STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**
to
Contract Number **MA220000001254**

CONTRACTOR	
	FIRST DATA GOVERNMENT SOLUTIONS LP
	255 Fiserv Dr.
	Brookfield WI 53045
	Jason Clark
	513-207-5265
	JasonW.Clark@Fiserv.com
	CV0060377

STATE			
	Program Manager	Various	Various
	Contract Administrator	Brandon Samuel	DTMB
		517-249-0439	
		samuelb@michigan.gov	

CONTRACT SUMMARY			
Centralized Electronic Payment Authorization System (CEPAS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
August 1, 2022	June 30, 2026	5 - 12 Months	June 30, 2028
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
ALTERNATE PAYMENT OPTIONS		**EXTENDED PURCHASING**	
☐ P-Card ☐ Direct Voucher (PRC) ☐ Other		☒ Yes ☐ No	
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☐		☐		
CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**		
$9,700,000.00	$0.00	$9,700,000.00		

DESCRIPTION

Effective December 20, 2024, the Contractor Contract Administrator has changed from Leon Fox to Jason Clark (513-207-5265; JasonW.Clark@Fiserv.com; 600 N Vel R. Phillips Ave - Milwaukee, WI 53203)

Additionally, the State Contract Administrator has changed from Patrick Russel to Brandon Samuel.

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

Program Managers

for

Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Lucy Pline	517-636-5052	plinel@michigan.gov
TREA	Amy Kelso	517-636-5372	kelsoa@michigan.gov

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
320 S. WALNUT ST., LANSING, MICHIGAN 4893
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**

to

Contract Number **220000001254**

CONTRACTOR	
	FIRST DATA GOVERNMENT SOLUTIONS LP
	255 Fiserv Dr.
	Brookfield, WI 53045
	Leon Fox
	689-244-7377
	leon.fox@fiserv.com
	CV0060377

STATE			
	Program Manager	Various	TREA
	Contract Administrator	Patrick Russell	DTMB
		(517) 648-7767	
		russellp2@michigan.gov	

CONTRACT SUMMARY			
CENTRALIZED ELECTRONIC PAYMENT AUTHORIZATION SYSTEM (CEPAS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
August 1, 2022	June 30, 2026	5 - 1 Year	June 30, 2026
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	☐		June 30, 2028
CURRENT VALUE	**VALUE OF CHANGE NOTICE**		**ESTIMATED AGGREGATE CONTRACT VALUE**	
$7,900,000.00	$1,800,000.00		$9,700,000.00	

DESCRIPTION

Effective 11/28/2023, this contract is exercising 2- 1 year option and is increased by $1,800,000.00, the revised contract expiration date is 6/30/2028.

All other terms, conditions, specifications, and pricing remain the same. Per contractor and agency agreement, DTMB Central Procurement Services approval, and State Administrative Board approval on 11/28/2023.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Lucy Pline	517-636-5052	plinel@michigan.gov
TREA	Amy Kelso	517-636-5372	kelsoa@michigan.gov

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
320 S. WALNUT ST., LANSING, MICHIGAN 4893
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**

to

Contract Number **220000001254**

CONTRACTOR	
	FIRST DATA GOVERNMENT SOLUTIONS LP
	255 Fiserv Dr.
	Brookfield, WI 53045
	Leon Fox
	689-244-7377
	leon.fox@fiserv.com
	CV0060377

STATE			
	Program Manager	Various	TREA
	Contract Administrator	Patrick Russell	DTMB
		(517) 648-7767	
		russellp2@michigan.gov	

CONTRACT SUMMARY			
CENTRALIZED ELECTRONIC PAYMENT AUTHORIZATION SYSTEM (CEPAS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
August 1, 2022	June 30, 2026	5 - 1 Year	June 30, 2026
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, 2026
CURRENT VALUE	**VALUE OF CHANGE NOTICE**		**ESTIMATED AGGREGATE CONTRACT VALUE**	
$7,840,000.00	$60,000.00		$7,900,000.00	

DESCRIPTION

Effective 9/16/2023, adding funds of $60,000.00. Adding updated Schedule B – Pricing and Schedule J – Fraud Detect Schedule.

Please note the Contract Administrator has been changed to Patrick Russell.

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

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Lucy Pline	517-636-5052	plinel@michigan.gov
TREA	Amy Kelso	517-636-5372	kelsoa@michigan.gov

SCHEDULE B – PRICING

Compensation and Payment

A. **Firm Pricing:** All prices will be firm for the term of the Contract. If the Contract is extended beyond the initial term of the Contract, the State and the Contractor may negotiate price.

B. **Unit Price Contract:** This is 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 (with the exclusion of NACHA or card association passthrough fees):

- an authorization
- an ACH return
- communication failures
- errors
- chargebacks
- duplicate transactions attributable to the Contractor
- refunds of duplicate transactions attributable to the Contractor

C. Pricing

Transaction Fee Pricing: The transaction fees include all costs for providing the system defined in the Statement of Work. The State expects volume discounts in the transaction fee pricing based on a monthly review of the transaction volume processed

Bank of Hours: This bank of 1000 hours is to be used for customized enhancements that the State may request.

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). The 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 also must 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, Office of Financial Services Division.

<table>
<tr><th>Billing #</th><th>Element</th><th>Description</th><th>Price (USD $)</th><th>Per Unit</th></tr>
<tr><td>5243</td><td>GATEWAY FEES FOR CARD TRANSACTIONS</td><td>This element identifies the charge for processing PayPoint transaction for One-time Card transactions and Recurring Card Transactions.</td><td><table><tr><th>Unit Price</th><th>Range of Monthly Transactions</th></tr><tr><td>0.150</td><td>0 - 150,000</td></tr><tr><td>0.140</td><td>150,001 - 250,000</td></tr><tr><td>0.130</td><td>250,001 - 300,000</td></tr><tr><td>0.130</td><td>300,001 - 350,000</td></tr><tr><td>0.120</td><td>350,001 - 400,000</td></tr><tr><td>0.110</td><td>400,001 - 450,000</td></tr><tr><td>0.095</td><td>450,001 - 500,000</td></tr><tr><td>0.095</td><td>500,001 - 550,000</td></tr><tr><td>0.085</td><td>550,001 - 600,000</td></tr><tr><td>0.085</td><td>600,001 - 650,000</td></tr><tr><td>0.080</td><td>650,001 - 700,000</td></tr><tr><td>0.080</td><td>700,001 - 750,000</td></tr><tr><td>0.080</td><td>750,001 - 800,000</td></tr><tr><td>0.080</td><td>800,001 - 850,000</td></tr><tr><td>0.080</td><td>850,001 - 900,000</td></tr><tr><td>0.080</td><td>900,001 - 950,000</td></tr><tr><td>0.080</td><td>950,001 - 1,000,000</td></tr></table>
Note: Transactions for Element 5243 only are Pick the Tier above.</td><td>/transaction</td></tr>
<tr><td>5245</td><td>GATEWAY FEES FOR ACH TRANSACTIONS
(With TeleCheck ACH processing)</td><td>This element identifies the charge for processing One-Time eCheck Transactions and Recurring eCheck Transactions.

This includes successful, declined, and cancelled eCheck payments with standard eCheck processing.

Standard eCheck processing includes basic processing through TeleCheck. Additional TeleCheck services are priced and contracted separately.

For applications that charge convenience fees separately, two transaction fees will be incurred- one for the primary payment and a separate fee for the convenience fee.</td><td><table><tr><th>Unit Price</th><th>Range of Monthly Transactions</th></tr><tr><td>0.150</td><td>0 - 150,000</td></tr><tr><td>0.140</td><td>150, 001 - 250,000</td></tr><tr><td>0.130</td><td>250,001 - 300,000</td></tr><tr><td>0.130</td><td>300,001 - 350,000</td></tr><tr><td>0.120</td><td>350,001 - 400,000</td></tr><tr><td>0.110</td><td>400,001 - 450,000</td></tr><tr><td>0.095</td><td>450,001 - 500,000</td></tr><tr><td>0.095</td><td>500,001 - 550,000</td></tr><tr><td>0.085</td><td>550,001 - 600,000</td></tr><tr><td>0.085</td><td>600,001 - 650,000</td></tr><tr><td>0.080</td><td>650,001 - 700,000</td></tr><tr><td>0.080</td><td>700,001 - 750,000</td></tr><tr><td>0.080</td><td>750,001 - 800,000</td></tr><tr><td>0.080</td><td>800,001 - 850,000</td></tr><tr><td>0.080</td><td>850,001 - 900,000</td></tr><tr><td>0.080</td><td>900,001 - 950,000</td></tr><tr><td>0.080</td><td>950,001 - 1,000,000</td></tr></table>
Note: Transactions for Element 5245 only are Pick the Tier above.</td><td>/transaction</td></tr>
<tr><td></td><td>ACH Validation for NACHA Web Debit Rule</td><td></td><td>0.05</td><td>/transaction</td></tr>
<tr><td>5246</td><td>CONSUMER PAYMENTS</td><td>This element identifies the per transaction surcharge for a payment using Consumer</td><td>0.07</td><td>/transaction</td></tr>
</table>

<table>
<tr><td></td><td></td><td>Payments Web in addition to the Gateway Fees.

Excludes applications that “redirect” to Consumer Web pages.</td><td></td><td></td></tr>
<tr><td>5247</td><td>CONSUMER PAYMENTS SUMMARY PRESENTMENT</td><td>This element identifies the per transaction surcharge to use summary presentment feature – includes uploading summary billing data and displaying it to a consumer using the Consumer Payments interface in addition to the Gateway Fees.</td><td>0.07</td><td>/transaction</td></tr>
<tr><td>5244</td><td>IVR MINUTES</td><td>This element identifies the charge for telecommunication fees for using Consumer Payments IVR.</td><td>0.10</td><td>/transaction</td></tr>
<tr><td>5249</td><td>DEVELOPMENT SURCHARGE</td><td>This element identifies the custom project charges, including but not limited to: consultation, project management, development, and testing. Custom projects beyond the scope of standard initial onboarding will be quoted separately.</td><td>150/hour</td><td>One-time</td></tr>
<tr><td>5275</td><td>NACHA UNAUTHORIZED RETURN FEES</td><td>This element applies only to Clients who use PayPoint/TeleCheck services and identifies the charge for each eCheck return received for one of the following NACHA Unauthorized Return Codes:
<table><tr><th>Return Code</th><th>Return Description</th></tr><tr><td>R05</td><td>REQUIRED PRENOTIFICATION NOT RECEIVED</td></tr><tr><td>R07</td><td>AUTHORIZATION REVOKED BY CUSTOMER</td></tr><tr><td>R10</td><td>CUSTOMER ADVISES NOT AUTHORIZED</td></tr><tr><td>R29</td><td>CORPORATE CUSTOMER ADVISES NOT AUTH</td></tr><tr><td>R51</td><td>ITEM IS INELIGIBLE, NOTICE NOT PROVIDED, SIGNATURE NOT GENUINE</td></tr></table></td><td>5.00</td><td>/eCheck Return</td></tr>
</table>

	FRAUD DETECT SERVICES	The State will not be assessed any gateway fees for card transactions that are declined through the State's receipt of the Fraud Detect solution and such transactions shall not be counted toward the gateway fee transaction volume tiers.	**Unit Price** 0.040	Fraud Detect Transaction Event

Monthly Invoice: The Contractor must provide a monthly invoice no later than 10 calendar days of the next month.

