	Scheduled Payment End Date	The end date of a scheduled payment definition. Required to define a scheduled payment.	Yes		
65	Scheduled Payment Next Payment Date	The date on which the next scheduled payment is scheduled.	Yes		Yes
66	Disabled Date	Used to define the date a scheduled payment is disabled.		Yes	
67	Scheduled Payment Interval	A code value to define the interval at which a scheduled payment is scheduled. The State currently supports daily, monthly and yearly intervals.	Yes		
68	Scheduled Payment Interval Parameters	The State supports a series of three parameters to arrange payment schedules for payers.	Yes		
69	Payment Status	A code returned on a payment inquiry transaction that describes the status of a payment within the Contractor system, such as "approved" or "declined".			Yes

Appendix E
Feedback File Data Elements

Item Number	Feedback File Data Item	Definition
1	Site Identifier	A unique identifier assigned by the Contractor that identifies the State enterprise.
2	State Entity	A unique identifier assigned by the Contractor that identifies an Agency within the State enterprise.
3	State Entity Application	A unique identifier assigned by the Contractor that identifies an Application within an Agency.
4	Payment Method	The State currently supports the type credit card, debit card, and Debit ACH.
5	Payment Identifier	A unique identifier assigned by the Contractor that identifies a payment.
6	Transaction Date-Time	The date and time of a transaction.
7	Payment Code	A code that describes the specific kind of payment being made. The State supports primary payment, convenience fee, chargeback, prenote, and chargeback convenience fee.
8	Payment Command	A code that describes the action being performed. Actions must include payment, refund, partial refund, void, ACH return reason codes, chargeback, and chargeback reversal.
9	Payment Amount	The dollar amount of the transaction.
10	Confirmation Number	A unique identifier generated by the electronic payment Contractor that is associated to all payments and enrolled transactions.
11	Authorization Code	6 character authorization code when a credit card transaction has been approved.
12	Enrolled Identifier	A unique number assigned to a registered account. Assignment made by the Contractor system.
13	Scheduled Payment Identifier	A unique identifier assigned by the Contractor that identifies a scheduled payment arrangement stored in the enrolled database of the Contractor.
14	Credit Card Type	The brand of card used in a transaction. The file must support: Visa, MasterCard, American Express, Discover, and PINless and PIN-based debit.
15	Bank Routing Number	The ACH routing number for the bank at which the Account Number resides.
16	Account Number	The last 4 digits of the Savings or Checking account used in an ACH transaction to satisfy the payment or the last 4 digits of the credit card number.
17	Payer First Name	Payer's first name.
18	Payer Middle Initial	Middle initial of a payer.
19	Payer Last Name	Last name of a payer.
20	Payer Full Name	Full name of a payer. May be required for address verification.
21	Payer Email Address	Payer's email address
22	Payer Street Address Line One	First line in a payer's address. May be required for credit card address verification.
23	Payer Street Address Line Two	Second line in a payer's address. May be required for credit card address verification.
24	Payer City	City in which Street Address Line One resides. May be required for credit card address verification.
25	Payer State	State in which Payer City resides. May be required for credit card address verification.
26	Payer Zip Code	Zip code in which payer address resides. May be required for credit card address verification.
27	Payment Channel	Describes the means used to make a payment. The State currently tracks IVR, web, walk-in, voice, fax, mail, scheduled, and unknown.

28	Comment Field	A free-form text field that may be used by an application to attach information specific to its operations. Especially useful as a payment feedback tool. Available for all payments and enrolled transactions.
29	Total Records for Application	Count of all records for the application.
30	Total Dollar Amount for Application	Total dollar amount for all records for the application.

Appendix F
CEPAS Incident Report



Appendix F
CEPAS Incident Report

Michigan Department of Treasury
4350 (Rev. 5-06)

CEPAS Incident Report

PART 1: CONTACT INFORMATION

1. Name	2. Incident Report Number
3. Office Telephone Number	4. Emergency Contact Number
5. E-mail Address	6. Fax Number
7. Alternate Contact Name	8. Alternate's Telephone Number

PART 2: INCIDENT INFORMATION

Incident Category

□ Downtime
□ Duplicates
□ Settlement
□ Unauthorized/Unlawful Activity
□ Weakness in Internal Controls
□ Other: _______

Date of Incident	Date Incident Discovered

Incident Location

Involved Parties/Entities

Description of Incident

Date of Initial Report

PART 3: INCIDENT RESOLUTION

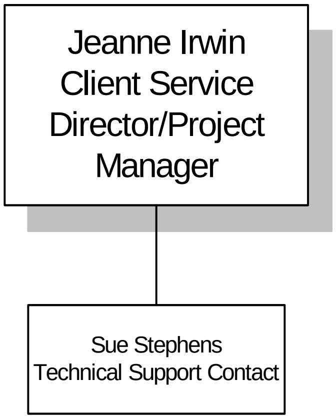
Action Taken

Incident Impact

Post Incident Recommendations

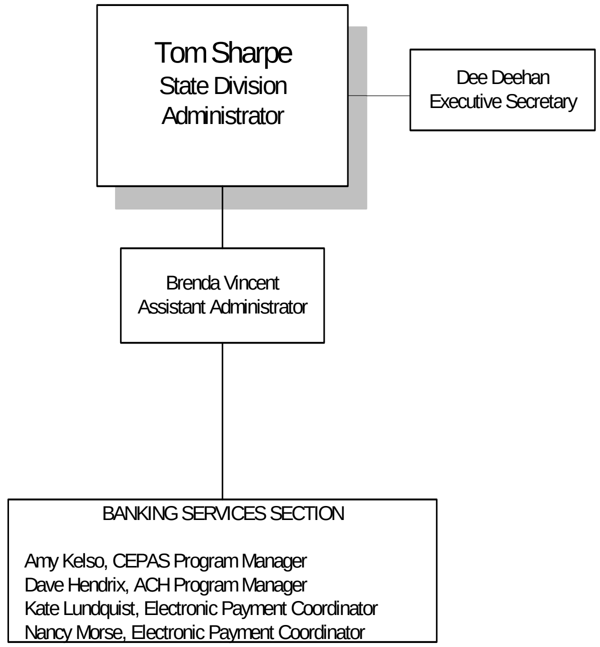
Date of Final Report

Appendix G
DTMB Organization Chart



Appendix H
Receipts Processing Division Organization Chart

DEPARTMENT OF TREASURY
RECEIPTS PROCESSING DIVISION



Tom Sharpe
State Division
Administrator

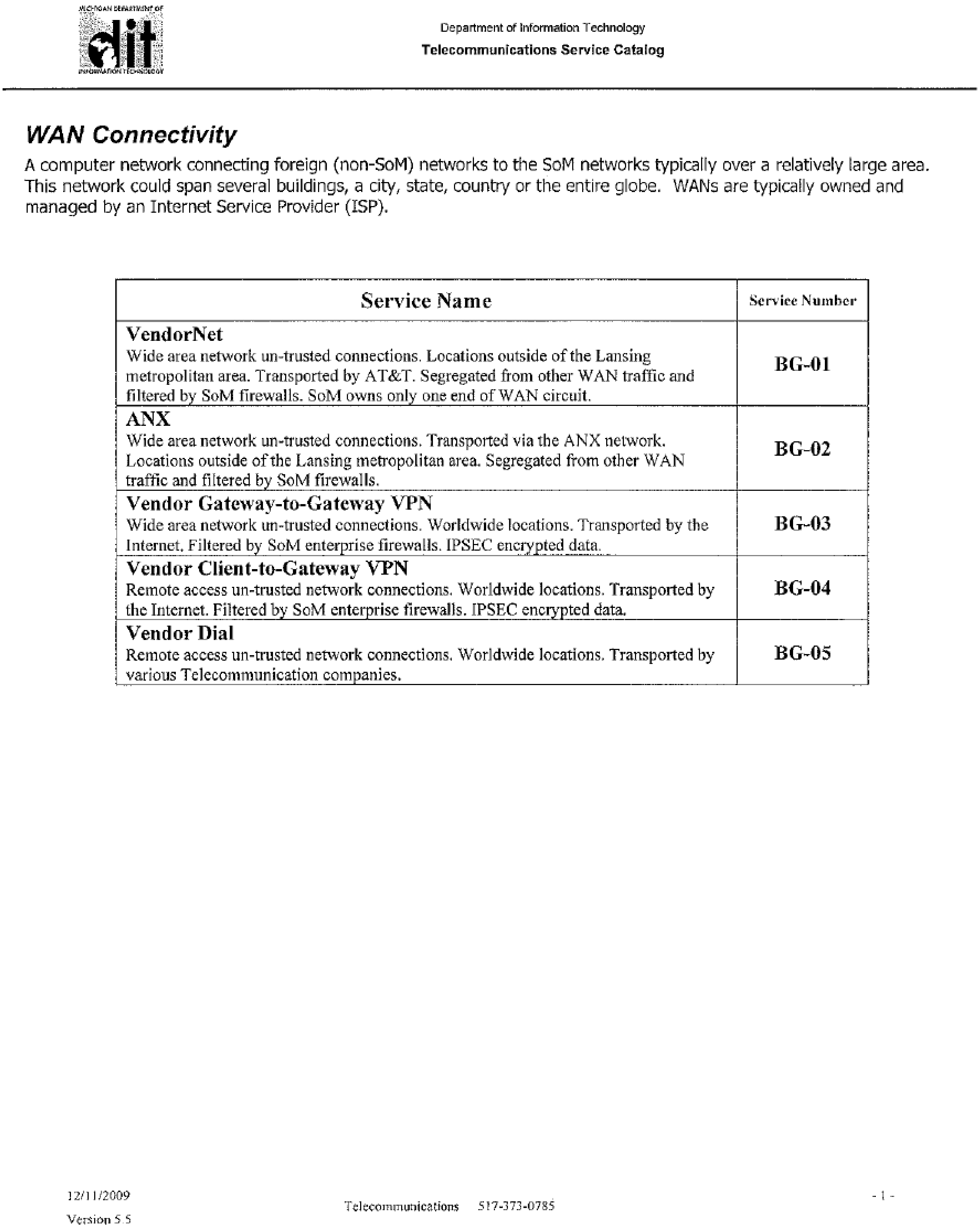
Dee Deehan
Executive Secretary

Brenda Vincent
Assistant Administrator

BANKING SERVICES SECTION

Amy Kelso, CEPAS Program Manager
Dave Hendrix, ACH Program Manager
Kate Lundquist, Electronic Payment Coordinator
Nancy Morse, Electronic Payment Coordinator

Appendix K
Vendor Gateway-to-Gateway VPN Service



MICHIGAN DEPARTMENT OF dit INFORMATION TECHNOLOGY

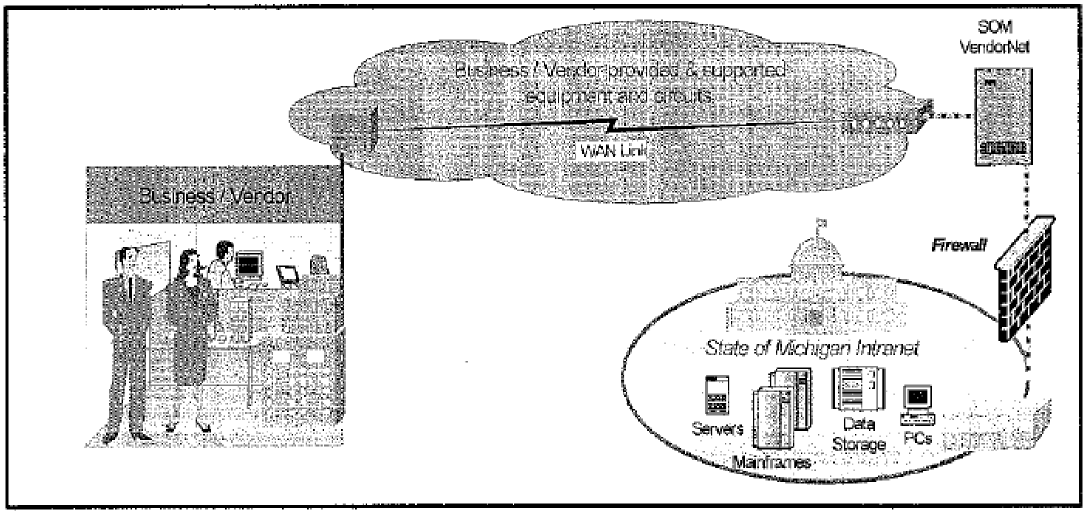
Department of Information Technology
Telecommunications Service Catalog

WAN Connectivity

A computer network connecting foreign (non-SoM) networks to the SoM networks typically over a relatively large area. This network could span several buildings, a city, state, country or the entire globe. WANs are typically owned and managed by an Internet Service Provider (ISP).

Service Name	Service Number
VendorNet Wide area network un-trusted connections. Locations outside of the Lansing metropolitan area. Transported by AT&T. Segregated from other WAN traffic and filtered by SoM firewalls. SoM owns only one end of WAN circuit.	**BG-01**
ANX Wide area network un-trusted connections. Transported via the ANX network. Locations outside of the Lansing metropolitan area. Segregated from other WAN traffic and filtered by SoM firewalls.	**BG-02**
Vendor Gateway-to-Gateway VPN Wide area network un-trusted connections. Worldwide locations. Transported by the Internet. Filtered by SoM enterprise firewalls. IPSEC encrypted data.	**BG-03**
Vendor Client-to-Gateway VPN Remote access un-trusted network connections. Worldwide locations. Transported by the Internet. Filtered by SoM enterprise firewalls. IPSEC encrypted data.	**BG-04**
Vendor Dial Remote access un-trusted network connections. Worldwide locations. Transported by various Telecommunication companies.	**BG-05**

VendorNet Service BG-01


SOM
VendorNet
Business / Vendor provided & supported equipment and circuits
WAN Link
Business / Vendor
Firewall
State of Michigan Intranet
Servers
Mainframes
Data Storage
PCs

Description

- ❑ Intended for business partners (vendors) and the State of Michigan to share access to specific resources
- ❑ Requires OES approval prior to installation
- ❑ Support for IP V4 protocol suite only
- ❑ Supports 10 / 100 Ethernet interface only

SERVICE RATING	

① = Low
⑤ = High
	① ② ③ ④ ⑤

Speed	✪ ✪ ✪ ✪
Reliability	✪ ✪ ✪ ✪
Cost	N / A

Base Rates (per month)

- ❑ None – included in basic Internet rate
- ❑ Hosting center charges for vendor owned equipment apply

Services Included

- ❑ Troubleshoot and repair of MDIT Telecommunications managed equipment
- ❑ Standard configuration changes
- ❑ MDIT Telecommunications owned and managed equipment refresh
- ❑ Maintenance and support of SoM network hardware and software

Customer Responsibilities

- ❑ WAN circuit and Ethernet connectivity to the State of Michigan
- ❑ Pre-cofigured router to attach to Vendor provided WAN circuit
- ❑ Provide primary and secondary technical point of contact

Service Level Agreement SILVER (See SLA in Appendix for additional info)*

- ❑ 24 X 7 response to trouble for SoM equipment

Installation Timeframe

Typically 10 business days after the request is accepted by MDIT Telecommunications and approved by OES

Ordering Process

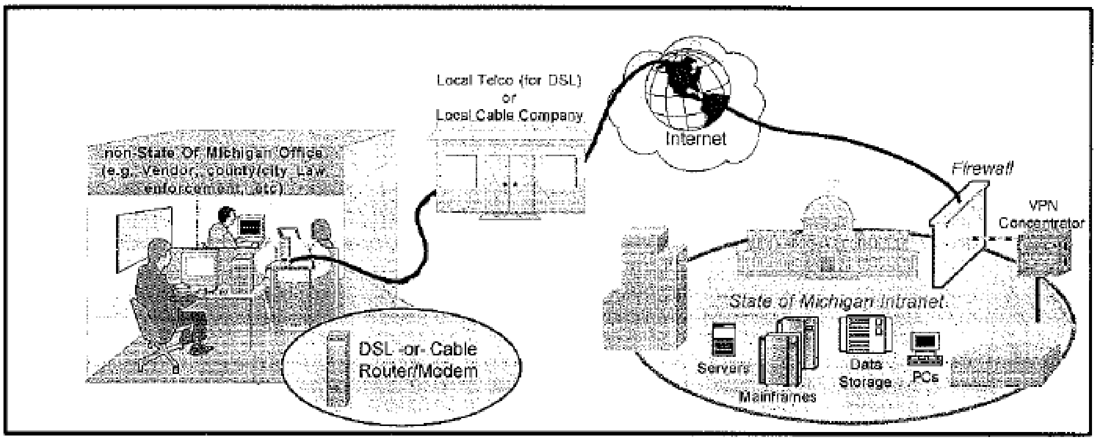
- □ A Remedy case must be submitted by an Agency Services Authorized Requestor

Questions?

- □ Phone - 517-373-0785

***Provided all customer responsibilities have been met**

(Vendor) Gateway-to-Gateway VPN Service BG-03


Local Telco (for DSL)
or
Local Cable Company
Internet
non State Of Michigan Office (e.g. Vendor, county/city Law enforcement, etc)
Firewall
VPN Concentrator
State of Michigan Intranet
DSL -or- Cable Router/Modem
Servers
Mainframes
Data Storage
PCs

Description

- □ Can be used by either business to government or local government to government partners
- □ Requires a customer provided public static IP address for the remote gateway device
- □ Intended for non State of Michigan clients to connect to specific State of Michigan resources within the State of Michigan intranet
- □ Access limitations may apply and are subject to the approval of the Office of Enterprise Security (OES)
- □ Requires an IPSEC compliant device at the customer site and the technical resources to configure that device

SERVICE RATING	

① = Low
⑤ = High
	① ② ③ ④ ⑤

Speed	● ● ●
Reliability	● ●
Cost	●

Base Rates (per month)

- □ See *Rate Table* in Appendix

Services Included

- □ Troubleshoot and repair of MDIT Telecommunications managed equipment
- □ Standard configuration changes
- □ SoM owned and managed equipment refresh
- □ Maintenance and support of SoM network hardware and software

Customer Responsibilities

- □ Provide a primary and secondary technical point of contact for customer end support
- □ Provide TCP/IP data needed to configure the tunnel i.e. destination IP addresses and ports
- □ Requires an IPSEC compliant device at the customer site and the technical resources to configure that device

Service Level Agreement BRONZE (See SLA in Appendix for additional info)*

- □ No MDIT guarantee of performance, reliability, or time to repair
- □ Service Level Agreement with ISP is customers responsibility

Installation Timeframe

- ❑ Typically 2 weeks after properly filled out request has been approved by OES. This is subject to customer schedule/capability to configure distant end

Ordering Process

- ❑ A properly filled out DIT-0051 must be submitted by an Authorized Requestor to the Client Service Center (CSC) via e-mail at DITService@Michigan.gov. The CSC will open a Remedy case, attach the electronic form to the ticket, and assign the case to MDIT Telecommunications. Phone requests are also acceptable. A phone request can be opened by calling the CSC at 517-241-9700; please have all the information required on the DIT-0051when placing your request by phone. To fax the completed form to the CSC, use 517-241-8439. The electronic form is located on MDIT's official Forms and Publications website.
- ❑ The Remedy case must be approved in the work log by an Authorized Requestor prior to case assignment to MDIT Telecommunications.