SCHEDULE J – FRAUD DETECT SCHEDULE
Fraud Detect Schedule

This Schedule adds the Fraud Detect Services to Contract No. 171-220000001254 (**Agreement**) between First Data Government Solutions, LP (**First Data**) and the State of Michigan (**State**). The Fraud Detect Services are a Service under the Agreement.

The parties agree:

1 Fraud Detect Services

1.1 First Data will provide State with services to help identify Fraud Detect Transaction Events that are likely to be fraudulent (**Fraud Detect Services**). First Data will provide the Fraud Detect Services using (1) supervised machine learning capabilities that use and analyze State's Fraud Detect Data (defined in *Section 1.6*), including information from or about and across consumers' computers or mobile devices, and may also use similar data from other Fraud Detect Services customers in the analysis, and (2) a real-time fraud rules engine, which uses fraud rules determined in consultation with State. **Fraud Detect Transaction Events** means the digital payment transactions or card or user registrations within the United States to which the Fraud Detect Services will be applied (as indicated in the *Implementation Form*).

1.2 The Fraud Detect Services will provide State with: (1) Fraud Detect Responses, and (2) access to a **User Interface** to: (a) review each Fraud Detect Response and resolve a Fraud Detect Response, if desired, (b) obtain fraud analytics, and (c) create and obtain reporting about Fraud Detect Responses and Fraud Detect Transaction Events (report contents will vary depending on the data elements that State provides or makes available to First Data in connection with the Fraud Detect Services). **Fraud Detect Response** means a real-time automated score that consists of an "allow" or "prevent" recommendation response OR an "allow", "prevent" or "review" recommendation response, as selected by State, for each Fraud Detect Transaction Event.

1.3 The Fraud Detect Services are a fraud detection tool. The data provided to State by the Fraud Detect Services do not constitute 'consumer reports' under the Fair Credit Reporting Act (**FCRA**) (15 U.S.C. sec 1681), as amended. State may use the data provided by the Fraud Detect Services solely for purposes of detecting and preventing fraud. State certifies and agrees that it will not use the data provided by the Fraud Detect Services as a factor in establishing a consumer's eligibility for credit, insurance, employment or other FCRA purposes.

1.4 Reserved.

1.5 First Data will implement the Fraud Detect Services according to the terms of the Agreement, in addition to the selections identified in the Implementation Form substantially in the form of Exhibit A (**Implementation Form**). In addition to Contractor's responsibilities set forth in the Agreement, the Implementation Form defines the scope of the Fraud Detect Services, each party's respective implementation responsibilities, and acceptance criteria and testing timeframe for the Fraud Detect Services.

1.6 In order for First Data to provide the Fraud Detect Services, State must make available to First Data the Fraud Detect Data required by the First Data specifications applicable to the State's respective integration to the Fraud Detect Services. To the extent that the State elects to share Chargeback Data, the State will securely transmit Chargeback Data (as described below) to First Data using the format and specifications First Data provides. The State acknowledges that it will not receive the full benefit of the Fraud Detect Services if it does not provide Chargeback Data. By way of example only, without Chargeback Data, the Fraud Detect Services will not have the ability to recognize 1st and 3rd party fraud related to repeated chargebacks from the same card PAN. First Data will notify State of any changes to its data transmission format or specification requirements, which will become effective after receipt from First Data. **Fraud Detect Data** means all card or user registration, payment transaction and related ancillary data made available to the Fraud Detect Services, which may include, without limitation, the following data:

Fraud Detect Data:

Merchant Data		
Merchant ID (MID)	Merchant Category Code (MCC)	
Consumer Data		
Customer ID (unique number generated by State)	Registration time	Telephone Number
Email Address	Name	
Payment Method Data		
Card last four digits	Cardholder billing address*	Registration time
Method Type (card brand or wallet type)	Cardholder name	Instrument ID (PAN first 6 and last 4, token number or Paypal payor ID number)
Successful registration (Y/N)	Card BIN	
Order Data		
Order ID	From (location) (store fulfilling the order)*	Creation time

App platform	To (location) (ship to address)*	Price
Currency	Market (territory or brand)	State's App name
Items	Seller ID (specific State store number)	State's App domain
Item Data		
SKU	Quantity	Price
Name	Category	Currency
Transaction Data		
Transaction ID	Time	Gateway reference or ID number (generated by the gateway)
Amount	Type	
Success (Issuer approval or decline)	Gateway Name	
Location Data*		
Latitude + longitude (may be derived from street addresses and postal codes provided by State)	Postal code	Street 1+Street 2 + City +Locality+ Region + Country
Chargeback Data (First Data to provide if First Data provides acquiring services for State)		
Transaction ID (or Gateway reference)	Dispute time	Currency
Gateway	Status	
Non Fraud	Amount	
Device Data Elements Generally		
Device ID (for device used to initiate a Fraud Detect Transaction Event)	Device type (phone (Android/ios, desktop, ipad)	IP address (of device at time of Fraud Detect Transaction Event)
Session ID	Geo Location (latitude + longitude + altitude of device at time of Fraud Detect Transaction Event)	Operating System and Version
Fingerprint Source (identifier for platform submitting device data)	Time zone information (offset to UTC in hours and time zone string)	
ios/Android Device Data Elements		

Device properties (Emulator or jailbreak status (Y/N))	Device info (manufacturer, model)	Fonts installed on device
Timestamp	Android or ios ID	Customer ID
System language	Carrier information	Screen information (resolution, scale, height and width)
Carrier information (country, type, operator ID and name)	Country/Operator of SIM card	Mobile Country Code of operator
Mobile Network Code of operator	Location access status (permission granted to app)	
Browser Data Elements		
URL	Language	Color Depth
Display (pixel, resolution, available resolutions)	Does session or local storage occur (Y/N)	Browser platform
User agent	Language set by browser	Does browser support Indexed Database or Open Database (Y/N)
Do not track enabled (Y/N)	Plug Ins (name, description)	MIME types
Ad blocker software enabled (Y/N)	Spoofing (browser language, screen resolution, OS, browser)(Y/N)	Max # of touchpoints if mobile device
CPU information (class of CPU and # of cores)	Browser name	Fonts available
Does browser support Canvas or webGL APIs (Y/N)	Could a touchpoint be created (Y/N)	Is Touch start available (Y/N)

1.7 Reserved.

1.8 State is solely responsible for determining if the Fraud Detect Services and State's Settings satisfy its business, legal, or network scheme requirements. **State's Settings** means the instructions, settings, options, rules, requirements, strategies, or other instructions related to the Fraud Detect Services that State provides, selects, or acts upon (or that are provided, selected, or acted upon at State's direction).

1.9 First Data may terminate the Fraud Detect Services if its rights or access to third party technology or software used to provide the Fraud Detect Services is terminated or ends.

1.10 ***First Data disclaims all warranties (express or implied) that the Fraud Detect Services will accurately identify every instance of fraud or that***

every transaction identified as fraudulent is, in fact, fraudulent. State is solely responsible for State's Settings and all decisions it makes or actions it takes or does not take (or are made or taken or not taken at State's direction) on Fraud Detect Transaction Events.

2 Support

First Data will provide State with the following support for the Fraud Detect Services:

(1) Severe Issue Support. For severe technical issues, State may contact the First Data Global Command Center at +1 800-555-9966 on a 24/7/365 basis.

(2) Production Support. Production support for frequently asked questions (**FAQ Support**), issue triage, and escalations to application support and unblocking is available by contacting First Data's relationship team. Production support is also available by email to FraudDetectSupport@fiserv.com. Production support may be provided at varying hours of operation depending on the access point's standard operating business hours.

(3) Implementation Manager. An implementation manager will assist with implementation, integration, and production readiness for the Fraud Detect Services (**Implementation Manager**). During the implementation process, Fraud Detect Services support will be provided by the Implementation Manager.

(4) Portfolio Manager. During implementation and continuing post-implementation, a non-dedicated portfolio manager will periodically provide macro-level fraud trend analysis and suggestions designed to enhance State's overall fraud prevention and risk strategy.

The response time and downtime relative to the Fraud Detect Services shall not be included in the calculation of the service level agreements and associated penalties set forth in Schedule D of the Agreement. For the avoidance of doubt, the Service Level Agreement set forth in Schedule D of the Agreement will continue to apply to the Paypoint Gateway Services and shall remain in effect as calculated under Schedule D of the Agreement prior to the date that this Schedule J is executed.

3 Data Usage

3.1 Notwithstanding anything in the Agreement to the contrary with respect to the State's license grant to First Data related to State Data, First Data may retain, use, and share the Fraud Detect Data that State provides or makes available to First Data in connection with the Fraud Detect Services, including personally identifiable information, to provide and improve the Fraud Detect Services or other fraud prevention services; for product development,

analytics, and reporting. Any data retained by First Data pursuant to this paragraph remains subject to the requirements of the Agreement pertaining to data loss and data protection.

3.2 State obtains no rights or license to First Data's models, products, services, or the scores generated by them, and First Data reserves all rights to the foregoing not expressly granted to State.

4 Data Privacy

4.1 When First Data uses State's Fraud Detect Data to provide Fraud Detect Services to other Fraud Detect Services customers, First Data will not identify State as the source of the Fraud Detect Data.

4.2 State is responsible for and agrees that it will comply with all applicable law in connection with this Schedule and will provide any consumer disclosures or collect and receive any consumer consents (including, without limitation, any required consent to carry out automated individual decision making), authorizations or permissions required under applicable law with respect to the collection and transmission of Fraud Detect Data, including, without limitation, authorizing First Data to perform the Fraud Detect Services and for First Data to otherwise retain, use, and share Fraud Detect Data as set forth in this Schedule. State will provide reasonable cooperation and assistance upon First Data's request to enable First Data to meet its legal and internal compliance obligations with respect to the Fraud Detect Data, including providing First Data with documentation establishing that State has complied with the above obligations. State is responsible for the accuracy, quality, and legality of the Fraud Detect Data it provides to First Data or enables First Data to collect under this Schedule.

4.3 State acknowledges and agrees that the Fraud Detect Services may automatically collect a variety of information from or about end-users' computers or mobile devices, such as geolocation data, information from which location may be inferred, and unique identifiers; and associate such information with the end-user's transaction and such other information as State may provide First Data about the end-user. The information collected automatically may change from time to time at First Data's sole discretion. First Data's Fraud Detect Privacy Statement, available at https://merchants.fiserv.com/en-us/fraud-detect-privacy-statement/ or via another URL, link or delivery method provided by First Data from time to time. describes First Data's privacy practices in connection with the Fraud Detect Services.

4.4 If an individual submits a privacy inquiry regarding information First Data maintains about the individual, State will direct the individual to contact First Data with the request.

Exhibit A – Fraud Detect Implementation Form

This Implementation Form is between the State of Michigan (**State**) and First Data Government Solutions, LP (**First Data**); and supplements the Schedule J - Fraud Detect Schedule between the parties. Capitalized or other defined terms used, but not defined in this Implementation Form, have the meanings given to them in the Agreement or Schedule.

1 Purpose

The purpose of this Implementation Form is to describe the scope of Fraud Detect Services First Data will provide to State and the Fraud Detect Services implementation requirements. First Data is only responsible for providing the Fraud Detect Services as described in this Implementation Form. **Scope**

The Fraud Detect Services will provide:

1.1 Supervised machine learning model, to score transactions as described in *Section 2.5*.

1.2 Real-time fraud rules engine.

1.3 An automated Fraud Detect Response for each of the Fraud Detect Transaction Events types noted in *Section 7* and Payment Methods noted in *Section 6.5*.

1.4 Access to the User Interface to review/resolve each Fraud Detect Response, and obtain analytics and reporting.

2 Training

Up to 40 hours of training and consulting on how to use the User Interface and Fraud Detect Services, to be used within the first 30 days following implementation.

3 Assumptions

First Data's ability to implement and deliver the Fraud Detect Services is subject to, and dependent on, State timely performing its responsibilities under the Agreement, and responding to reasonable requests for information from First Data. First Data may rely on all data, information, decisions, and approvals provided by State.

4 Fraud Detect Services Implementation Management

First Data's Implementation Manager will:

4.1 Manage and coordinate First Data personnel assigned to implementing the Fraud Detect Services for State.

4.2 Act as First Data's point of contact for all implementation issues and the Change Process (defined in the Agreement).

4.3 Together, with State's Project Manager (defined the Agreement), establish an implementation project plan with targeted implementation events. The Change Process (described in the Agreement) will be used if either party desires a change to the finalized implementation project plan.

4.4 Conduct status meetings with State to review implementation progress, issues, and potential risks. Frequency of these meetings will be mutually agreed by State and First Data.

5 State Implementation Selections

5.1 Indicate if Fraud Detect Responses will consist of:

_____ Allow and Prevent, OR
__X__ Allow, Prevent and Review

6.8 Indicate which Payment Methods will be sent to the Fraud Detect Services:

__X__ Visa
__X__ MasterCard
__X__ Discover
__X__ American Express
_____ Wallet Payments

6.9 Integrate to the following First Data gateways, as applicable: Paypoint

7 Fraud Detect Transaction Events:

__X__ Pre Authorization Transaction (if selected, cannot select Post Authorization Transaction)
_____ Post Authorization Transaction (if selected, cannot select Pre Authorization Transaction)
__X__ Purchase Transaction
__X__ Deposit Transaction
_____ Card Registration
_____ User Registration

8 Change Process

Will be governed by the terms of the Agreement.

9 Acceptance Criteria

Fraud Detect Services will be deemed "accepted" and ready for production use once State is able to do each of the following (**Acceptance Criteria**) and meets the requirements as listed in 10. Software Acceptance Testing:

9.1 Validate that Fraud Detect Transaction Events (as requested above) are being received by the Fraud Detect Services for scoring.

9.2 Validate that State can receive a Fraud Detect Response for Fraud Detect Transaction Events (as requested above).

9.3 Validate that State's fraud rules have been deployed within the Fraud Detect Services.

9.4 Validate that State's Payment Types (as requested above) are deployed within the Fraud Detect Services.

9.5 Access the User Interface of the Fraud Detect Services.

9.6 Action data within the User Interface of the Fraud Detect Services (e.g., allow a transaction within the User Interface).

9.7 Access Fraud Detect Services reports (via User Interface).

If the Fraud Detect Services fail to materially meet the Acceptance Criteria, State shall notify First Data in writing in accordance with 10. Software Acceptance Testing With respect to Fraud Detect Services only, First Data will have a reasonable amount of time (no more than 30 days) to remedy such failure.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**

to

Contract Number **220000001254**

CONTRACTOR	
	FIRST DATA GOVERNMENT SOLUTIONS LP
	255 Fiserv Dr.
	Brookfield, WI 53045
	Leon Fox
	689-244-7377
	leon.fox@fiserv.com
	CV0060377

STATE			
	Program Manager	Various	DTMB
	Contract Administrator	Katelyn LaHaye	DTMB
		(517) 388-7422	
		lahayek@michigan.gov	

CONTRACT SUMMARY			
CENTRALIZED ELECTRONIC PAYMENT AUTHORIZATION SYSTEM (CEPAS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
August 1, 2022	June 30, 2026	5 - 1 Year	June 30, 2026
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, 2026
CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**		
$7,840,000.00	$0.00	$7,840,000.00		

DESCRIPTION

Effective 9/28/2022, the Contractor Contract Administrator and the Relationship Manager have been changed from Ryan Kelsey to Leon Fox.

Please note the State Contract Administrator has also been changed from Jennifer May to Katelyn LaHaye.

All other terms, conditions, specifications and pricing remain the same. Per (DTMB) contractor (request/ proposal) and agency (request) agreement, and DTMB Procurement approval.

STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management and Budget
525 W. Allegan St. Lansing, MI 48913
P.O. Box 30026, Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **171-220000001254**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	
	First Data Government Solutions LP
	255 Fiserv Dr.
	Brookfield, WI 53045
	Ryan Kelsey
	312-907-4823
	Ryan.Kelsey@fiserv.com
	CV0060377

STATE			
	Program Manager	Lucy Pline	DTMB
		517-636-5052	
		PlineL@michigan.gov	
	Contract Administrator	Jennifer May	DTMB
		517-242-6664	
		MayJ7@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Centralized Electronic Payment Authorization System (CEPAS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
8/1/2022	6/30/2026	5 – 1 year	6/30/2026
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45			
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card ☐ Payment Request (PRC) ☐ Other			☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
Effective 8/1/2022 This contract replaces contract 071B13000185. The contract is hereby extended thru 6/30/2026 with additional 5 – 1 year options added to the agreement. Contract is also increased by $7,840,000.00. Per contractor and agency agreement, DTMB Central Procurement Services approval, and State Administrative Board approval on 12/14/2021.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$7,840,000.00**

FOR THE CONTRACTOR:

First Data Government Solutions LP
Company Name


Authorized Agent Signature

Shane McCullough
Authorized Agent (Print or Type)

07/29/2022
Date

FOR THE STATE:

Signature

Jennifer Bronz, IT Category Manager
Name & Title

DTMB Central Procurement
Agency

Date

STATE OF MICHIGAN

SOFTWARE TERMS AND CONDITIONS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this "Contract") are agreed to between the State of Michigan (the "**State**") and First Data Government Solutions, LP ("**Contractor**"), a Delaware Limited Partnership. This Contract is effective on May 1, 2022 ("**Effective Date**"), and unless terminated, will expire on June 30, 2026 (the "**Term**").

This Contract may be renewed for up to 5 additional 1 year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via Contract Change Notice.

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

"**Acceptance**" has the meaning set forth in **Section 10**.

"**Acceptance Tests**" means such tests as may be conducted in accordance with **Section 10.1** and a Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

"**Allegedly Infringing Materials**" has the meaning set forth in **Section 19.2(b)**.

"**Approved Third Party Components**" means all third party components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in Schedule A – Statement of Work or as part of the State's Security Accreditation Process defined in Schedule E – Data Security Schedule.

"**Authorized Users**" means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

"**Business Day**" means a day other than a Saturday, Sunday or other day on which the State is authorized or required by law to be closed for business.

"**Business Requirements Specification**" means the initial specification setting forth the State's business requirements regarding the features and functionality of the Software, as set forth in a Statement of Work.

"Change" has the meaning set forth in **Section 2.2.**

"Change Notice" has the meaning set forth in **Section 2.2(b).**

"Change Proposal" has the meaning set forth in **Section 2.2(a).**

"Change Request" has the meaning set forth in **Section 2.2.**

"Confidential Information" has the meaning set forth in **Section 23.**

"**Configuration**" means State-specific changes made to the Software without Source Code or structural data model changes occurring.

"**Contract**" has the meaning set forth in the preamble.

"**Contract Administrator**" is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party's Contract Administrator will be identified in a Statement of Work.

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor Hosted**" means the Hosted Services are provided by Contractor or one or more of its Permitted Subcontractors.

"**Contractor Personnel**" means all employees of Contractor or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

"**Contractor Project Manager**" means the individual appointed by Contractor and identified in a Statement of Work to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

"**Customization**" means State-specific changes to the Software's underlying Source Code or structural data model changes.

"**Deliverables**" means the Software, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in a Statement of Work and all Work Product.

"**Documentation**" means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

"**DTMB**" means the Michigan Department of Technology, Management and Budget.

"**Effective Date**" has the meaning set forth in the preamble.

"**Fees**" means the fees set forth in the Pricing Schedule attached as **Schedule B**.

"**Financial Audit Period**" has the meaning set forth in **Section 24**.

"**Harmful Code**" means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

"**HIPAA**" has the meaning set forth in **Section 22**.

"**Hosted Services**" means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

"**Implementation Plan**" means the schedule included in a Statement of Work setting forth the sequence of events for the performance of Services under a Statement of Work, including the Milestones and Milestone Dates.

"Integration Testing" has the meaning set forth in **Section 10.2(a)**.

"**Intellectual Property Rights**" means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable law in any jurisdiction throughout the world.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in the Contract.

"**Loss or Losses**" means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

"**Maintenance Release**" means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

"**Milestone**" means an event or task described in the Implementation Plan under a Statement of Work that must be completed by the corresponding Milestone Date.

"**Milestone Date**" means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under a Statement of Work.

"**New Version**" means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

"**Nonconformity**" or **"Nonconformities"** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

"**Open-Source Components**" means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

"**Operating Environment**" means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

"PAT" means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

"**Permitted Subcontractor**" means any third party hired by Contractor to perform Services for the State under this Contract or have access to State Data.

"**Person**" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

"**Pricing Schedule**" means the schedule attached as **Schedule B.**

"Process" means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. **"Processing"** and **"Processed"** have correlative meanings.

"**Representatives**" means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

"**Services**" means any of the services, including but not limited to, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

"**Service Level Agreement**" means the schedule attached as **Schedule D**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

"**Site**" means the physical location designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Software.

"**Software**" means Contractor's software as set forth in a Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract.

"**Source Code**" means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

"**Specifications**" means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, if any, for such Software, or elsewhere in a Statement of Work.

"**State**" means the State of Michigan.

"**State Data**" has the meaning set forth in **Section 22.1**.

"**State Hosted**" means the Hosted Services are not provided by Contractor or one or more of its Permitted Subcontractors.

"**State Materials**" means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

"State Program Managers" are the individuals appointed by the State, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Software and other Deliverables; and (c) perform other duties as may be specified in a Statement of Work Program Managers will be identified in a Statement of Work.

"State Systems" means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

"**Statement of Work**" means any statement of work entered into by the parties and incorporated into this Contract. The initial Statement of Work is attached as **Schedule A**.

"**Stop Work Order**" has the meaning set forth in **Section 16**.

"**Support Services**" means the software maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

"**Support Services Commencement Date**" means, with respect to the Software, the date on which the Warranty Period for the Software expires, and fees for support become applicable, or such other date as may be set forth in a Statement of Work.

"**Technical Specification**" means, with respect to any Software, the document setting forth the technical specifications for such Software and included in a Statement of Work.

"**Term**" has the meaning set forth in the preamble.

"**Testing Period**" has the meaning set forth in **Section 10.1(b)**.

"**Transition Period**" has the meaning set forth in **Section 17.3**.

"**Transition Responsibilities**" has the meaning set forth in **Section 17.3**.

"**Unauthorized Removal**" has the meaning set forth in **Section 2.5(b)**.

"**Unauthorized Removal Credit**" has the meaning set forth in **Section 2.5(c)**.

"**User Data**" means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon extracting the Software without additional user input without the inclusion if user derived Information or additional user input.

"**Warranty Period**" means the ninety (90) calendar-day period commencing on the date of the State's Acceptance of the Software and for which Support Services are provided free of charge.

"WCAG 2.0 Level AA" means level AA of the World Wide Web Consortium Web Content Accessibility Guidelines version 2.0.

"**Work Product**" means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to Customizations, application programming interfaces, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Duties of Contractor. Contractor will provide Services and Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Services and Deliverables in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement(s) of Work.

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each party's Contract Administrator. The term of each Statement of Work will commence on the parties' full execution of a

Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 17**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to a Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 2.2**.