Other Information

- ❑ Follow The Sun (FTS) is a combination of two Telecom's standard offerings, Two Factor Authentication and Gateway to Gateway VPN. Traditionally, Two Factor Authentication is used to identify and validate an individual. With regard to FTS, Two Factor Authentication is the mechanism used to control when a vendor can access into the State's infrastructure. This is how it works, when a SoM agency requests that a vendor connect to a system that the vendor supports, the agency, the vendor, and the Client Service Center (CSC) partake in a conference call. During the conference call, the SecurID token number is shared with the vendor to allow that vendor logs in to a jump server using the provided token number. From the jump server the vendor can then access the supported server.

Questions?

- ❑ Phone - (517) 373-0785

***Provided all customer responsibilities have been met**

Appendix L
Non-Disclosure Agreement - DIT-0049

Per contract negotiations, the contractor will provide certification that all FDGS employees involved in this contract have signed the FDGS Code of Conduct.

Appendix M
Downtime
Service Level Agreement

The parties acknowledge that unscheduled downtime will interfere with the timely and proper completion of the Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any such delay. Therefore, Contractor and the State agree that in the case of any such unscheduled downtime in respect of which the State does not elect to exercise its rights under **Section 2.191**, the State may assess Monetary Assessments against Contractor as specified in this Section.

The Contractor is expected to meet a service level objective of 99.9% availability, less than .75 (point 75) hours of unscheduled downtime per calendar month. If unscheduled downtime occurs that exceeds this expectation, then the State shall be entitled to collect damages in the amount specified in the following chart. The amount of the Monetary Assessment will be based on the number of downtime occurrences each month and the total length of time the system is down each month. The purpose of including the number of occurrences in the damage calculation is to emphasize the State's expectation that continuous, ongoing downtime of short duration is unacceptable. The Monetary Assessment will be a percentage of the Contractor's per transaction charges for the month that the downtime occurred. At the start of a new month, the State will provide the Contractor with a list of downtime that occurred the previous month that it expects to receive Monetary Assessments for. Amounts due the State will be reflected as a credit on the corresponding monthly invoice. No delay by the State in assessing or collecting Monetary Assessments shall be construed as a waiver of such rights. The State also reserves the right to waive Monetary Assessments based on the Contractors recent system performance.

The Contractor shall not be liable for Monetary Assessments when incidents or delays result directly from causes beyond the control and without the fault or negligence of the Contractor. Such causes may include, but are not restricted to, acts of God, fires, floods, epidemics, acts of terrorism, and labor unrest; but in every case the delays must be beyond the control and without the fault or negligence of the Contractor. In addition, any outages related to the following causes shall be excluded from any calculation of downtime:

- Periods of scheduled or emergency maintenance activities or a scheduled outage;
- Problems with the State's site content or the State's or other third party's programming errors;
- Problems caused by systems administration, commands, or file transfers performed by the State's representatives;
- Interruptions in third party networks that prevent users of the Internet from accessing the State Web site;
- Other activities the State directs, denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and the Contractor's other vendors), and other force majeure events;
- Lack of availability or untimely response by the State to incidents that require the State's participation for problem source identification and/or resolution; and
- The State's breach of its obligations under this Statement of Work.

Appendix M
Downtime
Service Level Agreement

Monetary Assessments will be assessed as follows:

Number of Occurrences

>10	10%	15%	20%	25%
7-9	7.5%	10%	15%	20%
4-6	5%	7.5%	10%	15%
1-3	2.5%	5%	7.5%	10%
	.75-2	**>2-4**	**>4-8**	**>8**

Hours of Downtime

For example, if the Contractor experienced 5 occurrences of unscheduled downtime for the month, and the hours of downtime totaled 4 hours, the Contractor would be subject to Monetary Assessments of 7.5% of the monthly invoice amount for the month the downtime occurred.

Appendix N
System Response Time
Service Level Agreement

The parties acknowledge that slow system response time will interfere with the timely and proper completion of the Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any such slow system response time. Therefore, Contractor and the State agree that in the case of any such slow system response time in respect of which the State does not elect to exercise its rights under **Section 2.191**, the State may assess Monetary Assessments against Contractor as specified in this Section.

Experience has shown that even short periods of extended response time causes the State additional work as customers attempting to process payments via slow responding Internet applications close the session if it takes too long and they start over or pay via another channel. Meanwhile the original transaction is completed behind the scenes. This causes duplicate payments that need to be identified and refunded by the agency. To make matters worse, the funds availability on the customer's credit card is also impacted as two (or more) charges are applied to the card. In some cases, the second charge will be declined because the customer doesn't have enough credit available on their card.

The Contractor is contractually obligated to provide an average cumulative daily response time of three (3) seconds or less for the State of Michigan from the point at which the inquiry hits the Contractors server complex to the point at which the server complex responds with the requested inquiry response as described in Section D4. This performance and responsiveness is based on the following assumptions:

- The response time excludes any ISP backbone-related availability or performance latency problems in the connectivity between the Contractor and the State. The calculation of metrics related to the server complex's ability to support the daily hit rate will be based upon response times internal to the hosting facility.

- The Contractor will use the appropriate tools to capture data on server-hit rates, concurrent user sessions and response time within the hosting environment.

- Daily response time is defined as a 24 hour period beginning at 12:00 a.m. ET to 11:59 p.m. ET.

- This response time objective is subject to a validation by both Contractor and the State. The tool used to establish payment response time is the *Payment Response Time Report* as described in section 1.302. It will be the State's responsibility to provide notification to Contractor that response time exceeded the allowable threshold using the *Payment Response Time Report* made available to the State by the Contractor.

  •Response time could be impacted by slow response from TSYS for credit card authorizations or possibly a subcontractor for E-Check authorizations. The Contractor is expected to immediately resolve these types of issues and notify the State immediately. Documentation supporting TSYS or subcontractor performance issues and timely resolution must be provided to the State to avoid Monetary Assessment as described in this SLA.

To reimburse the State for damages caused by slow payment response time the Contractor will be expected to meet a service level objective of an average cumulative daily response time of three (3) seconds or less for the State of Michigan from the point at which the inquiry hits the server complex to the point at which the server complex responds with the requested inquiry response. If slow response time occurs that exceeds this expectation, then the State shall be entitled to collect damages in the amount specified in the following chart. The amount of the Monetary Assessment will be based on the number of days during the calendar month where the system does not meet the objective specified above. The purpose of including the number of days in the damage calculation is to emphasize the State's expectation that continuous, ongoing slow response time of even short duration is unacceptable. The Monetary Assessment will be a percentage of the Contractor's invoice total for the month that the slow response time occurred. At the start of a new month, the State will provide the Contractor with a list of days slow response time occurred the previous month that it expects to receive Monetary Assessments for. Amounts due the State will be reflected as a credit on the corresponding monthly invoice. No delay by the State in assessing or collecting Monetary Assessments shall be construed as a waiver of such rights. The State also reserves the right to waive Monetary Assessments.

The Contractor shall not be liable for Monetary Assessments when incidents or delays result directly from causes beyond the control and without the fault or negligence of the Contractor. Such causes may include, but are not restricted to, acts of God, fires, floods, epidemics, acts of terrorism, and labor unrest; but in every case the delays must be beyond the control and without the fault or negligence of the Contractor. In addition, any slow response time related to the following causes shall be excluded from any calculation of slow response time:

- Periods of scheduled or emergency maintenance activities or a scheduled outage;
- Problems caused by systems administration, commands, or file transfers performed by the State's representatives;
- Other activities the State directs, denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and the Contractor's other vendors), and other force majeure events;
- Lack of availability or untimely response by the State to incidents that require the State's participation for problem source identification and/or resolution; and
- The State's breach of its obligations under this Statement of Work.

Monetary Assessments will be assessed as follows:

Number of days of slow response time	**Percentage of monthly invoice to be credited as a monetary assessment**
16+	50%
11-15	35%
6-10	25%
2-5	10%
1	0%

For example, if the Contractor experienced 5 days of slow response time the Contractor would be subject to Monetary Assessments of 10% of the monthly invoice amount for the month the slow response time occurred.

The Contractor's liability to the State for slow System Response Time for any one month is limited to the lesser of (i) twenty-thousand dollars ($20,000); or (ii) the amount of the monetary assessment as calculated above for the month in which the slow response time occurred, but in no event will Contractor's cumulative liability to the State exceed the limits on Contractor's liability provided in Section 2.221 of this RFP.

Appendix O
Escalation Process

MI CEPAS
PayPoint Support Interaction and Escalation Process

6/20/2016

Customer Service Commitment

First Data is committed to continually improving our service by listening to our customers and responding to their needs timely and efficiently.

Customer Support # - 877-869-0860
PaySupport@FirstData.com

Dedicated Staff

First Data is dedicated to supporting our clients with the best service available. Customer service representatives are available to assist during normal business hours and beyond. The staff is a group of dedicated personnel performing support for our customers. In the event we need help outside of the PayPoint Support staff, we have access to all company resources as needed.

The following section describes the First Data Team approach to product support. This section discusses our general approach to service.

Support Services Approach

The First Data PayPoint Support Team is committed to being our customers' most valued business partner by ensuring successful implementation and use of First Data products and services.

The PayPoint Support Team office hours are 8:00AM – 7:00PM ET and staff can be reached by phone at 877.869.0860 or by emailing us at PaySupport@FirstData.com. After hours we can be reached at 877.869.0860 option 1. Your call will be routed to our answering service and they will contact the on-call technician. All issues reported through the First Data Help Desk are logged into our Support Database, creating a call ticket. Each call ticket is assigned to a contact within your agency and assigned to a support member of our staff.

Staff:
First Data has assigned Ronda Earnhart as your primary PayPoint Support contact.. Ronda will be your primary point of contact when possible and will coordinate any incidents that are being worked by other technicians.

Senior Problem Analyst Ronda Earnhart. 303.967.5438 and Ronda.Earnhart@FirstData.com.

In the event Ronda is not available, we have assigned your second point of contact as:
PayPoint Support Manager Paul Hoglund. 303.967.5833 and Paul.Hoglund@FirstData.com.

When Ronda and Paul are not available we request you contact our Help Desk at: 877.869.0860 or by emailing us at PaySupport@FirstData.com.

Note: Any emails sent directly to Ronda or Paul must include a Cc: to PaySupport@FirstData.com. In addition, all Severity 1 issues should be reported by phone in addition to email to ensure immediate attention.

Process:

- All service requests will receive a response within 1 hour and will be worked according to severity.
- Our support technician is responsible for escalating the call according to our Production Escalation Matrix as described below.
    - Upon evaluating the incident, if there is a clear resolution path that falls outside of the escalation matrix timeframe, the technician may determine no escalation is necessary. Support technician will notify the merchant of expected timeframe for resolution and no escalation will take place.
- Our PayPoint Support team and Management is responsible for tracking the issue to its resolution and contacting the client at each level of escalation to provide updates on the action being taken to resolve the issue. This team will work collaboratively with the client to determine the Severity of a problem if there is a disagreement on the severity assignment. This team is also responsible for engaging resources as needed to efficiently resolve problems in a timely fashion.
- The Account and Relationship management team has a dotted-line relationship to the Support Team and will be made aware of any escalations.
- Once an issue is escalated and the First Data Management team and the client reach an agreement on next steps, the escalation process can be put on hold and not escalated to the next level unless either party requests the process be put back into motion. Note: This would be common on items that are put into a schedule for future enhancements or have planned/scheduled maintenance windows, etc.

Calls are classified into four Severity groups:

Severity 1:

- Any problem having MAJOR or GLOBAL impact, resulting in a LOSS of vital services or resources (i.e., any issue affecting greater than 50 percent of the application or solution, NACHA bank file transfers, or Payment Processing, (Unable to make payments :Web, Consumer Payments or Admin. Make Payment function is unavailable))
- Any problem causing an outage to the customer's critical path primary processing services or capabilities and, an acceptable secondary processing capability is not immediately available.
- Daily Posting file missing.

Severity 2:

- Any problem causing an outage for the customer's primary processing services or capabilities; however an acceptable workaround or secondary processing capability has been implemented.
- Any problem causing the system or application to function at a limited capacity. (i.e., any issue affecting less than 50 percent of the application or solution).
- Administrative site not available for general use.
- Mode changes (e.g. move from cert. to production).

Severity 3:

- A problem that degrades or compromises the usability or access to a non-critical application, system or function.
- Reporting issues.
- Unexplained payment error messages.
- UAT issues regarding processor site down.
- Manage User set-up issues.
- Application configuration issues.
- Integration Issues.
- Duplicate payment research.
- PayPoint UAT site is down.

Severity 4:

- Problems that have low or no impact to internal or external customers.
- Client questions to the Account Management Team requesting information about adding additional functionality to a current application, requesting custom application documents (DSD's), etc. Severity 4 tickets serve the function of allowing us to track client to project team communication that comes through the help desk.
- General inquires/communication.
- Boarding new applications. (E-check transactions have 10 business days per contract).

Production Escalation Process – Once an issue has been received and a Severity level assigned, the Support technician will own the issue up to the maximum times defined below before moving to the next escalation level. Any team member can escalate to the next level prior to the maximum time expiring if the situation requires additional resources. All levels of the escalation management team can reach out to the PayPoint product support, Telecheck, Vital, and CTO-Hosting as needed at any time in this process. . (Note: Ownership of ticket will remain with PayPoint Support Team and it is the responsibility of PayPoint support team to engage other groups and/or escalate as needed).

Production Escalation Chart

The Escalation chart outlines how Office Hours impact escalation times.

Production Escalation Chart

During FD Office Hours (8:00 am – 7:00 pm EST, M- F)

Contact Person	Severity 1 Critical (System Down)	Severity 2 **Loss of Functionality**	Severity 3 General Inquiry or Question	Severity 4 Client questions to Account Management or general inquiries. Other non impacting items
Ronda Earnhart or PayPoint Support Technician on Duty	2 Hours*	2 Hours*	**24 HOURS**	72 Hours
PayPoint Support Manager	2 Hours	4 Hours	48 Hours	336 Hours (10 business Days)
PayPoint Director / Relationship Manager	2 Hours	4 Hours	48 Hours	** If no resolution is reached after two weeks the PayPoint Director, Director Account Management, and Relationship Manager meet to devise an appropriate action plan for the Final Resolution of the case. **
VP, Payment Solutions	Final Resolution	Final Resolution	Final Resolution	

*** All Severity 1 issues require the Technician on Duty to immediately inform the Account Manager and Help Desk manager of the situation.**

After Hours, Weekends, and Holidays				
Contact Person	Severity 1 Critical (System Down)	Severity 2 **Loss of Functionality**	Severity 3 General Inquiry or Question	Severity 4 Client questions to Account Management or general inquiries. Other non impacting items
PayPoint Support Technician on Duty	2 Hours	2 Hours	**NEXT BUSINESS DAY -** **RESEARCHED AND, IF REQUIRED, ESCALATED ACCORDING PRODUCTION ESCALATION CHART (DURING FD OFFICE HOURS)**	**NEXT BUSINESS DAY -** Researched and, if required, escalated according Production Escalation Chart (During FIRST DATA Office Hours)
Escalate in this order: PayPoint Support Manager PayPoint Director / Relationship Manager VP, Payment Solutions	PayPoint Manager or designee will Contact the Client to Discuss Resolution and Timing	PayPoint Manager or designee will Contact the Client to Discuss Resolution and Timing	** If no resolution is reached after two weeks the PayPoint Director, Director Account Management, and Relationship Manager meet to devise an appropriate action plan for the Final Resolution of the case. **	

Incident Review:
First Data will distribute a weekly PayPoint Support incident report for your review. The report will include the open and closed incidents for the period and will provide you current status on Support incidents. The PayPoint Support staff will also participate in the regularly scheduled Monthly relationship meeting. An incident review will be

conducted that focuses on the open incidents and outstanding concerns or follow-up on closed incidents.

Formal Incident Reports:
First Data understands that the State of Michigan may request a formal Incident Report for global and major business impacting service events. First Data will review the requests for formal Incident Reports with you in our joint regularly scheduled Monthly meetings. First Data will have 10 business days to complete the formal Incident Report form with all available data for the Incident Information and Incident Resolution portions of the Report. In the event there is any outstanding investigation or follow-up information that is not available prior to completion of the formal Incident report, First Data will provide information around the pending item along with an estimated completion time for the close out of the pending items in the Incident Report.

The First Data Director of eService Account Management will be the owner of the formal Incident Report response process.

Contacts:
Ronda Earnhart, Senior Problem Analyst and Primary PayPoint Support contact.

303.967.5438 direct
303.799.3621 fax
Ronda.Earnhart@FirstData.com

Paul Hoglund, PayPoint Support Manager and Secondary contact

303.967.5833 direct
303.799.3621 fax
303.478.6111 mobile

Paul.Hoglund@firstdata.com

PayPoint Support
877.869.0860
PaySupport@FirstData.com.