(a) As soon as reasonably practicable, and in any case within twenty (20) Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Changes to any Services or Deliverables;

(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;

(iii) any additional State Resources Contractor deems necessary to carry out such Changes; and

(iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within thirty (30) Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to a Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within fifteen (15) Business Days following the State's response to a Change Proposal, the State may, in its discretion:

(i) require Contractor to perform the Services under a Statement of Work without the Change;

(ii) require Contractor to continue to negotiate a Change Notice;

(iii) initiate a Dispute Resolution Procedure; or

(iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Section 17.**

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of

preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

2.3 Contractor Personnel.

(g) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(h) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) ensure that such Contractor Personnel have the legal right to work in the United States;

(ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and

(iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

(i) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(j) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor. Contractor Project Manager will be identified in a Statement of Work.

(k) Contractor Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(l) Contractor Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.

(m) Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor Project Manager;

(ii) the State consents in writing to any removal requested by Contractor in writing;

(iii) Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(n) Contractor will promptly replace its Contractor Project Manager on the occurrence of any event set forth in **Section 2.4(c)**. Such replacement will be subject to the State's prior written approval.

2.5 Contractor's Key Personnel.

(o) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State Program Managers or their designees, and 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.

(p) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing 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. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 17**.

(q) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to determine and remedy the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 17**, Contractor will issue to the State an amount equal to $25,000 per individual (each, an "**Unauthorized Removal Credit**").

(r) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection 2.5(c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to provide Services to the State under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(s) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(t) name the State a third-party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;

(u) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(v) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

3. PayPoint Services. First Data, through one or more of its Affiliates or other subcontractors, will provide State with a payment administration solution that will allow State to manage payment and payment transaction data (**PayPoint Services**) using an internet-based gateway (**PayPoint Gateway**) described in this Section.

(a) The PayPoint Services will enable State to submit payment instructions initiated by their consumers (**Consumers**) to First Data using the following payment channels: web-based applications, interactive voice response (**IVR**), customer representative assisted calls, point-of-sale devices, payment kiosk or Consumer walk-in. The PayPoint Services will enable State to: (i) consolidate payment output files utilizing the PayPoint posting file(s); (ii) review payment reporting; (iii) perform detailed payment research related to status, date tracking, time tracking and successful or negative payment results; (iv) review payment authorization and return processing information; (v) perform payment void and refund processing; (vi) track payment chargeback and settlement activity; (vii) apply notes to specific payments or transactions; (viii) process ad hoc payments; (ix) access and manage multiple individual Consumer accounts; and (x) add certain personalization (State specific logo, color theme and/or text) to the Consumer Payment solution (if applicable).

(b) The PayPoint Services will support multiple payment types, including Card payments and electronic check (**eCheck**) payments and other Automated Clearing House (**ACH**) payments (collectively, **Payments**). The PayPoint Services will support Card Payments initiated by Consumers and processed using American Express Card, Discover Card, MasterCard Card, or VISA Card as well as other Card Payments that First Data identifies from time-to-time. The PayPoint Services will support eCheck Payments initiated by Consumers and submitted by State for processing by First Data using the ACH system. The PayPoint Services supports the following ACH Payment entry classes: TEL, WEB, CCD and PPD, as defined by the National Automated Clearing House Association (**NACHA**) Operating Rules and Guidelines (collectively, the **Rules**). To accept eCheck payments using premium services of First Data's Affiliate, TeleCheck Services, Inc. (TeleCheck®), including Verification, State must have a separate agreement with TeleCheck®. To accept debit card or credit card payments, State must have a separate agreement that includes card processing.

(c) First Data will fully host the PayPoint Services. In addition, if selected by State, the PayPoint Solution will provide State with a front-end solution (**Consumer Payments**) that includes a ready-made website and/or IVR that can be personalized and a toolkit for State to manage the web-site personalization, branding the consumer payments site with State's trademark and logo provided by State. State shall integrate to the PayPoint Solution via (i) real time integration of State front end website with the PayPoint application programming interface; (ii) xml batch integration; or (iii) the Consumer Payments solution. Upon request from First Data at any time during State's use of the PayPoint Gateway, State will complete any requested documentation and provide any requested information regarding State's use of the PayPoint Gateway. First Data will have the right to reasonably audit State's use of the PayPoint Gateway at any time while State is utilizing the PayPoint Gateway. State and First Data, when Consumer Payments is used, will maintain a copy of each Consumer's authorization for the longer of: (i) two (2) years or (ii) the period of time required by the Rules. State will provide First Data with legible copies of authorizations within seven (7) days of First Data's request for them.

(d) State will submit all Payments initiated by Consumers using the PayPoint Services and First Data's System. State will provide all transaction data, personal information, related information and instructions (collectively **Payment Data**) necessary for First Data to perform the PayPoint Services. State will be the "Originator" (as defined in the Rules) of any ACH Payments that State submits for processing under this Agreement and shall have all responsibilities and liabilities of an Originator under the Rules and Card association rules for such ACH Payments. First Data will be a "Third-Party Sender" (as defined in the Rules) with respect to such ACH Payments and shall have all of the responsibilities and liabilities of a Third Party Sender under the Rules with respect to such ACH Payments. State will comply with all applicable Rules and will not originate transactions in violation of any applicable law. State will not itself act as a Third-Party Sender on behalf of any other Originator under this Agreement without First Data's prior written consent. First Data may withhold its consent for any reason, including if the Originating Depository Financial Institution (**ODFI**) (as defined in the Rules) utilized by First Data does not provide consent to First Data. First Data will facilitate processing ACH Payments submitted by State by transmitting ACH files to one or more ODFIs that has agreed to originate ACH Payments for First Data's Originators. State authorizes First Data and its ODFI to originate entries on behalf of State to the accounts designated in the Payment Data. State will be fully responsible and liable for the amount of any ACH Payments that are returned or reversed for any reason, including non-sufficient funds. If State assesses and collects convenience fees, State shall be solely responsible for complying with the Card association rules and Rules related to convenience fees. First Data may initiate ACH debits to State's account for all such Returns or Reversals. State assumes all responsibilities and liabilities under applicable association rules or regulations related to processing Card Payments of its users. State represents and warrants that all Payments that it submits to First Data have been validly authorized in accordance with applicable law and the applicable Rules or the applicable card association rules and regulations for any Card Payments. CLIENT WILL BE SOLELY RESPONSIBLE FOR ENSURING THE VALIDITY, ACCURACY AND COMPLETENESS OF ALL PAYMENT DATA. FISERV WILL RELY UPON AND USE PAYMENT DATA SUBMITTED BY CLIENT WITHOUT FURTHER VERIFICATION IN ORDER TO PROVIDE THE SERVICES. State will be liable for any fees and fines (including fees and fines incurred by First Data) that result from inaccurate, or incomplete Payment Data. First Data will have no responsibility or liability for any error, omission, delay, failure to meet any processing timelines or accurately perform any of its PayPoint Services due to State (or its Consumers) submitting inaccurate, incomplete or untimely Payment Data, or failing to perform its settlement obligations.

(e) If First Data consents in writing to State, itself, acting as a Third Party Sender on behalf of any other Originator under this Agreement, State will (i) flow down all terms and conditions required by the Rules, including the applicable terms of Section (d) above, to the Originator, (ii) flow down First Data's right to audit the Originator's use of the PayPoint Gateway as described in Section (c) above, (iii) flow down to the Originator the obligation to complete any documentation and provide any information requested by First Data regarding its use of the PayPoint Gateway as described in Section (c) above, and (iv) shall have all of the responsibilities and liabilities of a Third-Party Sender under the Rules with respect to such ACH Payments. First Data may suspend State's ability to originate ACH Payments for that portion of the payments that are violating the Rules upon written notice to State. First Data may terminate State's ability to originate ACH Payments for that portion of the payments that are violating the rules upon written notice to State, if State has violated the Rules and has not cured such violation within 30 calendar days after receipt of such notice.

(f) Convenience Fee Support is available through the PayPoint Services where an additional processing fee can be charged along with the primary payment. The PayPoint Services do not process settlement of convenience fees. Rather, the PayPoint Services enable tracking and management of convenience fee data submitted with other

payment data received from State that assesses and collects convenience fees. Accordingly, if State assesses and collects convenience fees through the PayPoint Services, State shall be solely responsible for complying with the card association and NACHA rules related to convenience fees.

(g) The PayPoint Services do not include the following: (i) processing or management of TeleCheck® agreements for eCheck payments; (ii) processing or management of merchant acquiring agreements for credit and/or debit card payments; (iii) custom development by First Data (if State requires custom development, the effort will be separately scoped and quoted); or (iv) providing support directly to Consumers.

4. Notices. All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Jennifer May 525 W. Allegan Street Lansing, MI 48909 MayJ7@michigan.gov 517-242-6664	First Data Government Solutions, LP Attn: Legal Department 255 Fiserv Drive Brookfield, WI 53045 legalpapers@firstdata.com

5. Insurance. Contractor must maintain the minimum insurances identified in the Insurance Schedule attached as **Schedule C**.

6. Software License.

6.1 **Perpetual License**. If Contractor is providing the State with a license to use its Software indefinitely, then Contractor hereby grants to the State and its Authorized Users a non-exclusive, royalty-free, perpetual, irrevocable right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract, provided that:

(a) The State is prohibited from reverse engineering or decompiling the Software, making derivative works, modifying, adapting or copying the Software except as is expressly permitted by this Contract or required to be permitted by law;

(b) The State is authorized to make copies of the Software for backup, disaster recovery, and archival purposes;

(c) The State is authorized to make copies of the Software to establish a test environment to conduct Acceptance Testing;

(d) Title to and ownership of the Software shall at all times remain with Contractor and/or it's licensors, as applicable; and

(e) Except as expressly agreed in writing, the State is not permitted to sub-license the use of the Software or any accompanying Documentation.

6.2 **Subscription License.** If the Software is Contractor Hosted and Contractor is providing the State access to use its Software during the Term of the Contract only, then:

(a) Contractor hereby grants to the State, exercisable by and through its Authorized Users, a nonexclusive, royalty-free, irrevocable right and license during the Term and such additional periods, if any, as Contractor is required to perform Services under this Contract or any Statement of Work, to:

(i) access and use the Software, including in operation with other software, hardware, systems, networks and services, for the State's business purposes, including for Processing State Data;

(ii) generate, print, copy, upload, download, store and otherwise Process all GUI, audio, visual, digital and other output, displays and other content as may result from any access to or use of the Software;

(iii) prepare, reproduce, print, download and use a reasonable number of copies of the Specifications and Documentation for any use of the Software under this Contract; and

(iv) access and use the Software for all such non-production uses and applications as may be necessary or useful for the effective use of the Software hereunder, including for purposes of analysis, development, configuration, integration, testing, training, maintenance, support and repair, which access and use will be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Section 6.2(c)** below.

(b) License Restrictions. The State will not: (a) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make the Software available to any third party, except as expressly permitted by this Contract or in any Statement of Work; or (b) use or authorize the use of the Software or Documentation in any manner or for any purpose that is unlawful under applicable Law.

(c) Use. The State will pay Contractor the corresponding Fees set forth in a Statement of Work or Pricing Schedule for all Authorized Users access and use of the Software. Such Fees will be Contractor's sole and exclusive remedy for use of the Software, including any excess use.

6.3 **Certification**. To the extent that a License granted to the State is not unlimited, Contractor may request written certification from the State regarding use of the Software for the sole purpose of verifying compliance with this **Section 6.** Such written certification may occur no more than once in any twenty four (24) month period during the Term of the Contract. The State will to respond to any such request within 45 calendar days of receipt. If the State's use is greater than contracted, Contractor may invoice the State for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in **Schedule B**, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

6.4 **State License Grant to Contractor**. The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work**.** Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

7. Third Party Components. At least 30 days prior to adding new Third Party Components, Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third Party Components included in the Software.