Kristen Olson, Director PayPoint

303.967.5570 direct
303.967.5599 fax
303.949.3552 mobile
kristen.olson@FirstData.com

Jason Clark, Relationship Manager
513.489.9599 x184 direct
513.489.6521 fax
513.288.9313 mobile
chris.stevens@firstdata.com

Gerhard Milkuhn, Director eService Account Management
513.489.9599 x155 direct
513.489.6521 fax
513.379.3675 mobile
Gerhard.Milkuhn@firstdata.com

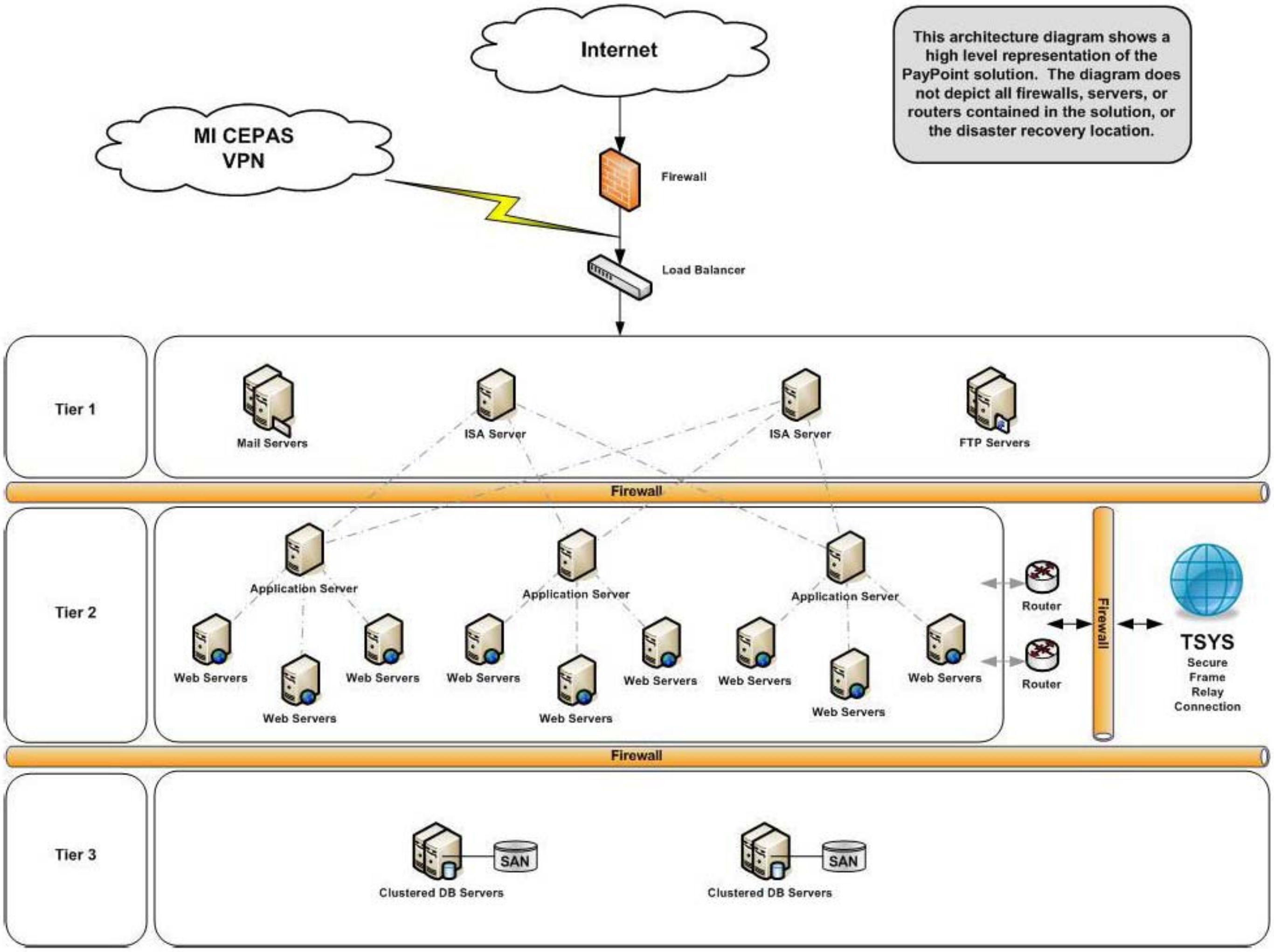
Chuck Eliasen, VP Payment Solutions
513.489.9599 x151 direct
513.489.6521 fax
Chuck.Eliasen@firstdata.com

If at any time, the Department is not satisfied with the level of service they are provided, they can contact the PayPoint Director:

Kristen Olson
12500 E Belford Ave
Englewood, CO 80112
303-967-5570
kristen.olson@firstdata.com

This page intentionally left blank.

Appendix P
FDGS Network Architecture



This architecture diagram shows a high level representation of the PayPoint solution. The diagram does not depict all firewalls, servers, or routers contained in the solution, or the disaster recovery location.

Appendix Q
New Acquirer Statement of Work

MI CEPAS

New Acquirer

Statement of Work

Submitted by

First Data Government Solutions

To

MI CEPAS

Version 1.3

May 14, 2010

Revision History

Revision Date	Version	Notes
05/13/2010	1.0	Draft
5/20/2010	1.1	Amy Kelso’s edits
5/28/2010	1.2	Amy and Jason’s Edits
6/1/2010	1.3	Clean Draft

STATEMENT OF WORK FOR
Hardware, Software, and Professional Services

This Statement of Work ("SOW"), effective as of the date last written below ("Effective Date"), is attached to, and made a part of, the Agreement dated December 1, 2006 (the "Agreement"), by and between First Data Government Solutions, Inc. ("FDGS") and the State of Michigan CEPAS ("Client"). All terms and conditions contained in the Agreement shall remain in full force and effect and shall apply to the extent applicable to this SOW, except as expressly modified herein. To the extent that the terms and conditions of this SOW are in conflict with the terms and conditions of this Agreement, or any other incorporated item, this SOW shall control relative to the Work Products and/or Services produced hereunder.

The terms of this SOW are limited to the scope of this SOW and shall not be applicable to any other SOWs, which may be executed between the parties.

This SOW consists of this signature page and the following sections that are incorporated in this SOW by this reference:

1. Project Description
2. Responsibilities of the Parties
3. Key Assumptions
4. Professional Services Requirements
5. Software Requirements & Specifications
6. Hardware Requirements & Specifications
7. Training
8. Documentation
9. Maintenance
10. Project Schedule
11. Deliverables
12. Pricing and Payment
13. Acceptance
14. Change Management
15. Key Contact Information
16. Miscellaneous

IN WITNESS WHEREOF, the duly authorized representatives of the parties hereto have caused this SOW to be duly executed.

First Data Government Solutions, Inc.	**Client** **by its duly authorized representative:**
By: ______________________	By: ______________________
Name: ______________________	Name:______________________
Title: ______________________	Title: ______________________
Date: ______________________	Date: ______________________

1.0 Project Description

The purpose of this SOW is to modify the existing credit card processing acquirer data within the FDGS PayPoint configuration to reflect the Clients new credit card processing acquirer information; Fifth Third Processing Solutions (FTPS).

Automated Process

FDGS to update processing acquirer data within the PayPoint configuration using an automated program or application developed by FDGS.

Steps include the following:

- Design document
- Develop & code application
- QA application
- Build spreadsheet with migration configuration items
- Run automated settlement
- Run Test transaction and reverse payment
- Monitor transactions after configuration changes
- Review logs
- Monitor next day settlement

2.0 Responsibilities of the Parties

Client:

- Responsible for providing updated configuration data one (1) to two (2) weeks prior to each Application migration
- Responsible for disabling all payment traffic prior to specified cutoff day/time.
- Monitor applications while FDGS tests the updated merchant information
- Enable payment traffic on designated application once FDGS confirms testing is complete/successful

FDGS:

- Provide project specifications
- Provide detailed project plan
- Provide updated documentation to reflect the new changes / functionality listed within the SOW
- Provide functionality listed in this SOW

3.0 Key Assumptions

- Implementation start date will be determined once the SOW is fully executed.
- The Migration schedule will be determined once the SOW is fully executed
- Approximately 339 applications to be converted to the new acquirer.
- Approximately 15 agencies
- Client will migrate agency-by-agency. All applications under an agency will be migrated during the same window; with the exception of the Department of State, which will be implemented over a three to four week time frame.
- Client will be responsible for disabling front-end apps for migration.
    - This includes Consumer Payments applications
- Client is responsible for providing updated configuration data to FDGS

- FDGS will perform Agency migrations will be done at a mutually agreeable time, which many may be during business hours.
- FDGS will verify that data provided by Client has been updated in the configuration per application. Should an update fail due to data inconsistencies between FDGS's configuration and the data provided by the client, FDGS will provide the Client with a list of updates that were rejected. If the "test" payment fails FDGS will revert back to the old Vital information, otherwise the Client will not be able to accept payments for that application. It is up to Client and FTPS to determine/manage the priority for correcting the rejects. Once the data has been updated and provided back to FDGS in the proper format FDGS will try to re-import the data using the automated process.

4.0 Professional Services Requirements

- Project management
- Development engineer
- Business analyst
- Quality assurance staff

5.0 Software Requirements & Specifications

- No new software requirements at this time

6.0 Hardware Requirements & Specifications

- No new hardware requirements at this time

7.0 Training

Not Applicable

8.0 Documentation

- Design Document
- Spreadsheet of old/new merchant information

9.0 Maintenance

- Not Applicable

10.0 Project Schedule

- A mutually agreeable project schedule to be defined upon completion of AccessNet project specification and based on FDGS resource availability. Client will be responsible for all correspondence, resource scheduling, and project management with FTPS.

11.0 Deliverables

- FDGS to provide project specifications
- FDGS to provide detailed project plan
- FDGS to provide updated documentation to reflect the new changes / functionality listed within the SOW
- FDGS to provide functionality listed in this SOW

12.0 Pricing and Payment

The pricing and payment terms listed below are good for 60 days from June 1, 2010

Automated Process

- Project management
- Development engineer
- Business analyst
- Quality assurance staff

Payment terms for the system are as follows:

- 100% of Professional Services to be invoiced upon successful migration of first agency. Total Cost **$13,175.00**
  FDGS to include the fee on the monthly invoice. FDGS to work with the State to determine fee split by agency if applicable.

- Should client cancel this SOW for any reason (e.g. Lack of funding, etc.), client will pay FDGS for work performed up to date of cancellation. If Client delays the project more than 30 days beyond the agreed upon schedule they will pay FDGS for services performed to date and a new price will need to be negotiated for the remainder of the project.

13.0 Acceptance

Each deliverable is deemed accepted by the client should client begin using the system in production, or if the client does not notify FDGS of any nonconformance, in writing, within five business days after delivery.

14.0 Change Management

- Not Applicable

15.0 Key Contact Information

Amy Kelso
CEPAS/Credit Card Program Manager
Dept. of Treasury - Receipts Processing Division
Phone (517) 636-5372
Fax (517) 636-5401
kelsoa@michigan.gov

Brandon Keith
Project Manager
First Data
Phone (303) 967-5540
Fax (303) 967.5867
Brandon.Keith@FirstData.com

Jason Clark
Relationship Manager
First Data
Phone (513) 489-9599 ext 184
Fax (513) 489-6521
Jason.Clark@FirstData.com

16.0 Miscellaneous

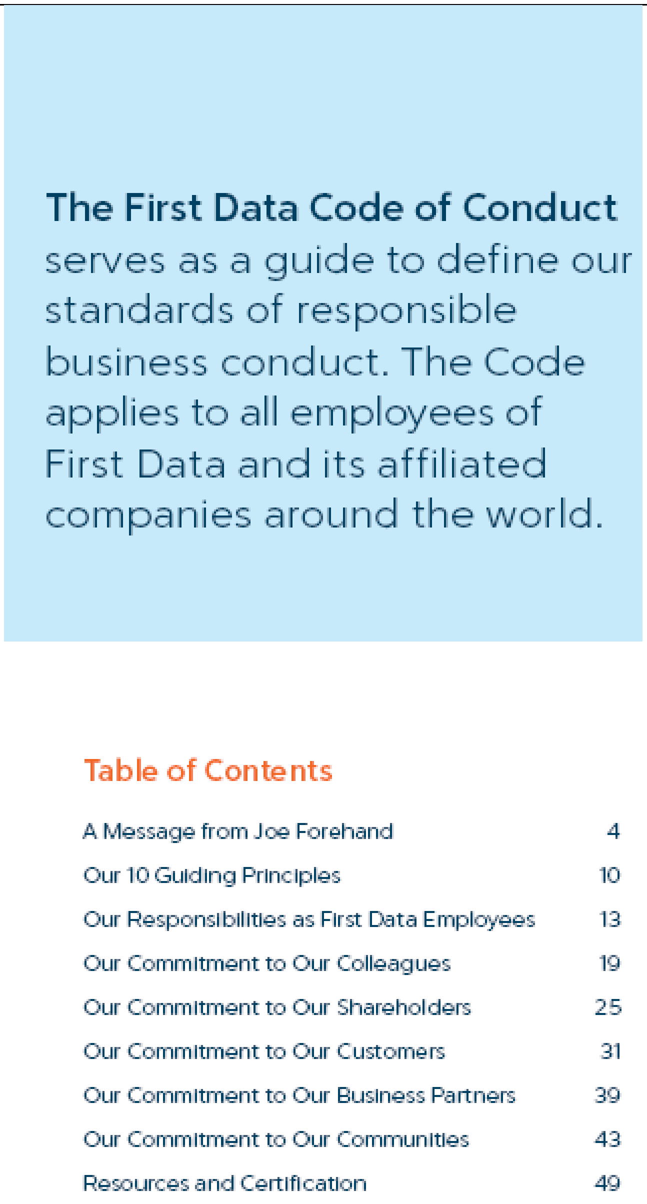
Limitation of Liability: (a) In no event shall First Data have any liability or responsibility for any indirect, incidental, punitive, exemplary, special or consequential damages (including, but not limited to, damages arising from loss of profits or data), even if advised of the possibility of such damages; (b) To the maximum extent permitted by applicable law, First Data's liability for damages hereunder shall not exceed the amount of fees paid under this SOW.

Appendix R
FDGS Code of Conduct

First Data™ Code of Conduct

Our Code of Conduct reflects the spirit of our culture and our commitment to trust, respect, security and excellence.

First Data.



The First Data Code of Conduct serves as a guide to define our standards of responsible business conduct. The Code applies to all employees of First Data and its affiliated companies around the world.

Table of Contents

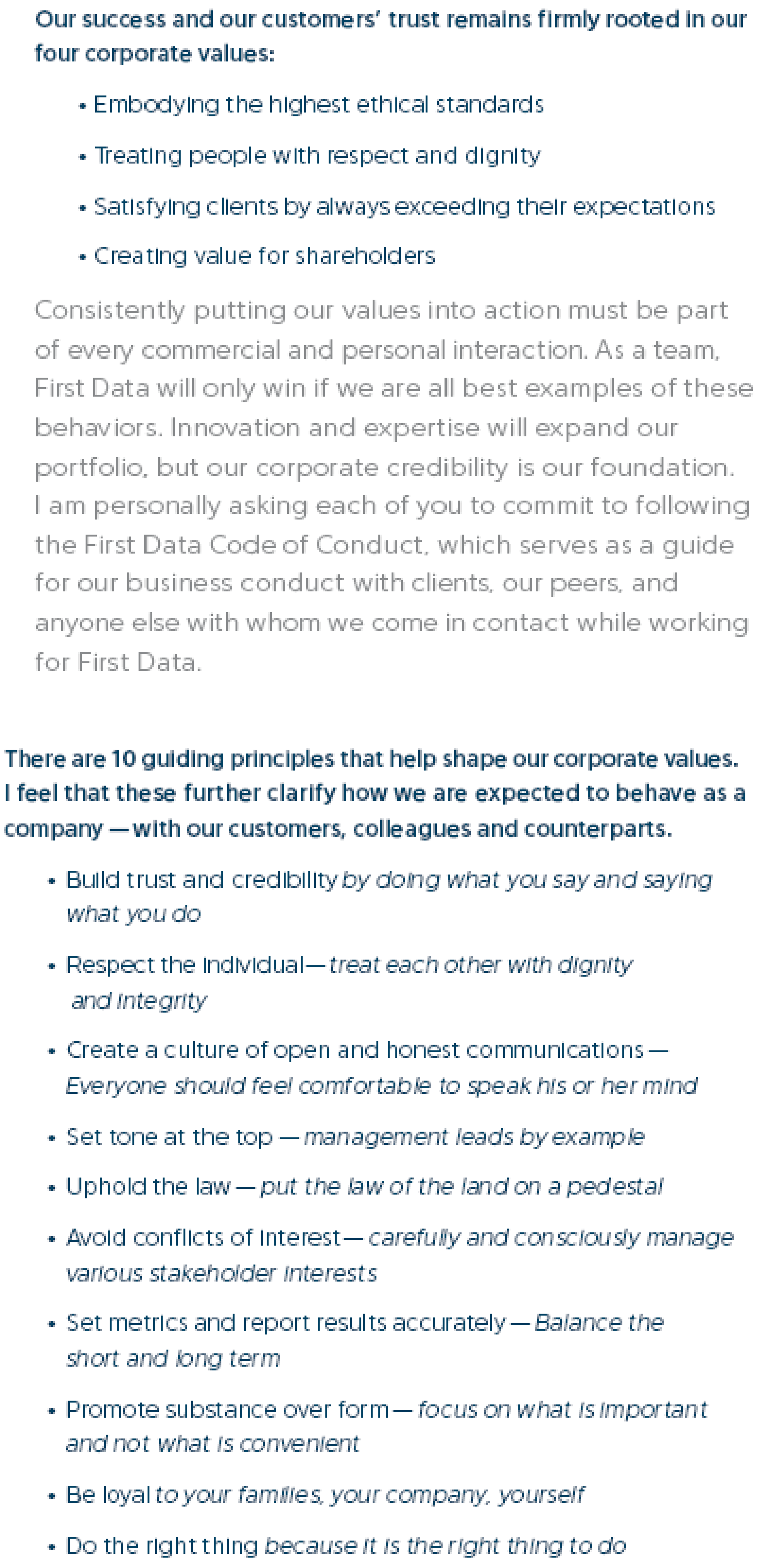
A Message from Joe Forehand

Dear First Data Colleague,

As First Data transforms and advances our scope of services, we continue to strengthen our position as one of global business' most loyal and valuable partners. The currency of this bond is our customers' trust.

We earn this trust through our unflinching commitment to customers coupled with our ongoing conviction to do what is right, both internally and externally. By following this commitment, we will continue to deliver strong results and expand our business.

I am proud of our accomplishments and excited about what lies ahead. We are providing new levels of service to our customers and capitalizing on emerging opportunities. These new opportunities present challenges and emphasize the importance of our ongoing collective commitment to a culture of lawful and ethical conduct.



Our success and our customers' trust remains firmly rooted in our four corporate values:

- Embodying the highest ethical standards
- Treating people with respect and dignity
- Satisfying clients by always exceeding their expectations
- Creating value for shareholders

Consistently putting our values into action must be part of every commercial and personal interaction. As a team, First Data will only win if we are all best examples of these behaviors. Innovation and expertise will expand our portfolio, but our corporate credibility is our foundation. I am personally asking each of you to commit to following the First Data Code of Conduct, which serves as a guide for our business conduct with clients, our peers, and anyone else with whom we come in contact while working for First Data.

There are 10 guiding principles that help shape our corporate values. I feel that these further clarify how we are expected to behave as a company — with our customers, colleagues and counterparts.