8. Intellectual Property Rights

8.1 Ownership Rights in Software

(a) For purposes of this **Section 8** only, the term "Software" does not include Customizations.

(b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Section 8.1(c)**:

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and

(ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(c) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to State Materials, User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

8.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the Work Product.

9. Software Implementation.

9.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan.

9.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in a Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

10. Software Acceptance Testing.

10.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, or in the case of Contractor Hosted Software, when Contractor notifies the State in writing that the Hosted Services are ready for use in a production environment, Acceptance Tests will be conducted as set forth in this **Section 10** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following installation of the Software, or the receipt by the State of the notification in **Section 10.1(a)**, and be conducted diligently for up to thirty (30) Business Days, or such other period as may be set forth in a Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in a Statement of Work or, if a Statement of Work does not specify, the State, provided that:

(i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

10.2 Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

(a) Upon delivery and installation of any application programming interfaces, Configuration or customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 10.1**, **Section 10.4**, and **Section 10.5**.

(b) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

10.3 Notices of Completion, Non-Conformities, and Acceptance. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 10.4** and **Section 10.5**.

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have thirty (30) Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 10.4** and **Section 10.5**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State Program Managers or their designees.

10.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance

with the requirements set forth in a Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Section 10.1(a)** or **Section 10.3(c)(i)**, identifying any Non-Conformities.

Fiasafsdrst Data

10.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 10**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract for cause in accordance with **Section 17**.

10.6 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) and any Deliverables will occur on the date that is the earliest of the State's delivery of a notice accepting the Software or Deliverables under **Section 10.3(b)**, or **Section 10.3(c)(ii)**.

11. Non-Software Acceptance.

11.1 All other non-Software Services and Deliverables are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("State Review Period"), unless otherwise provided in the Statement of Work. If the non-Software Services and Deliverables are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the non-Software Services and Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Services and Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the non-Software Services and Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 17**, Termination for Cause.

11.2 Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any non-Software Services and Deliverables, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable non-Software Services and Deliverables to the State. If acceptance with deficiencies or rejection of the non-Software Services and Deliverables impacts the content or delivery of other non-completed non-Software Services and Deliverables, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

11.3 If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may provide the non-Software Services and Deliverables and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

12. Assignment. Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

13. Change of Control. Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

(a) a sale of more than 50% of Contractor's stock;

(b) a sale of substantially all of Contractor's assets;

(c) a change in a majority of Contractor's board members;

(d) consummation of a merger or consolidation of Contractor with any other entity;

(e) a change in ownership through a transaction or series of transactions;

(f) or the board (or the stockholders) approves a plan of complete liquidation.

A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

14. Invoices and Payment.

14.1 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Services and Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all prices are inclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

14.2 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Services and Deliverables. Contractor's acceptance of final payment by the State constitutes 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 disputed.

14.3 The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at http://www.michigan.gov/SIGMAVSS to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

14.4 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

14.5 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

14.6 Pricing/Fee Changes. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

(b) Excluding federal government charges and terms. Contractor warrants and agrees that each of the Fees, economic or product terms or warranties granted pursuant to this Contract are comparable to or better than the equivalent fees, economic or product term or warranty being offered to any commercial or government customer of Contractor. If Contractor enters into any arrangements with another customer of Contractor to provide the products or services, available under this Contract, under more favorable prices, as the prices may be indicated on Contractor's current U.S. and International price list or comparable document, then this Contract will be deemed amended as of the date of such other arrangements to incorporate those more favorable prices, and Contractor will immediately notify the State of such Fee and formally memorialize the new pricing in a Change Notice.

15. Liquidated Damages.

15.1 The parties agree that any delay or failure by Contractor to timely perform its obligations in accordance with the Implementation Plan and Milestone Dates agreed to by the parties will interfere with the proper and timely implementation of the Software, to the loss and damage of the State. Further, the State will incur major costs to perform the obligations that would have otherwise been performed by Contractor. The parties understand and agree that any liquidated damages Contractor must pay to the State as a result of such nonperformance are described in a Statement of Work, and that these amounts are reasonable estimates of the State's damages in accordance with applicable law.

15.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event if Contractor fails to timely perform its obligations by each Milestone Date.

15.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause under **Section 17** and the State will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

15.4 Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

16. Stop Work Order. The State may, at any time, order the Services of Contractor fully or partially stopped for up to ninety (90) calendar days at no additional cost to the State. The State will provide Contractor a written notice detailing such suspension (a "**Stop Work Order**"). Contractor must comply with the Stop Work Order upon receipt. Within 90 days, or any longer period agreed to by Contractor, the State will either:

(a) issue a notice authorizing Contractor to resume work, or

(b) terminate this Contract. The State will not pay for any Services, Contractor's lost profits, or any additional compensation during a stop work period.

17. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

17.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:

(i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;

(ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or

(iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If the State terminates this Contract under this **Section 1**, the State will issue a termination notice specifying whether Contractor must:

(i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for public interest, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 2**.

(c) The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. Further, Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

17.2 Termination for Public Interest. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must:

(a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(b) continue to perform in accordance with **Section 3**. If the State terminates this Contract for public interest, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

17.3 Transition Responsibilities.

(a) Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to:

(i) continuing to perform the Services at the established Contract rates;

(ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee;

(iii) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 5** regarding the return or destruction of State Data at the conclusion of the Transition Period; and

(iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

(b) Contractor will follow the transition plan attached as **Schedule G** as it pertains to both transition in and transition out activities.

18. Indemnification

18.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to:

(a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;

(b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;

(c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and

(d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

18.2 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to:

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding;

(c) employ its own counsel; and to

(d) retain control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 18**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

18.3 The State is constitutionally prohibited from indemnifying Contractor or any third parties.

19. Infringement Remedies.

19.1 The remedies set forth in this Section are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

19.2 If any Software or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(a) procure for the State the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or

(b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

19.3 If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(a) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(b) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to six (6) months to allow the State to replace the affected features of the Software without disruption.

19.4 If Contractor directs the State to cease using any Software under **Section 3,** the State may terminate this Contract for cause under **Section 1**.Unless the claim arose against the Software independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

(a) Contractor's compliance with any designs, specifications, or instructions of the State; or

(b) modification of the Software by the State without the prior knowledge and approval of Contractor.

20. Disclaimer of Damages and Limitation of Liability.

20.1 The State's Disclaimer of Damages. THE STATE WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

20.2 The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

20.3 Contractor's Limitation of Liability. NOTWITHSTANDING ANYTHING CONTAINED HEREIN, IN THE EVENT OF A BREACH OF THE CONTRACTOR'S SYSTEM WHERE CARDHOLDER DATA HAS BEEN COMPROMISED, THE CONTRACTOR'S AGGREGATE LIABILITY FOR ANY AND ALL COSTS INCURRED BY THE STATE ASSOCIATED WITH THE BREACH SHALL NOT EXCEED TWENTY MILLION DOLLARS ($20,000,000).

21. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

(a) a criminal Proceeding;

(b) a parole or probation Proceeding;

(c) a Proceeding under the Sarbanes-Oxley Act;

(d) a civil Proceeding involving:

(i) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or

(ii) a governmental or public entity's claim or written allegation of fraud; or

(e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

22. State Data.

22.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes:

(a) User Data; and

(b) any other data collected, used, Processed, stored, or generated in connection with the Services, including but not limited to:

(i) personally identifiable information ("**PII**") collected, used, Processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and

(ii) personal health information ("**PHI**") collected, used, Processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations.

22.2 State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State.

22.3 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor must:

(a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss;

(b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law;

(c) keep and maintain State Data in the continental United States and

(d) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent.

22.4 Discovery. Contractor will immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Software and Hosted Services, if applicable. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. In no event will Contract provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for State review, revision and approval.

22.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable:

(a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence;

(b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;

(c) in the case of PII or PHI, at the State's sole election:

(i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or

(ii) reimburse the State for any costs in notifying the affected individuals;

(d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twenty-four (24) months following the date of notification to such individuals;

(e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence;

(h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and

(i) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination.

22.6 The parties agree that any damages relating to a breach of **Section 22** are to be considered direct damages and not consequential damages. **Section 22** survives termination or expiration of this Contract.

23. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. This **Section 23** survives termination or expiration of this Contract.

23.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that:

(a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party;

(b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; or,

(c) should reasonably be recognized as confidential information of the disclosing party.

The term "Confidential Information" does not include any information or documentation that was or is:

(d) in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA);

(e) already in the possession of the receiving party without an obligation of confidentiality;

(f) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights;

(g) obtained from a source other than the disclosing party without an obligation of confidentiality; or,

(h) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party).

For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

23.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor's subcontractor is permissible where:

(a) the subcontractor is a Permitted Subcontractor;

(b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and

(c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any of the Contractor's and Permitted Subcontractor's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 2**.

23.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

23.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

23.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within five (5) Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State's Confidential Information, including State Data, from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitation methods or as otherwise instructed by the State. If the State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within five (5) Business Days from the date of confirmation from the State.

24. Records Maintenance, Inspection, Examination, and Audit.

24.1 Right of Audit. Pursuant to MCL 18.1470, the State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain, and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for four (4) years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

24.2 Right of Inspection. Within ten (10) calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within forty-five (45) calendar days.

24.3 Application. This **Section 24** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

25. Support Services. Contractor will provide the State with the Support Services described in the Service Level Agreement attached as **Schedule D** to this Contract. Such Support Services will be provided:

(a) Free of charge during the Warranty Period.

(b) Thereafter, for so long as the State elects to receive Support Services for the Software, in consideration of the State's payment of Fees for such services in accordance with the rates set forth in the Pricing Schedule.

26. Data Security Requirements. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in **Schedule E** to this Contract.

27. Training. Contractor will provide, at no additional charge, training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State's request, Contractor will timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

28. Maintenance Releases; New Versions

28.1 Maintenance Releases. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

28.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

28.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions. If the State wishes to install any Maintenance Release or New Version, the State will have the right to have such Maintenance Release or New Version installed, in the State's discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract.

29. Reserved

30. Contractor Representations and Warranties.

30.1 Authority. Contractor represents and warrants to the State that:

(a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and

(d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms.

(e) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606.

30.2 Reserved

30.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) it has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

(d) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(e) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(f) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as delivered or installed by Contractor does not or will not:

(i) infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable law;

(g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:

(i) Harmful Code; or

(ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.

(h) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(i) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract and will devote adequate resources to meet Contractor’s obligations under this Contract;.

(j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;

(k) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever;

(l) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

(m) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.

(n) If Contractor Hosted:

(i) Contractor will not advertise through the Hosted Services (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by the State;

(ii) the Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in the Service Level Agreement;

(iii) all Specifications are, and will be continually updated and maintained so that they continue to be, current, complete and accurate and so that they do and will continue to fully describe the Hosted Services in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Hosted Services have any material undocumented feature;

(o) During the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Software or with the Hosted Services, if applicable, will apply solely to Contractor or its Permitted Subcontractors. Regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against State Systems or networks.

30.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

31. Offers of Employment. During the first twelve (12) months of the Contract, should Contractor hire an employee of the State who has substantially worked on any project covered by this Contract without prior written consent of the State, the Contractor will be billed for fifty percent (50%) of the employee's annual salary in effect at the time of separation.

32. Conflicts and Ethics. Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any Permitted Subcontractor that provides Services and Deliverables in connection with this Contract.