- Build trust and credibility *by doing what you say and saying what you do*
- Respect the individual — *treat each other with dignity and integrity*
- Create a culture of open and honest communications — *Everyone should feel comfortable to speak his or her mind*
- Set tone at the top — *management leads by example*
- Uphold the law — *put the law of the land on a pedestal*
- Avoid conflicts of interest — *carefully and consciously manage various stakeholder interests*
- Set metrics and report results accurately — *Balance the short and long term*
- Promote substance over form — *focus on what is important and not what is convenient*
- Be loyal *to your families, your company, yourself*
- Do the right thing *because it is the right thing to do*

The Code of Conduct helps us maintain our current momentum. It guides our collective business conduct while holding us accountable to each other and our customers. It defines our expected behavior and how it relates to our core values and guiding principles.

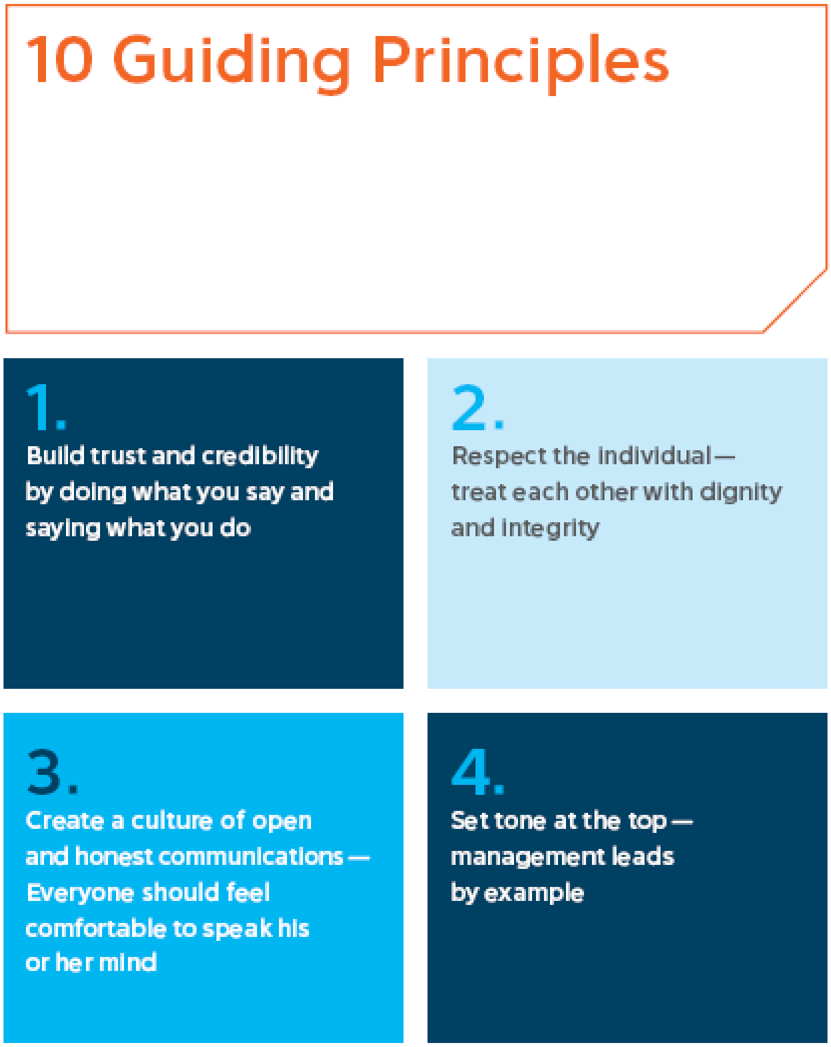
As part of our commitment to open and honest communication, all of us are empowered to raise any possible violation of the Code of Conduct. This responsibility extends to any business or accounting practice. You have my commitment that you will not suffer any adverse action or career disadvantage for questioning First Data practices, or for honestly raising a suspected violation of the Code of Conduct.

If you have any concerns regarding any such issues, please speak to your immediate supervisor or the human resource organization or, in your judgment when circumstances warrant, you should raise the issue with First Data's General Counsel *(303-967-5670)*, First Data's Chief Compliance and Privacy Officer *(303-967-5186)*, or me directly *(303-967-8010)*. Any of these avenues are open to you.

Whenever I meet with employees, I am consistently amazed at the passion for First Data and the desire for our collective success. Together, we are building one of the most esteemed and trusted companies in the world. As we move forward, I would ask you all to remember this trust we've earned requires constant vigilance from every one of us.

Thank you,

Joe Forehand
Chairman and CEO
First Data Corporation



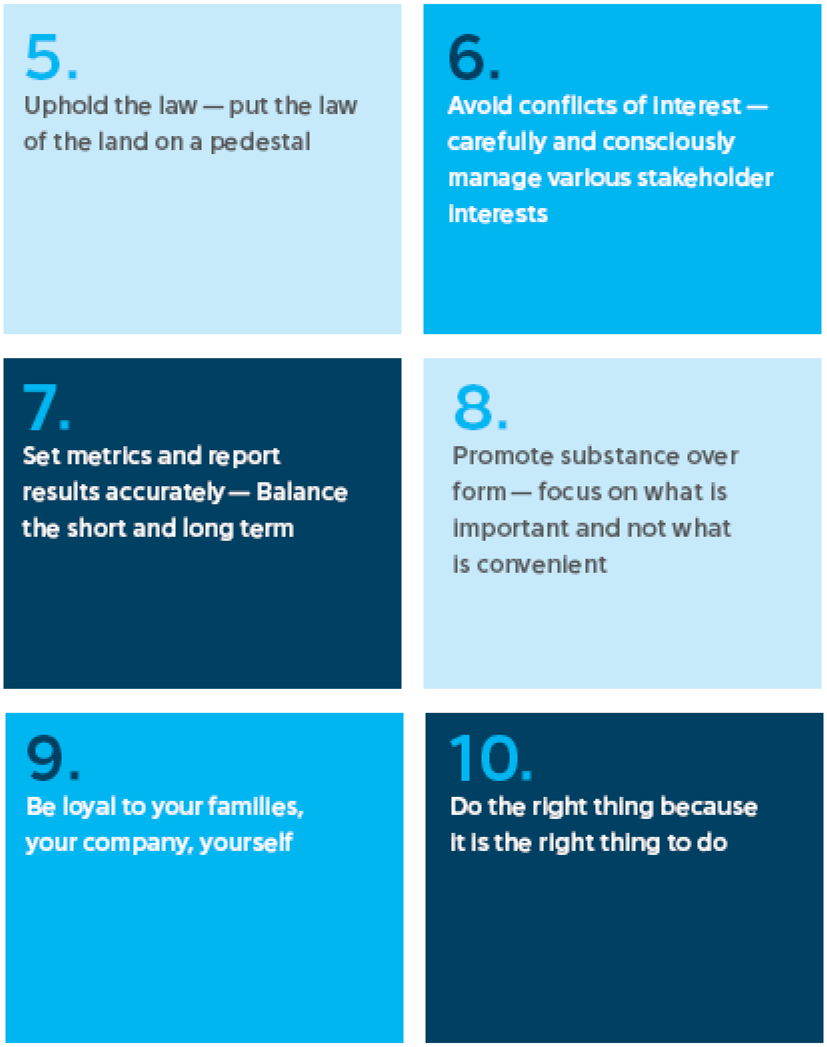
10 Guiding Principles

1\.
Build trust and credibility by doing what you say and saying what you do

2\.
Respect the individual — treat each other with dignity and integrity

3\.
Create a culture of open and honest communications — Everyone should feel comfortable to speak his or her mind

4\.
Set tone at the top — management leads by example



5.
Uphold the law — put the law of the land on a pedestal

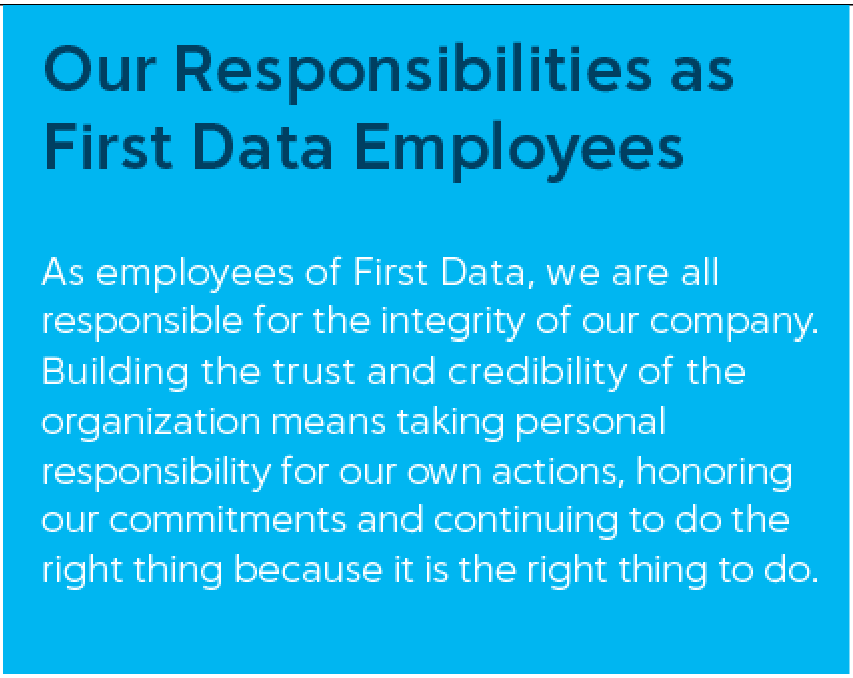
6.
Avoid conflicts of interest — carefully and consciously manage various stakeholder interests

7.
Set metrics and report results accurately — Balance the short and long term

8.
Promote substance over form — focus on what is important and not what is convenient

9.
Be loyal to your families, your company, yourself

10.
Do the right thing because it is the right thing to do



Our Responsibilities as First Data Employees

As employees of First Data, we are all responsible for the integrity of our company. Building the trust and credibility of the organization means taking personal responsibility for our own actions, honoring our commitments and continuing to do the right thing because it is the right thing to do.

The standards set forth in the Code reflect the spirit in which First Data employees should conduct themselves in their work lives.

While no manual can replace thoughtful decision-making by the people who work here, the Code does help promote honest and ethical conduct. It does this by helping us understand what it means to live our standards in the workplace, by guiding us in recognizing and dealing with ethical issues, by pointing us toward resources when we need them; and by discouraging wrongdoing.

Whenever there is any internal investigation or audit, including Code of Conduct, financial reporting or employee relations issues, we will fully cooperate in the investigation, provide truthful, honest and complete responses, and maintain the confidentiality of the investigation.

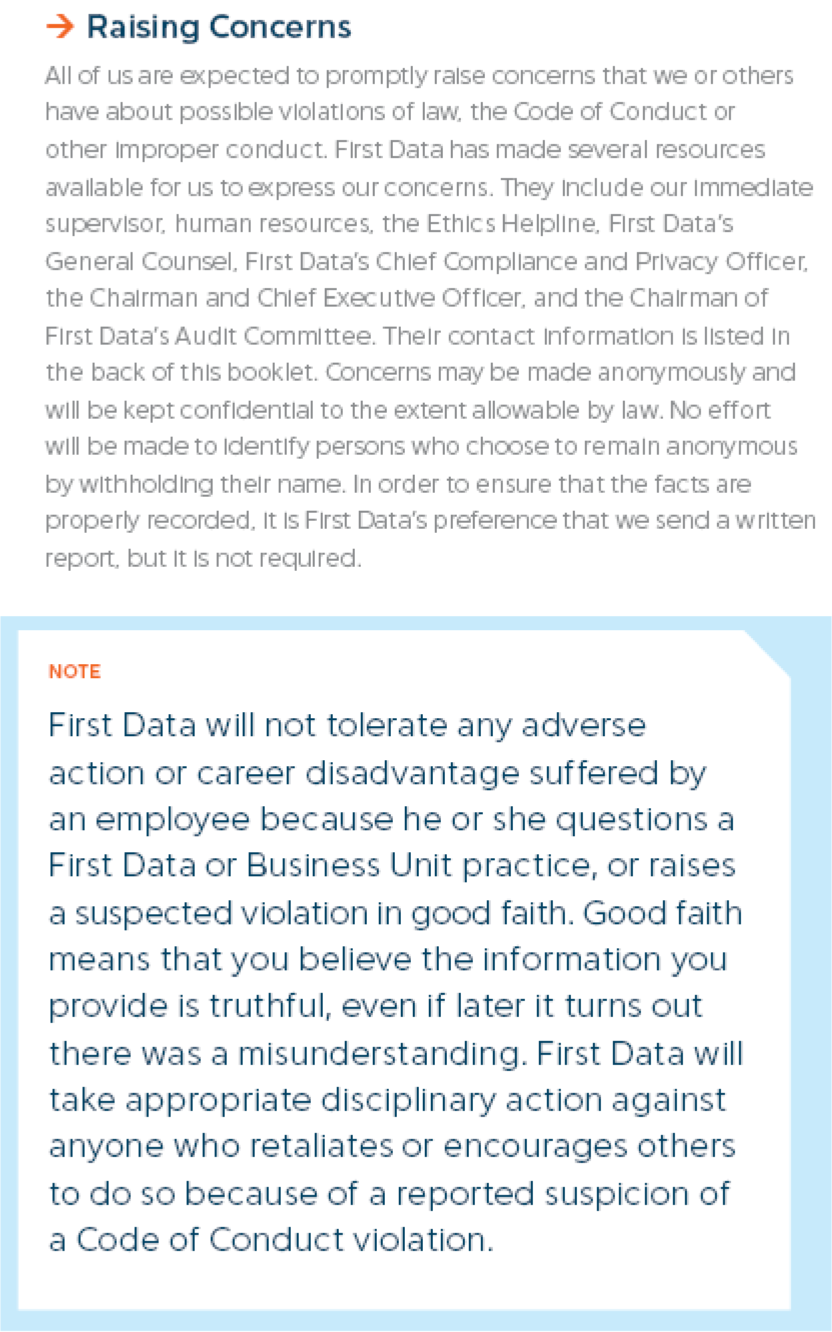
Each of us is responsible for reading, understanding and applying the Code. Complying with the Code is a condition of employment at First Data. Failure to follow its standards or failure to report a known violation can lead to disciplinary action, based on the violation, up to and including termination.

→ Special Responsibilities of Managers

The attitudes and actions of managers influence the attitudes and actions of their employees. As leaders, managers are expected to show integrity and respect in their dealings with everyone — fellow employees, customers, suppliers and the community. Their words and actions must show that business results are never more important than our ethical standards. They must ensure that employees are trained in our Code and in related topics and policies. They should create a workplace where employees can safely and freely raise questions and express concerns. Managers have the responsibility to carefully watch for indications that unethical or illegal behavior has occurred.

→ No Waivers

The Code of Conduct applies to all First Data employees and it is First Data’s policy not to grant any waivers. First Data recognizes that questions may arise when the Code applies to conduct that is legal and acceptable under the circumstances. If there are any questions on applicability of the Code, we should contact First Data’s General Counsel, First Data’s Chief Compliance and Privacy Officer, or other resources listed in the back of the Code.



→ Raising Concerns

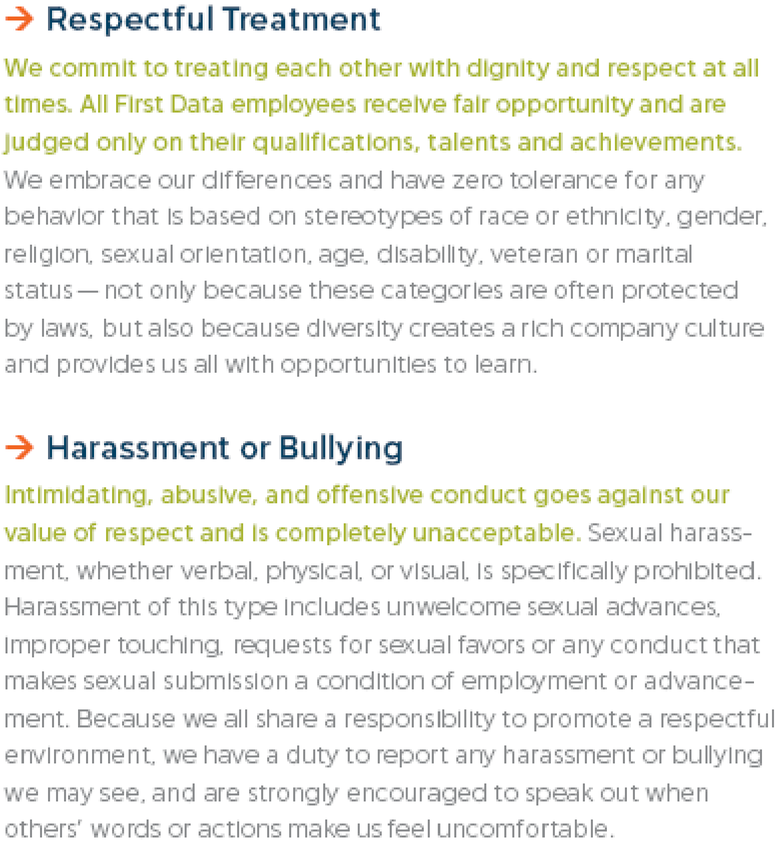
All of us are expected to promptly raise concerns that we or others have about possible violations of law, the Code of Conduct or other improper conduct. First Data has made several resources available for us to express our concerns. They include our immediate supervisor, human resources, the Ethics Helpline, First Data's General Counsel, First Data's Chief Compliance and Privacy Officer, the Chairman and Chief Executive Officer, and the Chairman of First Data's Audit Committee. Their contact information is listed in the back of this booklet. Concerns may be made anonymously and will be kept confidential to the extent allowable by law. No effort will be made to identify persons who choose to remain anonymous by withholding their name. In order to ensure that the facts are properly recorded, it is First Data's preference that we send a written report, but it is not required.

NOTE

First Data will not tolerate any adverse action or career disadvantage suffered by an employee because he or she questions a First Data or Business Unit practice, or raises a suspected violation in good faith. Good faith means that you believe the information you provide is truthful, even if later it turns out there was a misunderstanding. First Data will take appropriate disciplinary action against anyone who retaliates or encourages others to do so because of a reported suspicion of a Code of Conduct violation.

Our Commitment to Our Colleagues

Creating a culture of openness and candor, one in which we treat each other with the dignity we all deserve, ensures a strong and vital First Data. Leaders have an added responsibility to lead by example — their actions set the tone the rest of us follow.



Respectful Treatment

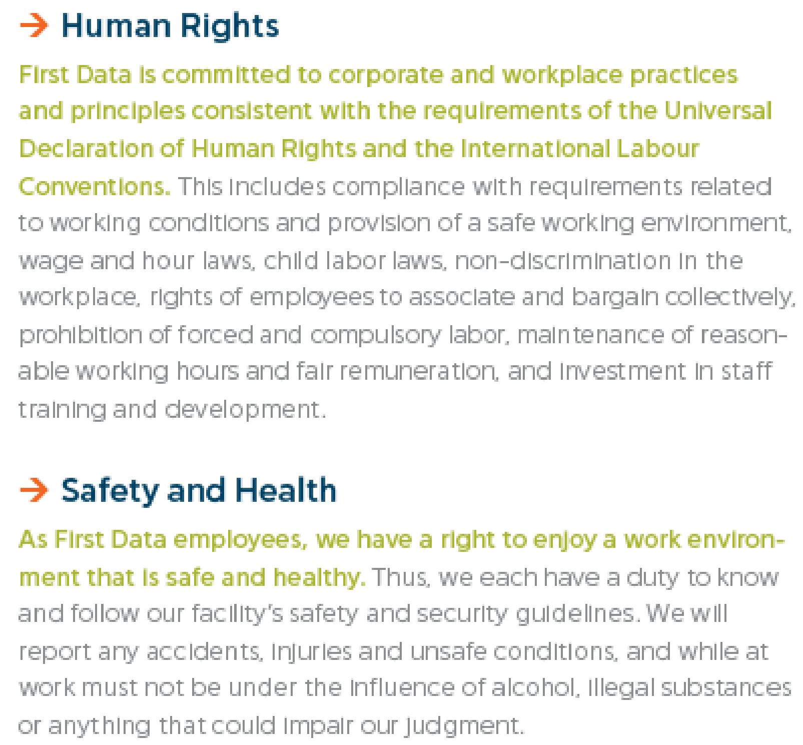
We commit to treating each other with dignity and respect at all times. All First Data employees receive fair opportunity and are judged only on their qualifications, talents and achievements. We embrace our differences and have zero tolerance for any behavior that is based on stereotypes of race or ethnicity, gender, religion, sexual orientation, age, disability, veteran or marital status — not only because these categories are often protected by laws, but also because diversity creates a rich company culture and provides us all with opportunities to learn.

Harassment or Bullying

Intimidating, abusive, and offensive conduct goes against our value of respect and is completely unacceptable. Sexual harassment, whether verbal, physical, or visual, is specifically prohibited. Harassment of this type includes unwelcome sexual advances, improper touching, requests for sexual favors or any conduct that makes sexual submission a condition of employment or advancement. Because we all share a responsibility to promote a respectful environment, we have a duty to report any harassment or bullying we may see, and are strongly encouraged to speak out when others' words or actions make us feel uncomfortable.

→ Employee Data Privacy

First Data is committed to maintaining the highest standards for the protection of the legitimate data privacy interests of its employees. As part of that commitment, First Data has adopted an Employee Data Privacy Policy and has also certified to the Safe Harbor standards for handling employee information.



Human Rights

First Data is committed to corporate and workplace practices and principles consistent with the requirements of the Universal Declaration of Human Rights and the International Labour Conventions. This includes compliance with requirements related to working conditions and provision of a safe working environment, wage and hour laws, child labor laws, non-discrimination in the workplace, rights of employees to associate and bargain collectively, prohibition of forced and compulsory labor, maintenance of reasonable working hours and fair remuneration, and investment in staff training and development.

Safety and Health

As First Data employees, we have a right to enjoy a work environment that is safe and healthy. Thus, we each have a duty to know and follow our facility's safety and security guidelines. We will report any accidents, injuries and unsafe conditions, and while at work must not be under the influence of alcohol, illegal substances or anything that could impair our judgment.

Our Commitment to Our Shareholders

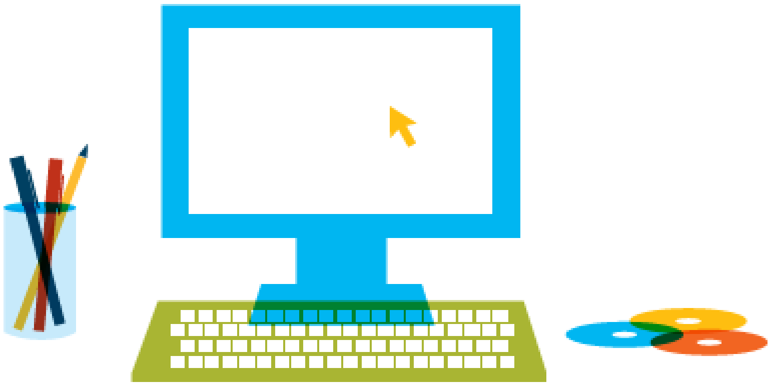
Delivering value to our shareholders goes beyond financial performance. It means ensuring that we never compromise our ethics for a financial goal, and that accurate reporting and a balanced view of our financial priorities will ultimately reap great rewards for our shareholders and for ourselves.

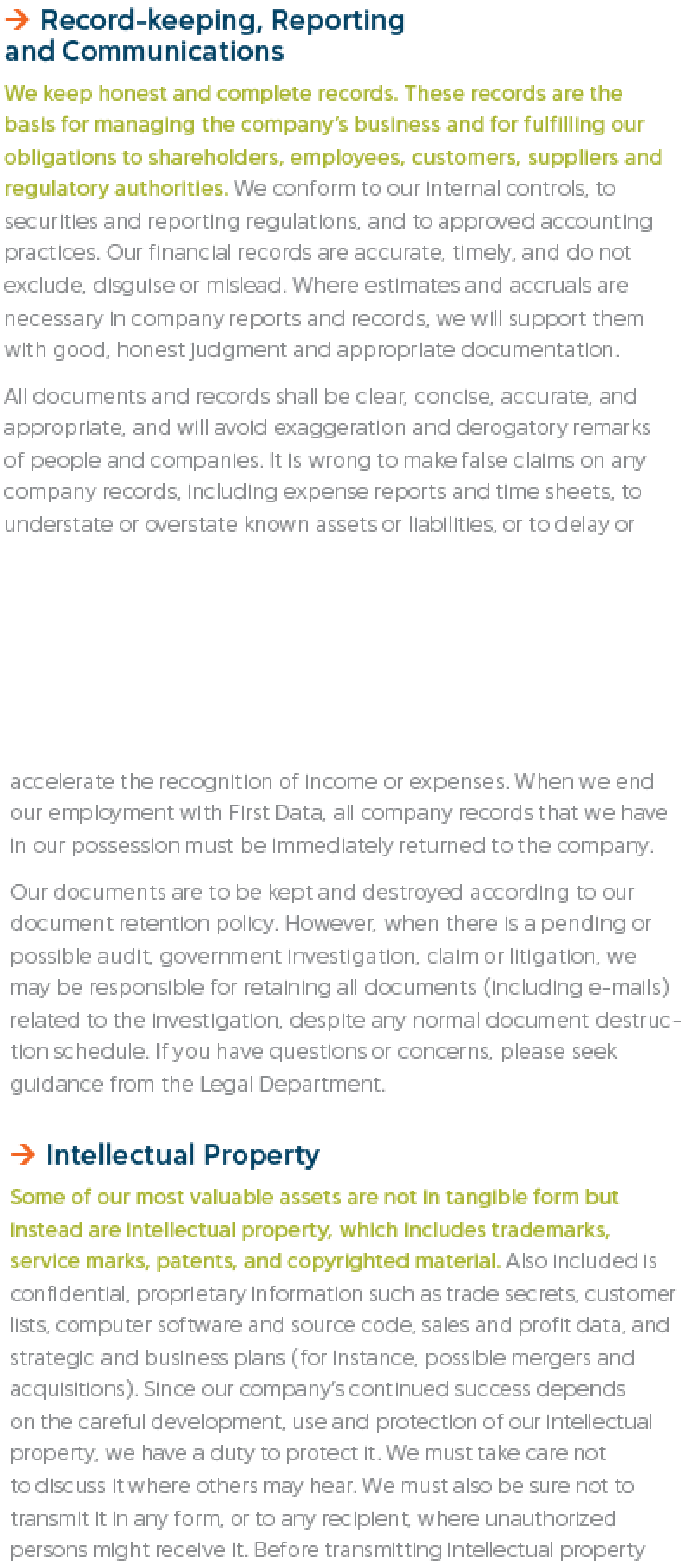
→ Use of Assets

Our shareholders entrust First Data assets to us. We take pride in living up to that trust. We are responsible for using company assets for business purposes only, and for protecting them from damage, loss, waste, misuse or theft.

We always make sure that we:

- **Receive prior approval before taking or giving away First Data property or assets, including any use of cash or company credit cards.**
- **Use email, telephones, computers and other company assets only for business purposes, unless we have our managers' approval for personal use.**





→ Record-keeping, Reporting and Communications

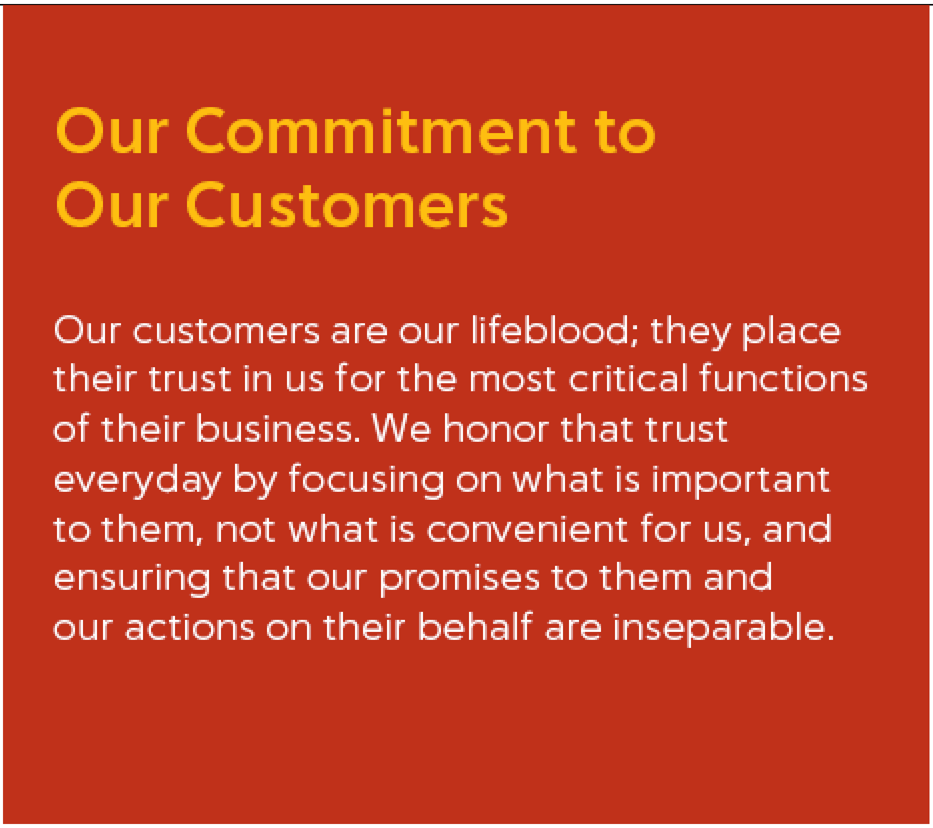
We keep honest and complete records. These records are the basis for managing the company's business and for fulfilling our obligations to shareholders, employees, customers, suppliers and regulatory authorities. We conform to our internal controls, to securities and reporting regulations, and to approved accounting practices. Our financial records are accurate, timely, and do not exclude, disguise or mislead. Where estimates and accruals are necessary in company reports and records, we will support them with good, honest judgment and appropriate documentation.

All documents and records shall be clear, concise, accurate, and appropriate, and will avoid exaggeration and derogatory remarks of people and companies. It is wrong to make false claims on any company records, including expense reports and time sheets, to understate or overstate known assets or liabilities, or to delay or accelerate the recognition of income or expenses. When we end our employment with First Data, all company records that we have in our possession must be immediately returned to the company.

Our documents are to be kept and destroyed according to our document retention policy. However, when there is a pending or possible audit, government investigation, claim or litigation, we may be responsible for retaining all documents (including e-mails) related to the investigation, despite any normal document destruction schedule. If you have questions or concerns, please seek guidance from the Legal Department.

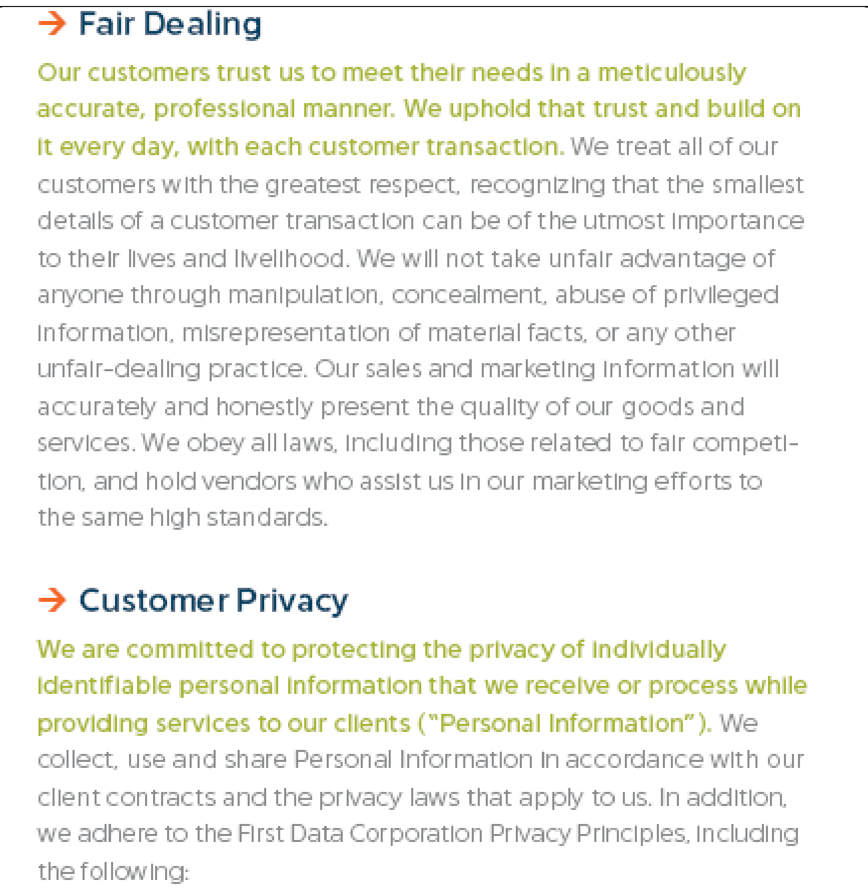
→ Intellectual Property

Some of our most valuable assets are not in tangible form but instead are intellectual property, which includes trademarks, service marks, patents, and copyrighted material. Also included is confidential, proprietary information such as trade secrets, customer lists, computer software and source code, sales and profit data, and strategic and business plans (for instance, possible mergers and acquisitions). Since our company's continued success depends on the careful development, use and protection of our intellectual property, we have a duty to protect it. We must take care not to discuss it where others may hear. We must also be sure not to transmit it in any form, or to any recipient, where unauthorized persons might receive it. Before transmitting intellectual property outside the company, including to a consultant or contractor, obtain the Legal Department's approval. Our obligation to preserve the confidentiality of First Data's proprietary information continues even after we are no longer employees of the Company. In the course of performing our job functions, we may receive information about possible transactions with other companies or receive confidential information about other companies. This type of material is often their intellectual property and is subject to the same confidentiality guidelines.



Our Commitment to Our Customers

Our customers are our lifeblood; they place their trust in us for the most critical functions of their business. We honor that trust everyday by focusing on what is important to them, not what is convenient for us, and ensuring that our promises to them and our actions on their behalf are inseparable.

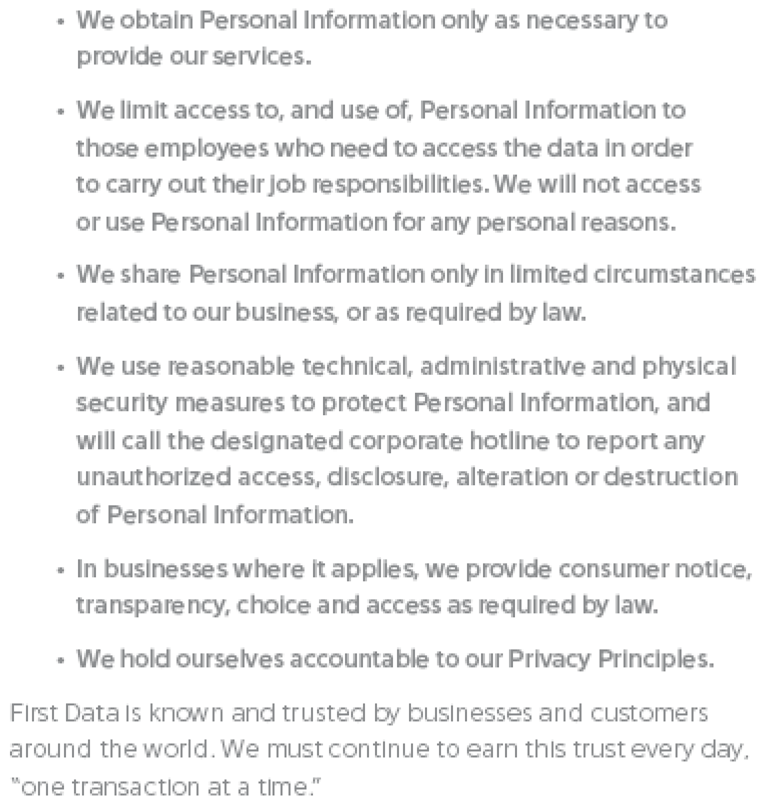


→ Fair Dealing

Our customers trust us to meet their needs in a meticulously accurate, professional manner. We uphold that trust and build on it every day, with each customer transaction. We treat all of our customers with the greatest respect, recognizing that the smallest details of a customer transaction can be of the utmost importance to their lives and livelihood. We will not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice. Our sales and marketing information will accurately and honestly present the quality of our goods and services. We obey all laws, including those related to fair competition, and hold vendors who assist us in our marketing efforts to the same high standards.