33. Compliance with Laws. Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

34. Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq*., and Executive Directive 2019-09, Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

35. Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

36. Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the Michigan Court of Claims. Complaints against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

37. Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

38. Reserved.

39. Dispute Resolution. The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely or fails to respond within fifteen (15) business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

40. Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

41. Severability. If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

42. Waiver. Failure to enforce any provision of this Contract will not constitute a waiver.

43. Survival. The rights, obligations and conditions set forth in this **Section 3** and **Section 1** (Definitions), **Section 3** (Transition Responsibilities), **Section 18** (Indemnification), **Section 20** (Disclaimer of Damages and Limitations of

Liability), **Section 22** (State Data), **Section 23** (Non-Disclosure of Confidential information), **Section 30** (Contractor Representations and Warranties), **Section 54** (Effect of Contractor Bankruptcy) and **Schedule C** Insurance, and any right, obligation or condition that, by its express terms or nature and context is intended to survive the termination or expiration of this Contract, survives any such termination or expiration.

44. Administrative Fee and Reporting. Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made online by check or credit card at: https://www.thepayplace.com/mi/dtmb/adminfee. The administrative fee and reporting requirements are not required on purchases made on this contract by Michigan courts.

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

45. Extended Purchasing Program. This contract is extended to MiDEAL members. MiDEAL members include local units of government, courts, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal.

Upon written agreement between the State and Contractor, this contract may also be extended to other states (including governmental subdivisions and authorized entities).

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

46. Contract Modification. This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Notice**"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

47. HIPAA Compliance. The State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.

48. Accessibility Requirements.

48.1 All Software provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA within twelve months from the Effective Date of this Contract. Contractor must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for each product provided under the Contract. At a minimum, Contractor must comply with the WCAG 2.0 Level AA conformance claims it made to the State, including the level of conformance provided in any PAT. Within twelve months from the Effective Date of this Contract and throughout the Term of the Contract thereafter, Contractor must:

(a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;

(b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;

(c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to WCAG 2.0 Level AA;

(d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor's Software;

(e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and

(f) participate in the State of Michigan Digital Standards Review described below.

48.2 State of Michigan Digital Standards Review. Contractor must assist the State, at no additional cost, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to validate Contractor's accessibility and compliance with WCAG 2.0 Level AA. Prior to the solution going-live and thereafter on an annual basis, or as otherwise required by the State, re-assessment of accessibility may be required. At no additional cost, Contractor must remediate all issues identified from any assessment of accessibility pursuant to plans and timelines that are approved in writing by the State.

48.3 Warranty. Contractor warrants that all WCAG 2.0 Level AA conformance claims made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to the State, are true and correct. If the State determines such conformance claims provided by the Contractor represent a higher level of conformance than what is actually provided to the State, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated WCAG 2.0 Level AA conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in addition to all other remedies available to the State, the State may terminate this Contract for cause under **Section 1**.

48.4 Contractor must, without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State arising out of its failure to comply with the foregoing accessibility standards

48.5 Failure to comply with the requirements in this **Section 48** shall constitute a material breach of this Contract.

49. Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

50. Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for nor bind the other party in any manner whatsoever.

51. Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

52. No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

53. Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available

from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual **damages** or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this Section.

54. Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and all Software and Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

55. Schedules. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing Schedule
Schedule C	Insurance Schedule
Schedule D	Service Level Agreement – Downtime Service Level Agreement – System Response Time
Schedule E	Data Security Requirements
Schedule E, Attachment 1	PCI Compliance
Schedule E, Attachment 2	Offshore Resources
Schedule F	Disaster Recovery Plan (if Contractor Hosted)
Schedule G	Transition Out
Schedule H	Key Entry Payment Screen Fields
Schedule I	Escalation Process

56. Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

57. Entire Agreement. These Terms and Conditions, including all Statements of Work and other Schedules and Exhibits (again collectively the "Contract") constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the Terms and Conditions, the Schedules, Exhibits, and a Statement of Work, the following order of precedence governs: (a) first, these Terms and Conditions and (b) second, Schedule E – Data Security Requirements and (c) third, each Statement of Work; and (d) fourth, the remaining Exhibits and Schedules to this Contract. NO TERMS ON CONTRACTOR'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO STATE'S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF

THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A – STATEMENT OF WORK

This schedule identifies the requirements of the Contract.

1. DEFINITIONS

The following terms have the meanings set forth below. All initial capitalized terms that are not defined in this Schedule shall have the respective meanings given to them in Section 1 of the Contract Terms and Conditions.

Term	Definition
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.
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 2021 began on October 1, 2020 and ends on September 30, 2021.
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.
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.
TRS	TeleCheck Recovery Services (pending full definition from product)

2. BACKGROUND

The State of Michigan (State), through the Michigan Department of Technology, Management and Budget (DTMB) and the Michigan Department of Treasury, Office of Financial Services Division 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.

The Department of Treasury, Office of Financial Services 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 all State agencies.

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 car swipe device.

Contractor will provide ACH services by acting as a third party sender by maintaining a relationship with a participating Originating Depository Financial Institution (ODFI). State of Michigan will be the "Originator" (as defined in the NACHA Rules) of any ACH Payments that the State of Michigan submits for processing.

2.1 Scope of Work and Deliverables

2.1.1 IN SCOPE

- Services for payment processing and authorization
  - Configuration
  - Interfaces
  - Integration
  - Testing
- Knowledge transfer to State staff
  - Training
  - Train the trainer
  - End user
  - 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

2.2 Summary of Scope

- The State 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.
- The Contractor will supply the State an enterprise-wide payment processing gateway to process both credit/debit (pin-based) cards and ACH debit payments that are submitted from multiple agency applications through a variety of payment channels including Web, IVR, , software which allows Manual Key Entry, and/or card swipe device.
- Note: Hereafter the term “credit card” refers to both credit and debit cards.
.
- Contractor will provide one-hundred-eighty (180) days written notice for any change that requires integration or programming changes by the State. If required by NACHA Card Association, or other regulatory entities, Contractor must communicate change within 14 calendar days upon receipt of information from the regulatory association.
- Contractor must provide sixty (60) days’ notice for regulatory changes that may require implementation.
- The Contractor must provide standard Application Program Interfaces (APIs) and Key Entry Screens to allow the State electronic payments to be securely collected, stored and settled, and the funds credited to the corresponding State bank accounts. The system must provide a response that contains a unique confirmation number and can be printed and used as a customer receipt.
- The Contractor must 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 must be capable of tracking individual business application activity at the application, 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 transactions and be capable of processing credit/debit cards swiped through the 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 must provide services to process ACH debit transactions under this contract.
- The Contractor must provide a registration process to allow State customers to set up financial accounts and 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 must allow for future-dated ACH payments; subject to the applicable ACH regulations.
- The Contractor’s system must 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 must be capable of enabling the State to 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 must be comprised of redundant hardware and software and 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, which is configurable by client and application.
- The Contractor’s system must provide fully functioning Initial Test and User Acceptance Test (UAT) environments that replicates the production environment functionality. The UAT must allow for end-to-end testing and include simulated ACH and credit card authorization (cards only), settlement and refunds. The Contractor must also provide system documentation, training, training material, dedicated business and technical contacts, and 24/7/365 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 posting file that contains details of the previous day's transactions.
- The Contractor must provide 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.
- The State requires the use of TSYS Processing Services.

2.3 OUT OF SCOPE

- Acquiring services are out of scope for 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.

3. IT ENVIRONMENT RESPOSIBILITIES

For a Contractor Hosted Software Solution:

Definitions:

Facilities – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.

Infrastructure – Hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.

Platform – Computing server software components including operating system (OS), middleware (e.g. Java runtime, .NET runtime, integration, etc.), database and other services to host applications

Application – Software programs which provide functionality for end user and Contractor services

Storage – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations

Backup – Storage and services that provide online and offline redundant copies of software and data

Development - Process of creating, testing and maintaining software components

Component Matrix	Identify contract components with contractor or subcontractor name(s), if applicable
Facilities	
Infrastructure	
Platform	
Application	
Storage	
Backup	
Development	

4. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 within twelve (12) months from the Effective Date of this Contract.

Upon execution of this Contract, Contractor must provide a copy of its most recent PAT. Within twelve months from the Effective Date of this Contract, Contractor must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for the Solution. If the Solution is comprised of multiple products, a PAT must be provided for each product. In addition to PATs, Contractors may include a verification of conformance certified by an industry-recognized third-party. If the Contractor is including any third-party products in the Solution, Contractor must obtain and provide the third-party PATs as well.

Each PAT must state exactly how the product meets the specifications. All "Not Applicable" (N/A) responses must be fully explained. Contractor must address each standard individually and with specificity; and clarify whether conformance is achieved throughout the entire product (for example – user functionality, administrator functionality, and reporting), or only in limited areas. A description of the evaluation methods used to support WCAG 2.0 Level AA conformance claims, including, if applicable, any third-party testing, must be provided. For each product that does not fully conform to WCAG 2.0 Level AA, Contractor must provide detailed information regarding the plan to achieve conformance, including timelines.

5. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
Public Citizen	Public	20,000	20,000/all instances
State Employee	Administrative	1,000	1,000
Approved Third Party	Administrative	300	300

Contractor Solution must meet the expected number of concurrent Users.

6. ACCESS CONTROL AND AUTHENICATION

If required and paid for by the State, Contractor's solution must integrate with the State's IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy (https://www.michigan.gov/dtmb/0,5552,7-358-82547_56345_56351_69611-336646--,00.html), which consist of:

6.1 MILogin/Michigan Identity, Credential, and Access Management (MICAM). An enterprise single sign-on and identity management solution based on IBM's Identity and Access Management products including, IBM Security Identity Manager (ISIM), IBM Security Access Manager for Web (ISAM), IBM Tivoli Federated Identity Manager (TFIM), IBM Security Access Manager for Mobile (ISAMM), and IBM DataPower, which enables the State to establish, manage, and authenticate user identities for the State's Information Technology (IT) systems.

6.2 MILogin Identity Federation. Allows federated single sign-on (SSO) for business partners, as well as citizen-based applications.

6.3 MILogin Multi Factor Authentication (MFA, based on system data classification requirements). Required for those applications where data classification is Confidential and Restricted as defined by the 1340.00 Michigan

Information Technology Information Security Policy (i.e. the proposed solution must comply with PHI, PCI, CJIS, IRS, and other standards).

6.4 MILogin Identity Proofing Services (based on system data classification requirements). A system that verifies individual's identities before the State allows access to its IT system. This service is based on "life history" or transaction information aggregated from public and proprietary data sources. A leading credit bureau provides this service.

To integrate with the SOM MILogin solution, the Contractor's solution must support SAML, or OAuth or OpenID interfaces for the SSO purposes.

7. END USER OPERATING ENVIRONMENT

The Supported Browsers must include the current and prior major versions supported by the Manufacturers listed below:

- Microsoft Edge
- Apple Safari
- Google Chrome
- FireFox
- [1]Microsoft Internet Explorer

[1] Note: Internet Explorer (IE) 11 desktop application will end support for certain operating systems starting June 15, 2022. Customers are encouraged to move to Microsoft Edge. – IE may be usable, but we cannot troubleshoot issues because Microsoft is in the sunset process for this browser.

8. TRAINING SERVICES

The Contractor must provide training to the Michigan Treasury team for new technologies added to the payment gateway.

9. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals, best practice guide, and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

Contractor must develop and submit complete, accurate, and timely Solution documentation matching the product functionality. Users can file cases via Paysupport or other service ticket systems, if available, throughout the life of the contract.

The Contractor's user documentation must provide up to date and detailed information about software features and functionality.

10. ADDITIONAL PRODUCTS AND SERVICES

The State may need additional products and services requested at a later date.

11. CONTRACTOR PERSONNEL

Contractor Contract Administrator. Contractor resource who is responsible to(a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
Name Ryan Kelsey **Address** 255 Fiserv Dr, Brookfield WI 53045 **Phone** 312.907.4823 **Email** Ryan.Kelsey@fiserv.com

12. CONTRACTOR KEY PERSONNEL

Contractor Project Manager. If the State has a project where a Project Manager needs to be assigned the Contractor will assign the appropriate resource who is responsible to serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services, matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
Name TBD based on project **Address** **Phone** **Email**

Contractor PayPoint Customer Services Representative. Contractor resource primary responsibility is to resolve problems, implement changes and maintain an effective client relationship. Troubleshooting: Interacts with SOM when there are systems, processor, or processing issue. Resource will either assist 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. This resource is responsible for total resolution of the issue meeting or exceeding the client's expectation. Application development/Boarding: Works directly with Processors and/or the Relationship/Account Managers to ensure a complete processing methodology is functioning as expected in a timely manner. . After normal business hours, 8:00am – 5:00pm EST, the client should call the Response Center at 800-337-1222. If there is an urgent issue impacting business operation, the client will be connected directly to Contractor's Command Center to resolve the issue immediately.

Contractor
Name Terrance Cherry **Address** 255 Fiserv Dr, Brookfield WI 53045 **Phone** 303.967.5833 **Email** Terrance.Cherry@Fiserv.com

Contractor PayPoint Customer Services Manager – Contractor resource would manage the support team dedicated to the ongoing operational needs of the State PayPoint platform. The resource is also 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. This resource acts as the key escalation contact for issues that have not been resolved per the PayPoint Help Desk MI CEPAS Escalation Process. The resource also plans and develops teams to address failing policies and procedures and effectively communicate the information to upper management. The resource will oversee negotiations and administration of vendor contracts, consultant contracts and service agreements. The resource will work closely with other departments to resolve issues outside the normal areas of responsibility and coordinates long-range operational goals.

Contractor
Name Ryne Weaver **Address** 255 Fiserv Dr, Brookfield WI 53045 **Phone** 531.910.1778 **Email** Ryne.weaver@fiserv.com

13. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks. Contractor must present certifications evidencing satisfactory Michigan State Police Background checks, ICHAT, and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

.

Offshore Resources Please see Schedule E, Attachment 2. .

14. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Contract Administrator	
Name	Jennifer May
Phone	517-242-6664
Email	MayJ7@michigan.gov

Program Managers. The DTMB and Agency Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

DTMB Program Manager	
Name	Lucy Pline
Phone	517-636-5052
Email	PlineL@michigan.gov

Agency Program Manager	
Name	Amy Kelso
Phone	517-636-5372
Email	KelsoA@michigan.gov

Other Roles and Responsibilities
The State has a statewide contract with Elavon for processing credit and debit cards. Elavon is the State's acquirer.

All credit/debit card transactions processed through this Contract will be processed through TSYS Processing Services.

15. MEETINGS

The Contractor must attend the following meetings, at a location and time as identified by the state, at no additional cost to the State:

- **Monthly Status Meetings: Contractor will meet monthly to review tickets, new ach/credit rule changes, ongoing support, maintenance, and open tickets.**
- **Quarterly meetings:** Subsequent to implementation, the Contractor Team and the Project Program 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.
- **Additional meetings as needed.**

16. REPORTS

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.

Ad Hoc Reporting: The Contractor's system must provide ad-hoc reporting. The Contractors system must be capable of exporting results in PDF, Excel or CSV format. The ad-hoc function returns results for 31 days. If running reports from the report's menu, PayPoint allows a maximum of 31 days. Additional data may be available depending upon the size of the data requested and returned.

- Contractors' system must allow for the ability to export search results.

- **Display Fields:** The Reporting provides 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 and Email Address
    i. Reference field
    j. Approval Code
    k. Confirmation Number
    l. Agency Name
    m. Application Name
    n. Settlement Date
    o. Settlement Batch Amount
    p. Card Type
    q. Payment Status
    r. Column Sub-Totals and Totals for number of transactions and dollar amounts

- **Reporting Options**: 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. Site, Agency, Agency Application
    g. Payment Channels
    h. Payment Type

- **Report Sorting:** System must allow user to sort the report by any specified field in ascending or descending order once the file has been exported to CEPAS The exported report can then be manipulated by CEPAS to meet their needs.

- **Reporting Templates:** System must provide the ability to create templates for reports that can be run without re-entry of data/field requirements using the standard available data fields. Templates created must be available for each user that created the template.

- CEPAS Incident Reports: The Contractor is required to provide written responses to CEPAS Incident Reports and maintain an Incident Report Summary document. Written responses to incidents reports are due within 10 business days of the receiving incident.

Security Performance Reports: The Contractor must provide Security Performance Reports weekly to designated State areas (i.e. Treasury Office of Financial Services)
Reports must show actions of users with User Management roles.

Report must contain:

- Username
  Description of action taken
  User name that made or took the action
  Date & time of change

SOC 1 and SOC 2 Type II and PCI Reports:

1. The Contractor must supply the Program Manager or designee annual FDR SOC 2 Type II audit for the data center environments, a SOC 1 TYPE II for PayPoint and ACH services processor, and PCI Attestation of Compliance (AOC) annually for the provided solution. A current NDA is required prior to any SSAE 18 audits, AOCs, bridge letters being released to DTMB.

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

3. The Contractor will be responsible for obtaining SOC 1 Type II 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. Per the SSAE 18, or current standard, any areas of weakness will require follow-up of Contractor and/or subcontractor. Per the standard, management responses and corrective action plans are noted in the report.

Billing Report: The Contractor must provide billing report(s) with details supporting the monthly invoice. The report(s) must include (but are not limited to) details for transactions, ACH returns, ACH account verifications and any credits), included on the invoice.

Management Reports: Management Reports are to be provided electronically to the designated Treasury staff by the 15th calendar day of the next month. The Contractor must provide monthly Management Reports including:

a. A fiscal year 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.

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.

17. PROJECT MANAGEMENT

Change Management During the terms of the Contract, 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 Central Procurement Services 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 Contract.

A written Change Notice must be signed by both parties to authorize implementation of the investigated changes. Change Notices will be processed through the State's DTMB Central Procurement Services.

The Contractor will utilize an in-house management system. Once the 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.

18. ADDITONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE A – TABLE 1 - Business Specification Worksheet

WORK AND DELIVERABLE
Contractor must provide Deliverables/Services and staff, and otherwise do all things necessary for or incidental to the performance of work identified **in Schedule A – Statement of Work**:

A. GENERAL TASKS - Reserved
A1. **Eastern Time Zone:** For reporting analysis, the system must allow the State to set the time stamps and time references on the Contractor's system to the Eastern Time zone.

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.

B2. **Track Program Activity:** The Contractor's system must be capable of tracking individual business application activity at the application level, agency level, and statewide level and summarizing transactions at the, agency, and statewide level.

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.

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.

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.

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 reference 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. The time period (in minutes) 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, Discover and American Express rules (e.g. Visa requires the payment and the convenience fee to be combined and processed as one transaction).

B8. **Settlement:** Contractor's system must allow for settlement processing seven (7) days a week. Funding occurs on business banking days.

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 **Schedule G - 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.

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.

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

C.) The system must have the capability to submit credit/debit card authorization requests and retain the approval codes. For transactions that receive a successful approval, the system must have the capability of submitting card transactions to TSYS and eCheck transaction to ACH services provider. 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/ACH services provider prior to sending the files. For example, transactions with alphanumeric zip codes may need to be changed to all zeros.

IAT (international ACH transaction) is not supported.

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

B11. **Credit/Debit Card Tasks**
Currently, the State accepts Visa, MasterCard, American Express and Discover credit/debit cards. 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 Law, Merchant Operating Guides for the credit cards, Payment Card Industry Data Security Standards, and other regulations that may apply.

Debit card (signature) 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 , Discover or American Express

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.

A.) **Payment Methods:** The Contractor's system must accept the following payment methods:
a.) Credit and off-line debit card – Visa, MasterCard, American Express and Discover processed through the credit card network.

b.) Debit Cards, PIN less – These transactions are processed through the debit card network.

B.) **Payment Channels:** The payment will be single entry. The Contractor's system must have the ability to accept payments initiated by any interface that supports either integration via Web Services or HTTPS protocols, such as:

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.

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.) Reference 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), captured, not stored.
1.) 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.)
i.) Other data as required by Visa, MasterCard, and Discover.
j.) A shipping address if different from the billing address.

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.) Reference 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.) Truncated Credit/Debit Card Number (e.g. Last 4 numbers)
k.) Payment Date (with a minimum search date range of 6 months of transaction data for a single search)
l.) Payment Status

The Contractors system must be capable of exporting search results in Excel CSV format. The ad-hoc search function returns results for 31 days. If running reports from the report's menu, PayPoint allows a maximum of 31 days. Additional data may be available depending upon the size of the data requested and returned.

E.) **Transaction Detail:** 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.) Reference 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

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). Batch files are submitted in a pre-defined XML format, which is documented in our Merchant Integration Guide. Files are processed in a First In/First Out order. 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.

2. Authorization requests must be returned in an average of 3 seconds or less. Contractor 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; subject to any rules or regulations by Associations or Networks. The Contractor's system will process authorization reversals for transactions voided in the same day.

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; subject to any rules or regulations by Associations or Networks. The Contractor's system will ensure that the refund amount does not exceed the original payment amount.

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; subject to any rules or regulations by Associations or Networks.

2. The Contractor's system will only allow refunds of previously successfully processed transactions 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 supported processor/acquirer listed below

- PayPoint Gateway supports TSYS, Elavon, and First Data merchant processing affiliates and their respective sponsor banks.

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), subject to TSYS certification.

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.

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.

K.) **Merchant Number:** The Contractor's system must capture and store the merchant number.

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.

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

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

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 must have edits/internal controls in place to make sure that only successfully authorized transactions are included in a settlement batch. Settlement errors are reviewed, and alerts are sent to the 7x24 monitoring staff who are able to work with the processor to determine cause of the error and make appropriate adjustments, as necessary. Settlements are executed at the times specified by the State.

5. The Contractor must maintain certification to TSYS during the contract period of performance and ensure transactions are processed correctly to TSYS and process the transaction/batch data in the required time frames to TSYS in order for the State to receive the lowest applicable interchange (processing fee) rate. The Contractor is not responsible for TSYS processing and certification to the State's acquirer.

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 State will notify the Contractor of issues and provide supporting documentation of the interchange rate(s) that a set of transactions should have qualified for. Contractor will review supporting documentation and reserves the right to do their own analysis.

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

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 services mandated by the card networks. Contractor may charge a one-time implementation fee and or per transaction fee for the use of the new or enhanced fraud prevention services not currently listed in the fee schedule or where development is required.

N.) **End-to-End Encryption:** The State utilizes End-to-End Encryption (E2EE) for its Point of Sale (POS) devices in order to minimize Payment Card Industry Data Security Standard (PCI DSS) exposure.

The solution must be capable of processing with TSYS.

The contractor must continue to support the E2EE solution. Including, but not limited to recertification.

The Contractor must ensure the solution is compliant with the current PCI DSS requirements.

The Contractor provided a white paper (per PCI DSS) to demonstrate the E2EE solutions design contains proper security and end to end encryption that qualifies the state for reduction in PCI scope or be a "listed P2PE solution per the PCI Data Security Council. Upon request. Fiserv will work with P2PE QSA to provide a quote for additional services as needed.