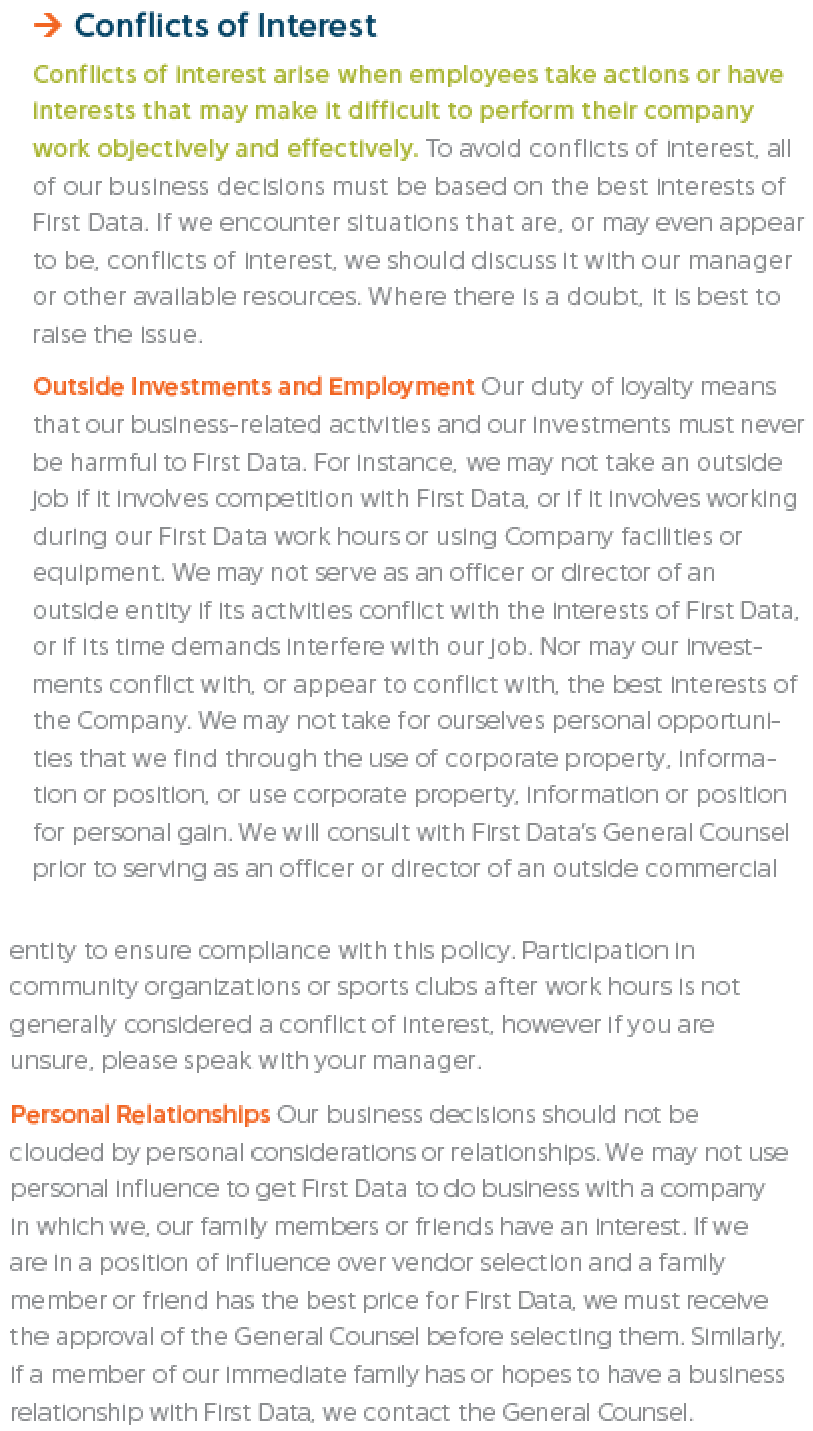
→ Customer Privacy

We are committed to protecting the privacy of individually identifiable personal information that we receive or process while providing services to our clients ("Personal Information"). We collect, use and share Personal Information in accordance with our client contracts and the privacy laws that apply to us. In addition, we adhere to the First Data Corporation Privacy Principles, including the following:



- We obtain Personal Information only as necessary to provide our services.
- We limit access to, and use of, Personal Information to those employees who need to access the data in order to carry out their job responsibilities. We will not access or use Personal Information for any personal reasons.
- We share Personal Information only in limited circumstances related to our business, or as required by law.
- We use reasonable technical, administrative and physical security measures to protect Personal Information, and will call the designated corporate hotline to report any unauthorized access, disclosure, alteration or destruction of Personal Information.
- In businesses where it applies, we provide consumer notice, transparency, choice and access as required by law.
- We hold ourselves accountable to our Privacy Principles.

First Data is known and trusted by businesses and customers around the world. We must continue to earn this trust every day, "one transaction at a time."



→ Conflicts of Interest

Conflicts of interest arise when employees take actions or have interests that may make it difficult to perform their company work objectively and effectively. To avoid conflicts of interest, all of our business decisions must be based on the best interests of First Data. If we encounter situations that are, or may even appear to be, conflicts of interest, we should discuss it with our manager or other available resources. Where there is a doubt, it is best to raise the issue.

Outside Investments and Employment Our duty of loyalty means that our business-related activities and our investments must never be harmful to First Data. For instance, we may not take an outside job if it involves competition with First Data, or if it involves working during our First Data work hours or using Company facilities or equipment. We may not serve as an officer or director of an outside entity if its activities conflict with the interests of First Data, or if its time demands interfere with our job. Nor may our investments conflict with, or appear to conflict with, the best interests of the Company. We may not take for ourselves personal opportunities that we find through the use of corporate property, information or position, or use corporate property, information or position for personal gain. We will consult with First Data's General Counsel prior to serving as an officer or director of an outside commercial entity to ensure compliance with this policy. Participation in community organizations or sports clubs after work hours is not generally considered a conflict of interest, however if you are unsure, please speak with your manager.

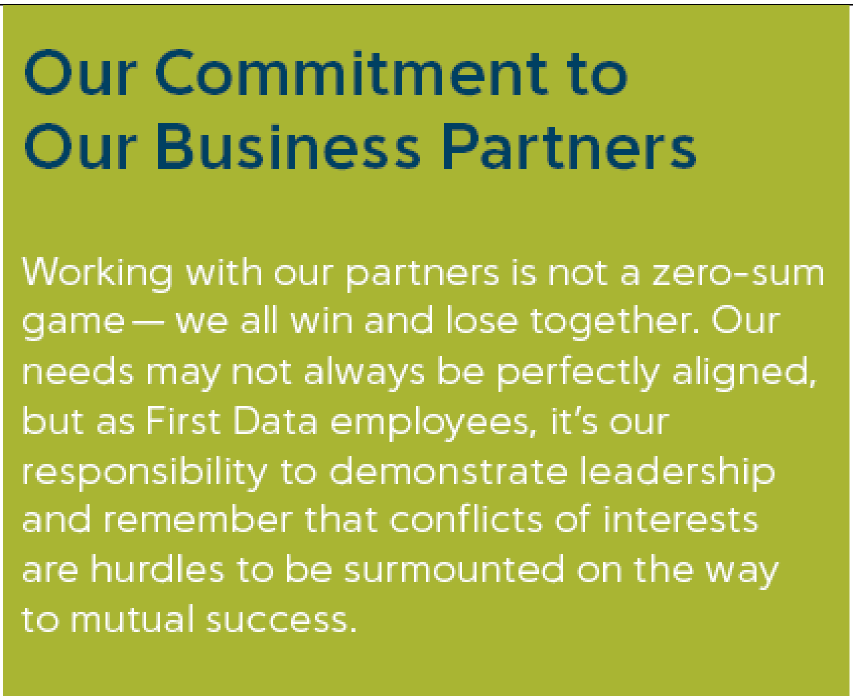
Personal Relationships Our business decisions should not be clouded by personal considerations or relationships. We may not use personal influence to get First Data to do business with a company in which we, our family members or friends have an interest. If we are in a position of influence over vendor selection and a family member or friend has the best price for First Data, we must receive the approval of the General Counsel before selecting them. Similarly, if a member of our immediate family has or hopes to have a business relationship with First Data, we contact the General Counsel.

Gifts and Entertainment

The giving and receiving of gifts and entertainment can sometimes be meant as a business courtesy to help build business relationships. However, providing and receiving gifts and entertainment can be tricky. On the one hand, human interaction is not only essential for doing business, it is valuable and healthy for both the Company and employees. Small tokens of appreciation and social gatherings are often a part of business interaction. On the other hand, the personal relationships we may form must not make us lose sight of the fact that our business decisions must be based only on what is best for the shareholders. Providing and receiving gifts and entertainment is not prohibited at First Data, but they must be moderate and reasonable in all instances. We never accept, provide or offer kickbacks, bribes or gratuities.

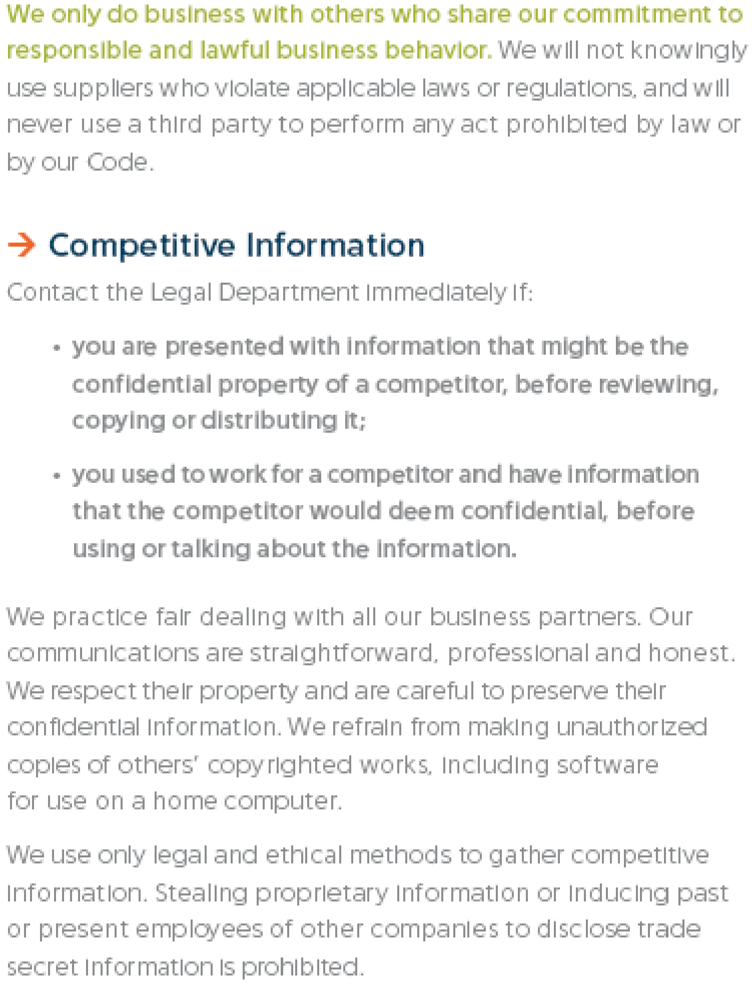
Receiving Gifts and Entertainment Entertainment is permissible as long as it is reasonable, occasional and disclosed to local management. We may accept gifts of nominal value, such as promotional items, as long as it does not create the appearance that our judgment may be compromised. Nominal value is generally considered to be less than $100 USD, or its equivalent in other currencies. However, accepting gifts of cash in any amount is prohibited. Requesting or soliciting personal gifts, favors or entertainment is also prohibited. If we are in a situation where it would be uncomfortable or insulting to refuse a gift that is of more than nominal value, we may accept it, however to ensure that the gift is properly donated to charity or shared among co-workers, our supervisor should be promptly informed.

Providing Gifts and Entertainment If we wish to give a gift, or provide entertainment, we must first make sure that it is okay to do so under the local law and policy of the recipient. We never give anything to a government official or representative, unless the Legal Department has cleared it in advance (see more on this in the section on Our Commitment to Our Communities).



Our Commitment to Our Business Partners

Working with our partners is not a zero-sum game — we all win and lose together. Our needs may not always be perfectly aligned, but as First Data employees, it's our responsibility to demonstrate leadership and remember that conflicts of interests are hurdles to be surmounted on the way to mutual success.



We only do business with others who share our commitment to responsible and lawful business behavior. We will not knowingly use suppliers who violate applicable laws or regulations, and will never use a third party to perform any act prohibited by law or by our Code.

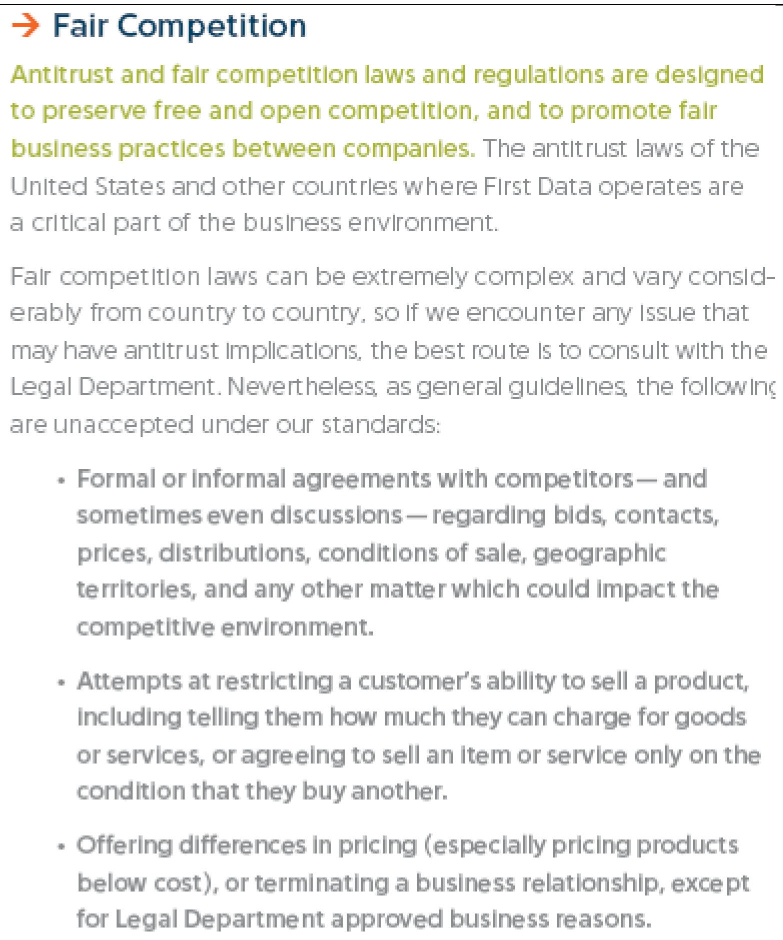
Competitive Information

Contact the Legal Department immediately if:

- **you are presented with information that might be the confidential property of a competitor, before reviewing, copying or distributing it;**
- **you used to work for a competitor and have information that the competitor would deem confidential, before using or talking about the information.**

We practice fair dealing with all our business partners. Our communications are straightforward, professional and honest. We respect their property and are careful to preserve their confidential information. We refrain from making unauthorized copies of others' copyrighted works, including software for use on a home computer.

We use only legal and ethical methods to gather competitive information. Stealing proprietary information or inducing past or present employees of other companies to disclose trade secret information is prohibited.



→ Fair Competition

Antitrust and fair competition laws and regulations are designed to preserve free and open competition, and to promote fair business practices between companies. The antitrust laws of the United States and other countries where First Data operates are a critical part of the business environment.

Fair competition laws can be extremely complex and vary considerably from country to country, so if we encounter any issue that may have antitrust implications, the best route is to consult with the Legal Department. Nevertheless, as general guidelines, the following are unaccepted under our standards:

- **Formal or informal agreements with competitors — and sometimes even discussions — regarding bids, contacts, prices, distributions, conditions of sale, geographic territories, and any other matter which could impact the competitive environment.**
- **Attempts at restricting a customer's ability to sell a product, including telling them how much they can charge for goods or services, or agreeing to sell an item or service only on the condition that they buy another.**
- **Offering differences in pricing (especially pricing products below cost), or terminating a business relationship, except for Legal Department approved business reasons.**

Our Commitment to Our Communities

First Data does not exist in a vacuum — we're a member of the community. The dedication we expect from each other should extend to our families, our neighbors and our civic institutions. The law of the land should guide our interactions in this regard and ensure that First Data remains an upstanding corporate citizen.

→ Complying with the Law

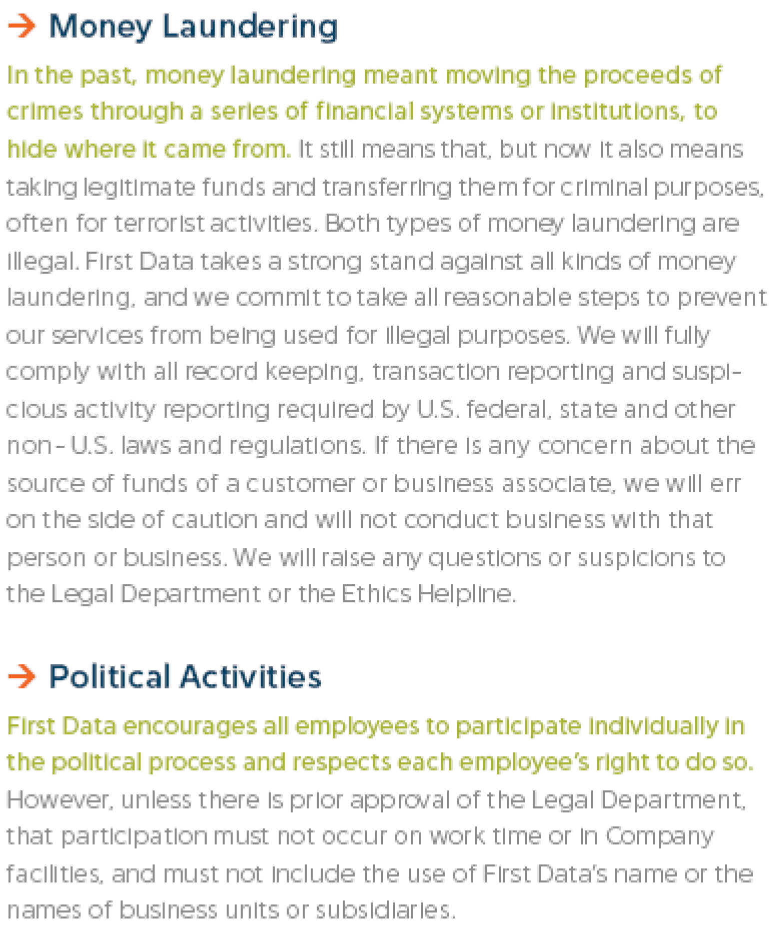
The fundamental obligation that we owe to the communities in which we do business is to obey the law. We adhere to all applicable laws everywhere we do business. There is no business excuse, no supervisory pressure, no unwritten understanding that justifies violating the law. If we ever feel pressured to violate a law, we immediately contact the Legal Department or the Ethics Helpline. While this requirement refers to all applicable laws, a few areas deserve special mention.

→ Anti-Corruption/Anti-Bribery Laws

First Data is a global organization and complies with all applicable anti-bribery laws, including, the U.S. Foreign Corrupt Practices Act, and others. These laws make it illegal to provide or offer something of value to government officials in order to improperly influence their acts or decisions. If we are asked to make any improper payments, including facilitating payments (small payments given in exchange for performing routine governmental functions), we contact the Legal Department immediately.

→ Insider Trading—Prohibited Activities

We may not use information that we receive as a result of working at First Data to influence our decision to buy or sell shares of First Data stock. This prohibition also includes stock of another company, such as a customer or supplier, about whom we receive confidential information as a result of our First Data employment.

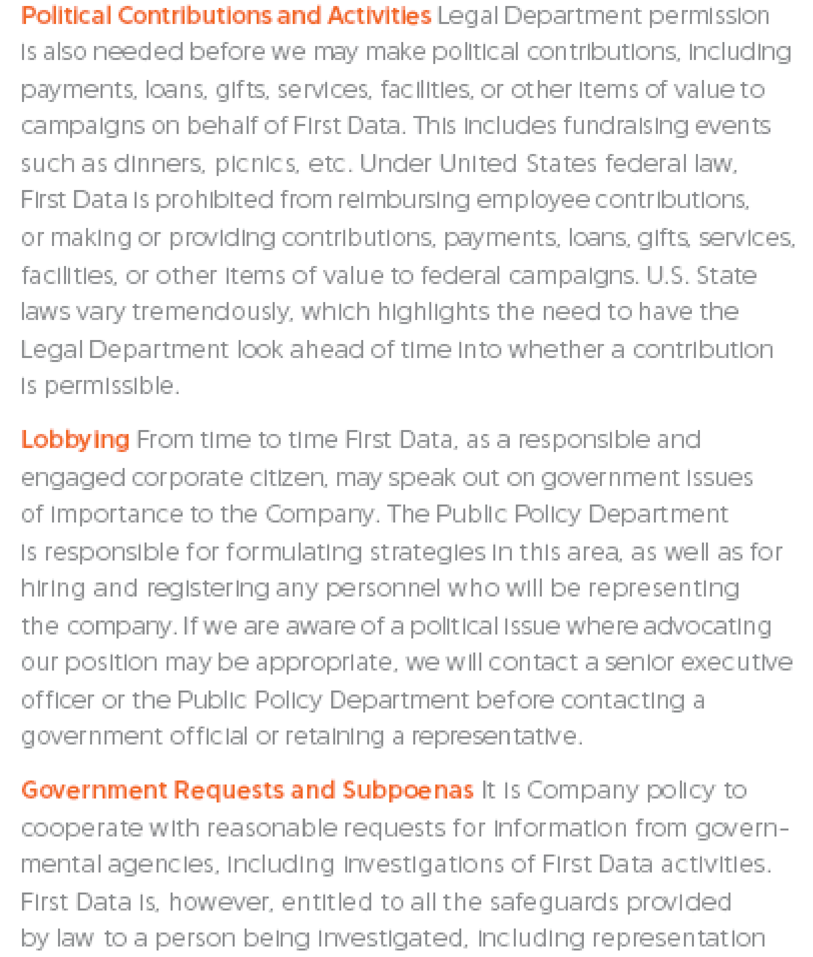


Money Laundering

In the past, money laundering meant moving the proceeds of crimes through a series of financial systems or institutions, to hide where it came from. It still means that, but now it also means taking legitimate funds and transferring them for criminal purposes, often for terrorist activities. Both types of money laundering are illegal. First Data takes a strong stand against all kinds of money laundering, and we commit to take all reasonable steps to prevent our services from being used for illegal purposes. We will fully comply with all record keeping, transaction reporting and suspicious activity reporting required by U.S. federal, state and other non-U.S. laws and regulations. If there is any concern about the source of funds of a customer or business associate, we will err on the side of caution and will not conduct business with that person or business. We will raise any questions or suspicions to the Legal Department or the Ethics Helpline.

Political Activities

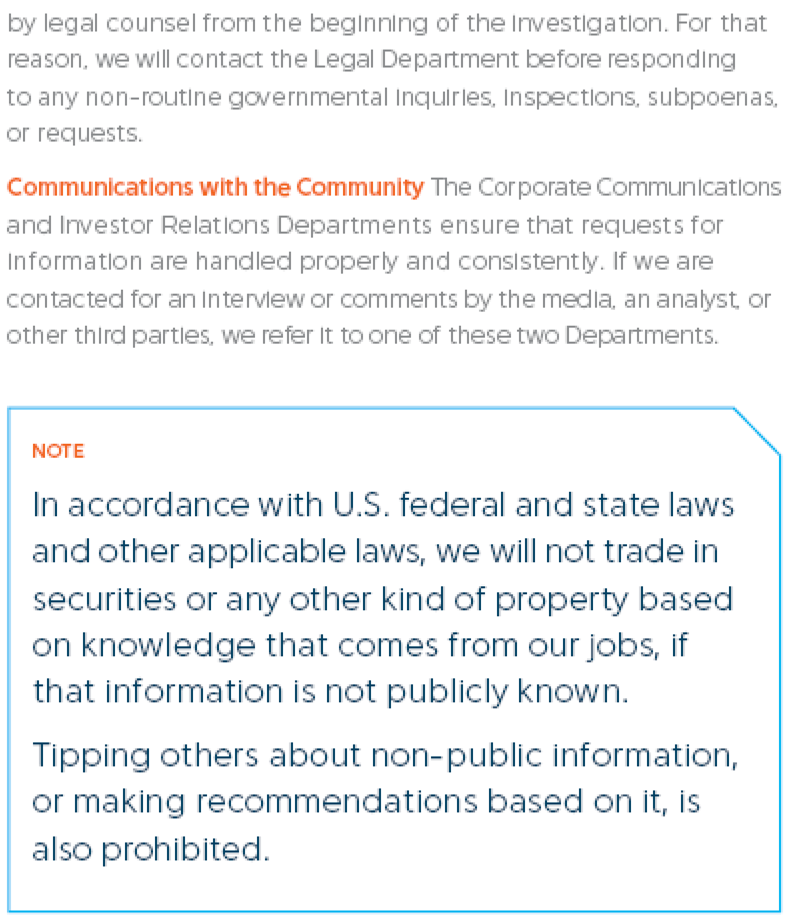
First Data encourages all employees to participate individually in the political process and respects each employee's right to do so. However, unless there is prior approval of the Legal Department, that participation must not occur on work time or in Company facilities, and must not include the use of First Data's name or the names of business units or subsidiaries.



Political Contributions and Activities Legal Department permission is also needed before we may make political contributions, including payments, loans, gifts, services, facilities, or other items of value to campaigns on behalf of First Data. This includes fundraising events such as dinners, picnics, etc. Under United States federal law, First Data is prohibited from reimbursing employee contributions, or making or providing contributions, payments, loans, gifts, services, facilities, or other items of value to federal campaigns. U.S. State laws vary tremendously, which highlights the need to have the Legal Department look ahead of time into whether a contribution is permissible.

Lobbying From time to time First Data, as a responsible and engaged corporate citizen, may speak out on government issues of importance to the Company. The Public Policy Department is responsible for formulating strategies in this area, as well as for hiring and registering any personnel who will be representing the company. If we are aware of a political issue where advocating our position may be appropriate, we will contact a senior executive officer or the Public Policy Department before contacting a government official or retaining a representative.

Government Requests and Subpoenas It is Company policy to cooperate with reasonable requests for information from governmental agencies, including investigations of First Data activities. First Data is, however, entitled to all the safeguards provided by law to a person being investigated, including representation



by legal counsel from the beginning of the investigation. For that reason, we will contact the Legal Department before responding to any non-routine governmental inquiries, inspections, subpoenas, or requests.

Communications with the Community The Corporate Communications and Investor Relations Departments ensure that requests for information are handled properly and consistently. If we are contacted for an interview or comments by the media, an analyst, or other third parties, we refer it to one of these two Departments.

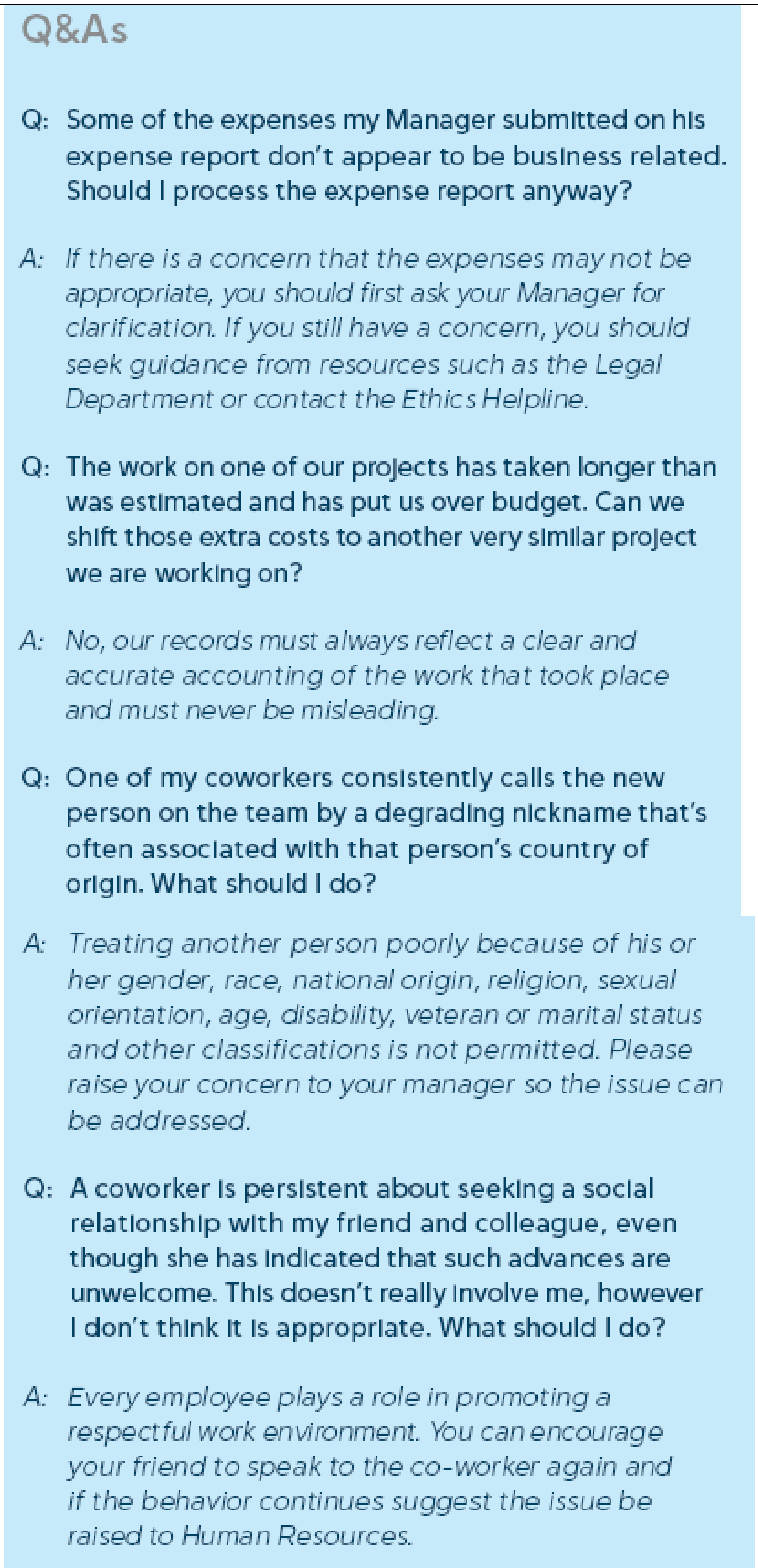
NOTE

In accordance with U.S. federal and state laws and other applicable laws, we will not trade in securities or any other kind of property based on knowledge that comes from our jobs, if that information is not publicly known.

Tipping others about non-public information, or making recommendations based on it, is also prohibited.

Resources and Certification

Just as we rely on each other to build a lasting and successful organization, so we also need to rely on each other for help in maintaining our commitment to doing the right thing. The following section features key resources all of us can turn to, and a final certification of our personal commitment.



Q&As

Q: Some of the expenses my Manager submitted on his expense report don't appear to be business related. Should I process the expense report anyway?

A: *If there is a concern that the expenses may not be appropriate, you should first ask your Manager for clarification. If you still have a concern, you should seek guidance from resources such as the Legal Department or contact the Ethics Helpline.*

Q: The work on one of our projects has taken longer than was estimated and has put us over budget. Can we shift those extra costs to another very similar project we are working on?

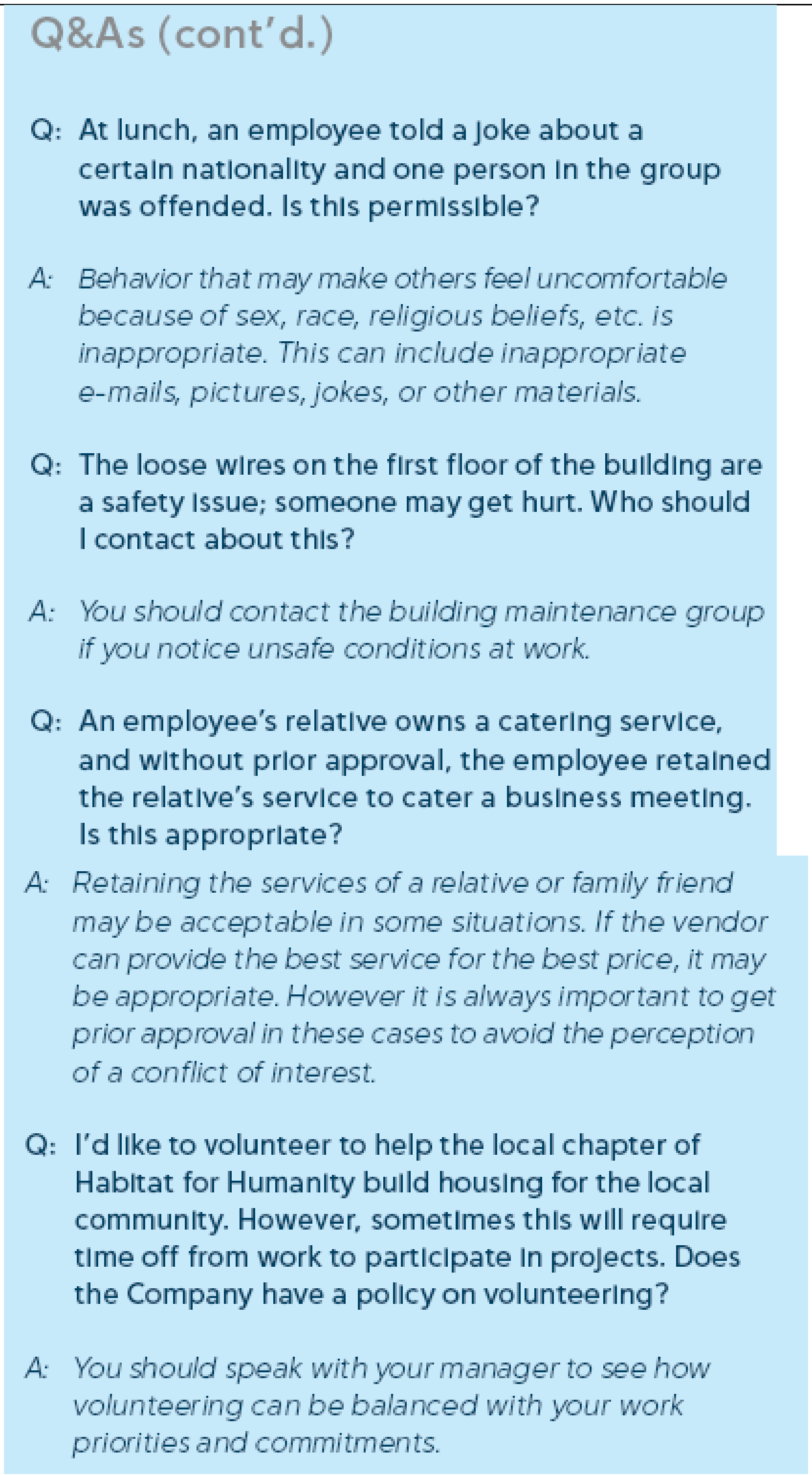
A: *No, our records must always reflect a clear and accurate accounting of the work that took place and must never be misleading.*

Q: One of my coworkers consistently calls the new person on the team by a degrading nickname that's often associated with that person's country of origin. What should I do?

A: *Treating another person poorly because of his or her gender, race, national origin, religion, sexual orientation, age, disability, veteran or marital status and other classifications is not permitted. Please raise your concern to your manager so the issue can be addressed.*

Q: A coworker is persistent about seeking a social relationship with my friend and colleague, even though she has indicated that such advances are unwelcome. This doesn't really involve me, however I don't think it is appropriate. What should I do?

A: *Every employee plays a role in promoting a respectful work environment. You can encourage your friend to speak to the co-worker again and if the behavior continues suggest the issue be raised to Human Resources.*



Q&As (cont'd.)

Q: At lunch, an employee told a joke about a certain nationality and one person in the group was offended. Is this permissible?

A: *Behavior that may make others feel uncomfortable because of sex, race, religious beliefs, etc. is inappropriate. This can include inappropriate e-mails, pictures, jokes, or other materials.*

Q: The loose wires on the first floor of the building are a safety issue; someone may get hurt. Who should I contact about this?

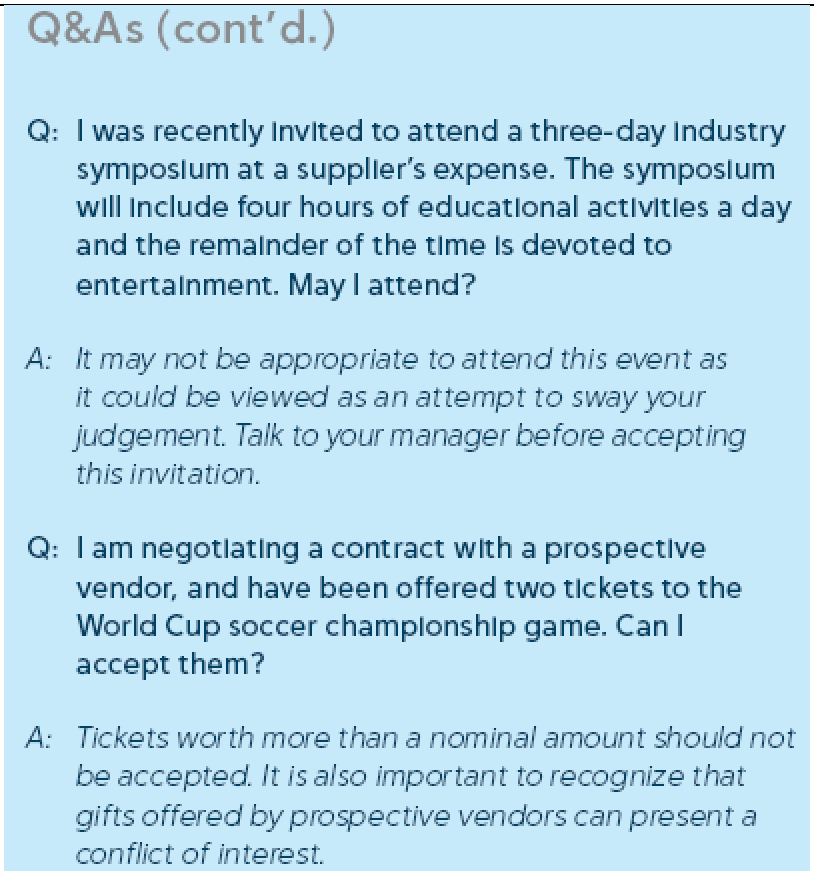
A: *You should contact the building maintenance group if you notice unsafe conditions at work.*

Q: An employee's relative owns a catering service, and without prior approval, the employee retained the relative's service to cater a business meeting. Is this appropriate?

A: *Retaining the services of a relative or family friend may be acceptable in some situations. If the vendor can provide the best service for the best price, it may be appropriate. However it is always important to get prior approval in these cases to avoid the perception of a conflict of interest.*

Q: I'd like to volunteer to help the local chapter of Habitat for Humanity build housing for the local community. However, sometimes this will require time off from work to participate in projects. Does the Company have a policy on volunteering?

A: *You should speak with your manager to see how volunteering can be balanced with your work priorities and commitments.*



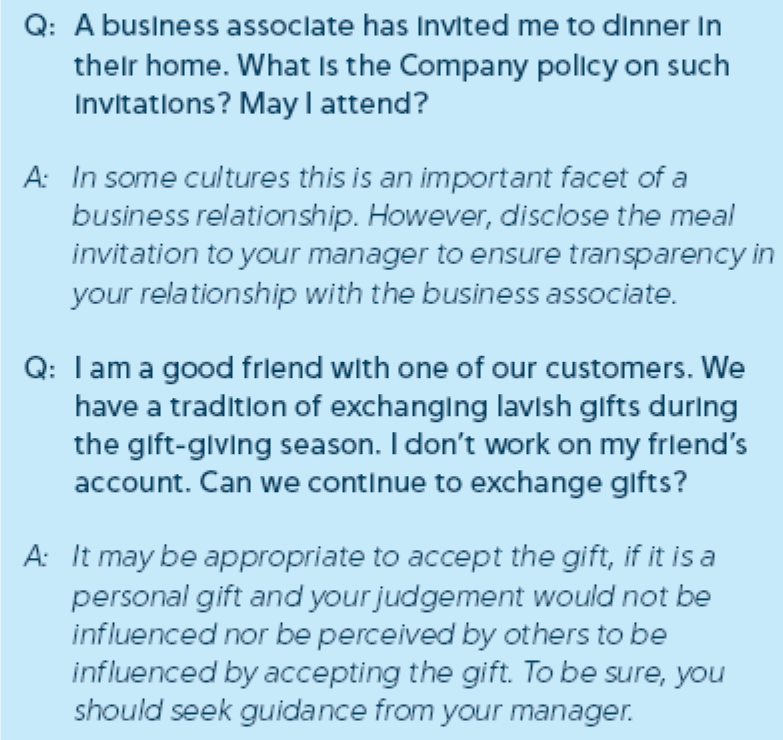
Q&As (cont'd.)

Q: I was recently invited to attend a three-day industry symposium at a supplier's expense. The symposium will include four hours of educational activities a day and the remainder of the time is devoted to entertainment. May I attend?

A: *It may not be appropriate to attend this event as it could be viewed as an attempt to sway your judgement. Talk to your manager before accepting this invitation.*

Q: I am negotiating a contract with a prospective vendor, and have been offered two tickets to the World Cup soccer championship game. Can I accept them?

A: *Tickets worth more than a nominal amount should not be accepted. It is also important to recognize that gifts offered by prospective vendors can present a conflict of interest.*

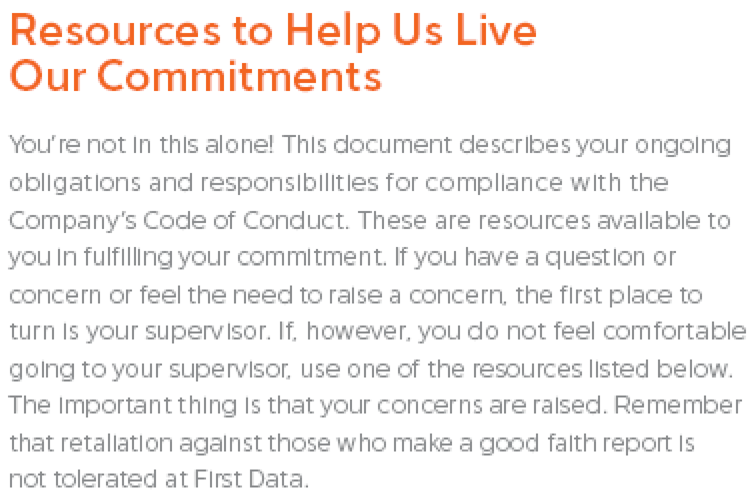


Q: A business associate has invited me to dinner in their home. What is the Company policy on such invitations? May I attend?

A: *In some cultures this is an important facet of a business relationship. However, disclose the meal invitation to your manager to ensure transparency in your relationship with the business associate.*

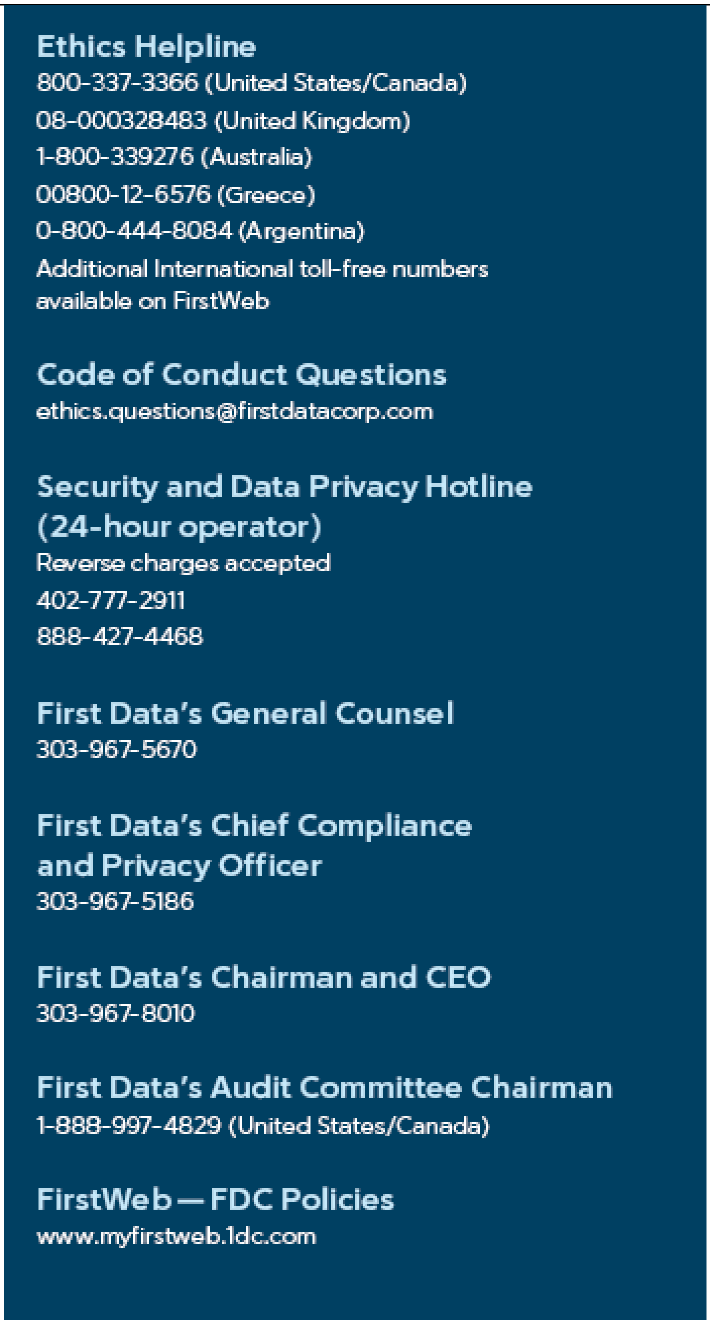
Q: I am a good friend with one of our customers. We have a tradition of exchanging lavish gifts during the gift-giving season. I don't work on my friend's account. Can we continue to exchange gifts?

A: *It may be appropriate to accept the gift, if it is a personal gift and your judgement would not be influenced nor be perceived by others to be influenced by accepting the gift. To be sure, you should seek guidance from your manager.*



Resources to Help Us Live Our Commitments

You're not in this alone! This document describes your ongoing obligations and responsibilities for compliance with the Company's Code of Conduct. These are resources available to you in fulfilling your commitment. If you have a question or concern or feel the need to raise a concern, the first place to turn is your supervisor. If, however, you do not feel comfortable going to your supervisor, use one of the resources listed below. The important thing is that your concerns are raised. Remember that retaliation against those who make a good faith report is not tolerated at First Data.



Ethics Helpline

800-337-3366 (United States/Canada)

08-000328483 (United Kingdom)

1-800-339276 (Australia)

00800-12-6576 (Greece)

0-800-444-8084 (Argentina)

Additional International toll-free numbers available on FirstWeb

Code of Conduct Questions

ethics.questions@firstdatacorp.com

Security and Data Privacy Hotline (24-hour operator)

Reverse charges accepted

402-777-2911

888-427-4468

First Data's General Counsel

303-967-5670

First Data's Chief Compliance and Privacy Officer

303-967-5186

First Data's Chairman and CEO

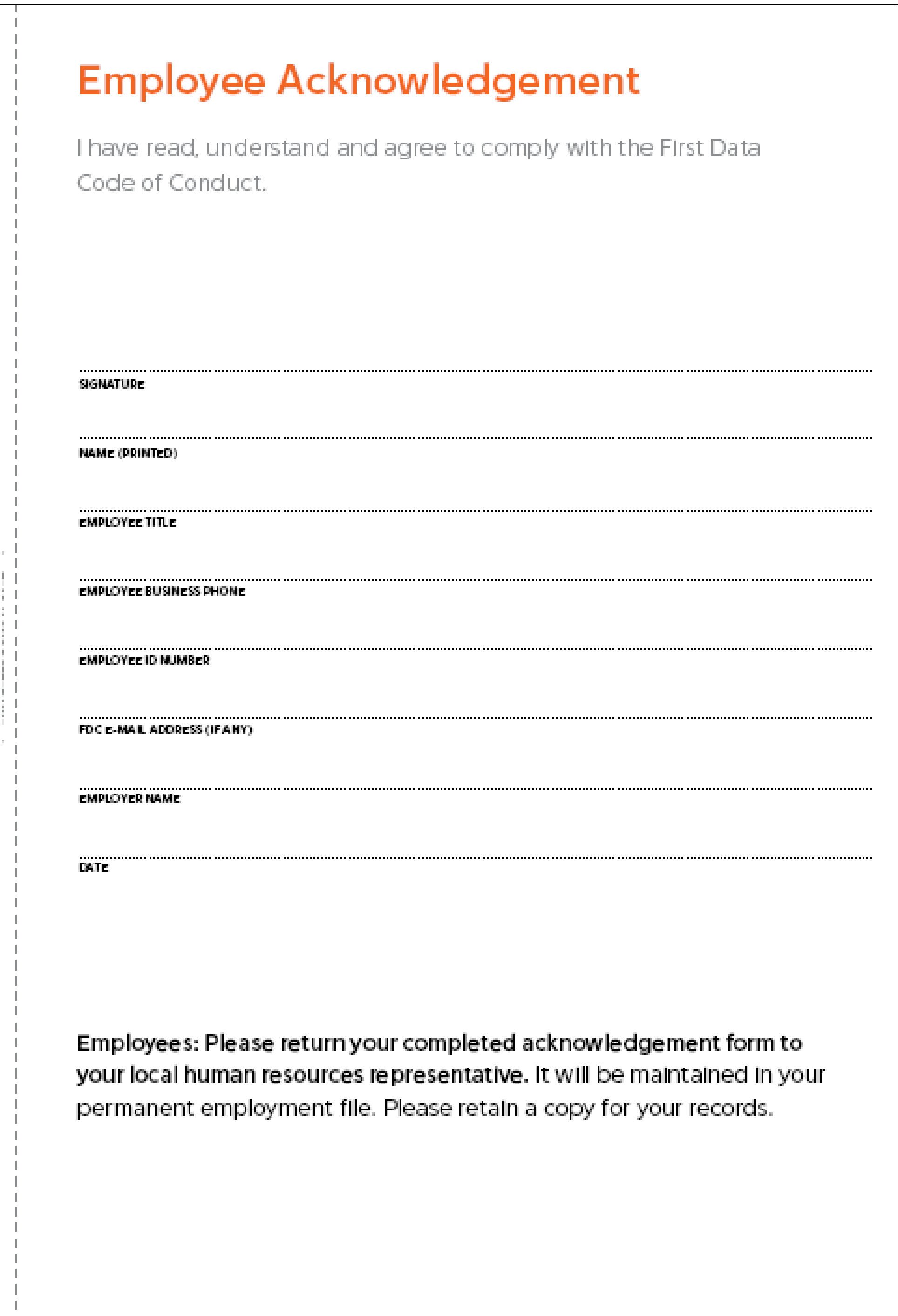
303-967-8010

First Data's Audit Committee Chairman

1-888-997-4829 (United States/Canada)

FirstWeb — FDC Policies

www.myfirstweb.1dc.com



Employee Acknowledgement

I have read, understand and agree to comply with the First Data Code of Conduct.

....

SIGNATURe

....

NAMe (PRINTeD)

....

eMPLOYee TITLe

....

eMPLOYee BUSINeSS PHONe

....

eMPLOYee ID NUMBeR

....

FDC e-MAIL ADDReSS (IF ANY)

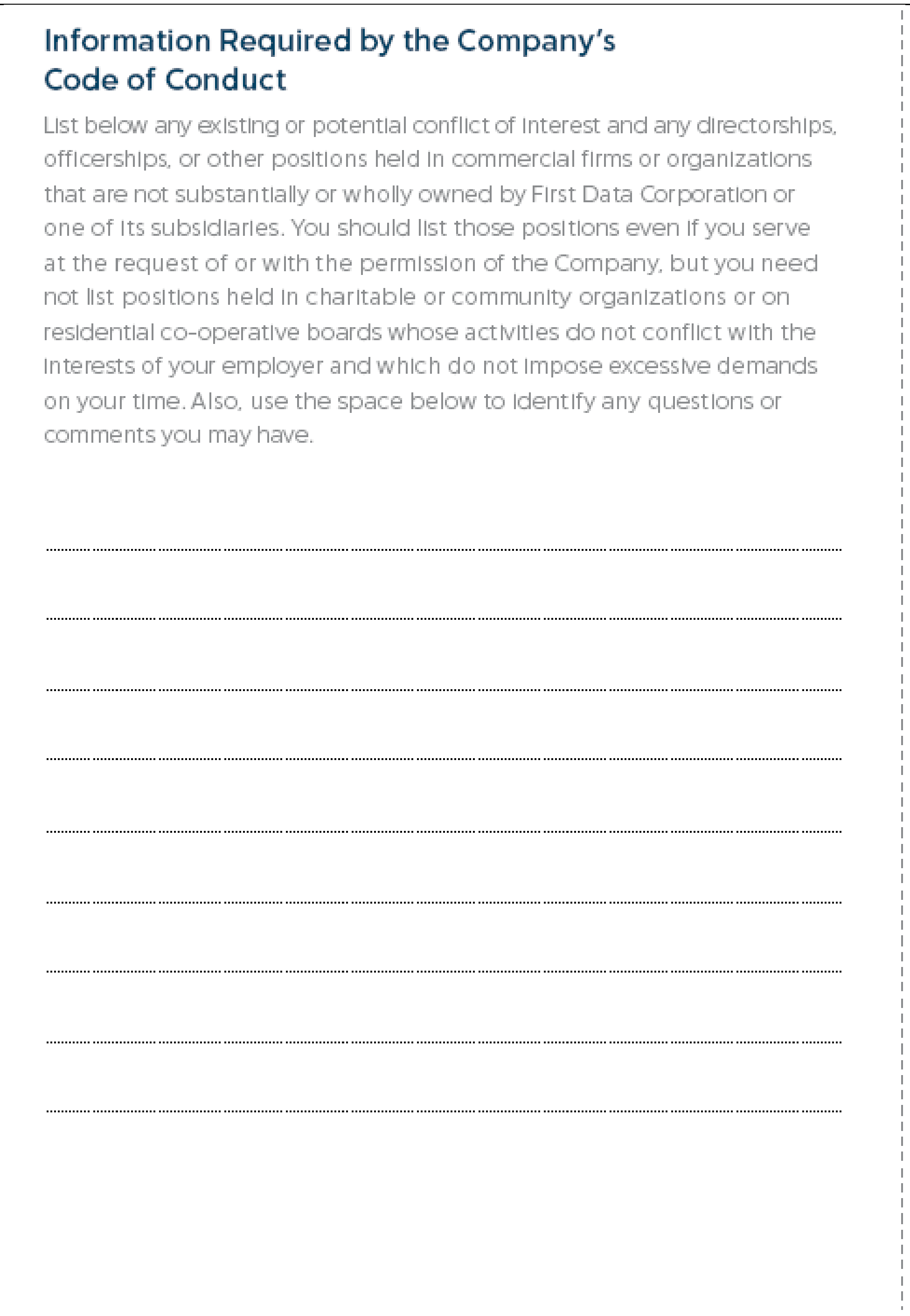
....

eMPLOYeR NAMe

....

DATe

Employees: Please return your completed acknowledgement form to your local human resources representative. It will be maintained in your permanent employment file. Please retain a copy for your records.



Information Required by the Company's Code of Conduct

List below any existing or potential conflict of interest and any directorships, officerships, or other positions held in commercial firms or organizations that are not substantially or wholly owned by First Data Corporation or one of its subsidiaries. You should list those positions even if you serve at the request of or with the permission of the Company, but you need not list positions held in charitable or community organizations or on residential co-operative boards whose activities do not conflict with the interests of your employer and which do not impose excessive demands on your time. Also, use the space below to identify any questions or comments you may have.