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.

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.) Truncated account number (ex. Last 4 digits)
g.) Reference Field data
h.) State (aka Site)
i.) Agency
k.) Application
l.) Truncated account number only

All date range searches must be capable of searching at least 1 month of transaction data in a single search. The Contractors system must be capable of exporting search results in Excel or CSV format.

C.) **Search Capability:** The Contractors system will allow users with the appropriate access rights to search a minimum date range of 1 month in a single search.

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.) Reference 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

E.) **Verification of Routing Transit Numbers:** 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 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, unless prohibited by NACHA regulations.

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 outstanding original transaction and refunds can only be issued on previously settled transactions.

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, 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.

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 transactions in a payment pending status. ACH transactions that are being warehoused by the Contractor. The cancellation must take place prior to the transaction being processed for settlement.

I.) **Settlement:** The Contractor will submit the settlement request to ACH services provider seven days a week.

a.) Separate Batches: At the designated settlement cut off time currently 11:59 p.m. ET (designated by the States application configuration) the Contractor's system will assemble the day's ACH transactions and forward to ACH services provider.
b.) The transactions will be processed for each 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.

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 for use with 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.

K.) **Standard Entry Class Codes:** The Contractor must use the appropriate NACHA Standard Entry Class Codes for ACH transactions processed under this contract, based upon the configuration requirements from the State, listed in the boarding document.

L.) **Legal and Rule Compliance:** The Contractor agrees that all processes related to ACH processing are in compliance with all applicable laws, rules, and regulations, including, but not limited to the NACHA Operating Rules, applicable State of Michigan legislation, Federal law and any other provisions of U.S. law and will remain in compliance throughout the contract term.

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

N.) **ACH Services:** The following tasks relate to the ACH Services:

1.) Any cost associated with the ACH services are to be included in the per transaction fee price.

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

3.) The Contractor will process ACH debit transactions on behalf of the State.

4.) The Contractor will be the point-of-contact for questions and issues related to daily operations. The Contractor is expected to provide detailed responses to routine questions relating to issues within one business day of the question being presented to the Contractor's designated contact. System issues where the application is unable to process payments will require response within one hour of the question being presented to the Contractor's designated contact.

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

6.) The Contractor is responsible for its compliance with NACHA Operating Rules, including the requirement that it undergoes an annual compliance audit via an SSAE18 (or current), SOC 1, SOC 2, and applicable bridge letter(s) The Contractor must provide a copy upon State of Michigan's request its annual compliance audit results to the Project Manager or designee upon completion of each annual audit. A proprietary information sharing agreement is required prior to any SOC audits, bridge letters being released to DTMB.

7.) The Contractor will provide complete and thorough documentation that describes the processing flow, unique processing rules, risk mitigation techniques, and set up requirements for ACH services.

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

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.

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.

3. The State requires 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. The “from” email address must be a contractor payment processing address.

4. The Contractor must ensure that the actual return code is presented on the Contractor’s system. No consolidation of return codes is allowed.

R.) **Reserved.**

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 States financial institution’s 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 will correct the problem within 48 hours of notification of such inaccuracies.

The daily liquidated damage amount (undeposited funds) will be calculated as follows:

- (“Value of Undeposited Funds” X “Treasury Bill three-month “ask yield” as stated in the last Friday of each month’s Wall Street Journal”) / 365 = (Daily Liquidated Damage Amount X Number of Days Delayed) = Liquidated Damage Amount

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.

A.) **Registration Process:** Based on State’s configuration, 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.

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 the necessary preliminary analysis of financial account information to identify and reject invalid Routing Transit Numbers, credit card numbers that do not pass check digit routines, or have invalid expiration dates. 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 unique 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 based on State configuration. When the customer logs in and chooses to make a registered payment, the business application will present a list of registered accounts only displaying the last four (4) digits of any account number and or a nickname created by the customer. 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.

2. **Registered Account Information:** Based on State configuration, the customers can set up both credit/debit 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.

3. **State Business Application using PayPoint API:** 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.

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

5. **Security:** The Contractor will ensure that financial data in transit and at rest will be encrypted using Federal Information Processing Standards (FIPS) validated encryption algorithms with a minimum key size of 128-bits and Transport Layer Security (TLS) version 1.2 or compliance with current non-deprecated FIPS encryption standard. A minimum of 128-bit AES encryption will be used for storage of confidential information.

6. **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.

7. **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 response file from the batch request to the submitting agency application. The response file will contain the original Registration CRD and Registration CRD results ID along with the newly assigned Registration ID.

8. **Returns:** 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.

9. **ACH Account Validation:** Contractor system must support ACH account validation for new accounts per the NACHA WEB Debit Account Validation Rule. Contractor system must return values for each web debit rule account validation request. The values returned are as follows:

Definition	Result
Known bad bank account	KnownBad
Unknown bank account	Unknown
Bank account seen but transaction not yet settled (5 days)	SeenButNotSettled
Known good bank account	KnownGood

Pricing for ACH account validation can be found in Schedule B – Pricing .

Monitoring NACHA WEB Debit Account Validation Rule Validation Results
Authorized users can monitor the results of the account validation process on the registration details page, on a new report, and on your billing report.

Registration Details Page
For registration using consumer eCheck as the payment medium, two fields display the validation result and validation date in the E-Check Information section of the registration details page. Account validation is not applicable to a corporate account/business e-Check, only to consumer accounts.

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.

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. Only the last four (4) digits of the account number will be displayed. Agency staff must have the ability to reactivate disabled accounts.

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 multi-factor authentication verification, when available, 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; subject to the States customized message available through the Consumer Payment website configuration. Identity federation outside of the State or Contractors directory services is prohibited. Currently, PayPoint manages all user login access.

3. **Disable Scheduled Payments:** The Contractor's system must provide the capability to State users with the appropriate access to disable scheduled payments.

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 allow warehousing of payment transactions up to 365 days.

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

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 limited customization to provide a seamless transition from the agency's website.

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.

B.) **Payment Methods:** The solution will support collecting payments via all major credit cards, ECheck, 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 provide a similar look and feel 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.

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

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.

G.) **Website Connection Options:** The Contractor's solution must allow customers to utilize a defined URL 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.

H.) **Pricing:** Separate per item fees will be charged for transactions processed through the hosted solution. See Table 4 - Schedule B – Pricing. 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 - Schedule B – Pricing. Also the Contractor will enter separate additional per item fees for utilizing other functions of the solution (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.

C. SECURITY CONTROL REQUIREMENTS

C1. **Management Controls**

A.) **Security Risk Assessment**

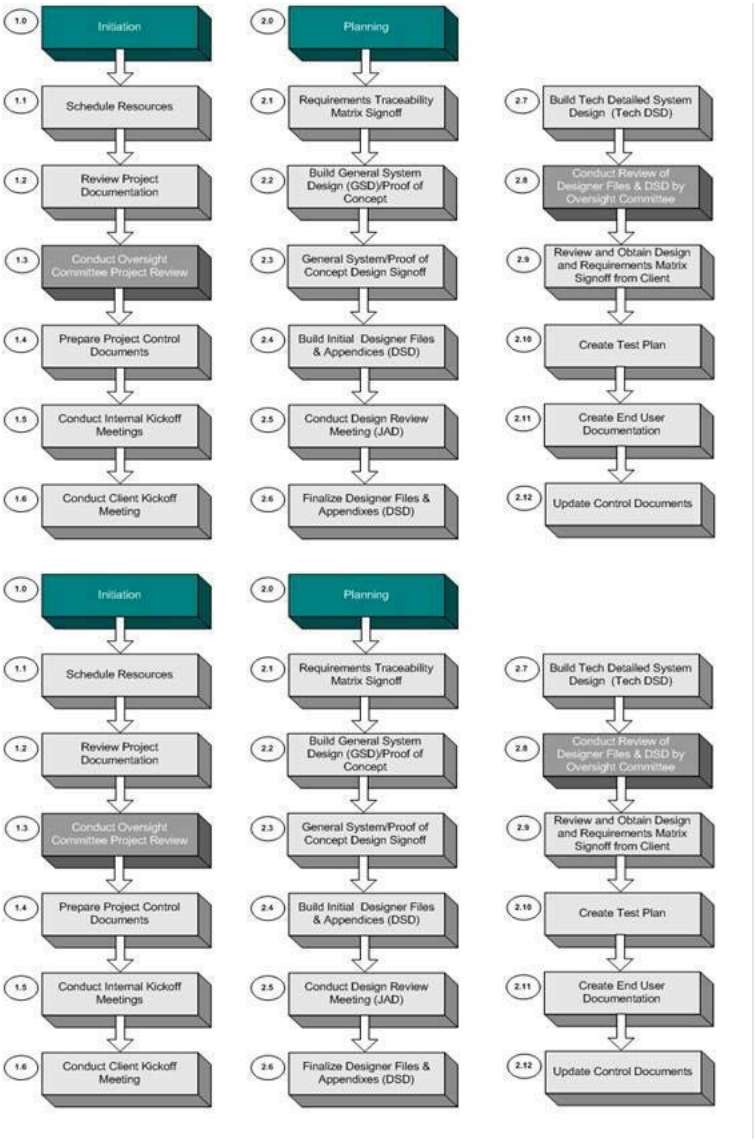
The assessment of potential risks and the type of risk (personnel, equipment, customer, logistics, or organization) are imperative throughout the project. The security risk assessment is a tool used by the State of Michigan, Departments of Information Technology and Treasury to identify risks and determine 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.

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.



C.) **System Security Plan**
The Contractor shall develop, publish, maintain and internally 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.

D.) **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.

E.) **Security Performance Reporting**
The Contractor will be required to supply monthly reports that reflect system performance including number and duration of outage events, and other information required to monitor the performance of the system. The details and timing of the reports will be determined during implementation.

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.

A.) **Personnel Security**
The Contractor shall have a formal documented, published, maintained, and internally 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 Standard 1340.00.130.02 (See Standard at https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf.

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).

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. Have a business continuity and disaster recovery plan and procedures addressing contingency roles, responsibilities and activities associated with restoring system after a disruption or failure.

2. 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.

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 including all backups using secure key management and recover option for off-site backups.

3. Periodically review/update formal documented procedures to facilitate full recovery and reconstitution of the information system.

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 maintain 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 (Treasury Electronic Receiving Section, Amy Kelso kelsoa@michigan.gov) must be informed promptly, but no later than 24 hours after identification of confirmed security incidents affecting the State. When feasible, decisions on how to handle the issues should include input from the Project Manager or designee.

4. Test Incident Response plan at least annually.

5. Personnel trained in their incident response roles and responsibilities at least annually.

The Contractor will maintain a security program which is consistent with the Contract terms, including any schedules and attachments, NIST, applicable laws, and regulatory requirements. The program and policies are reviewed annually and shall not make changes which adversely affect security controls.

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.

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.

G.) **Media Protection**

1. The Contractor shall implement a variety of measures, including FIPS validated encryption for application media, 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 internally 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.

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, tape, or any other data storage media must be destroyed by overwriting all data a minimum of three times or for magnetic based media, running a magnetic strip over and under entire area of disk at least three (3) times. If the media such as a 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 in compliance with state standards based on retention periods required by the Department of Treasury.

- 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 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.

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 internally disseminated Media Destruction and Disposal policy that addresses purpose, scope, roles, responsibilities and compliance; and formal documented procedures.

I.) **Data Security**
The Contract must meet the security requirements listed below in addition to those set forth in the Contract terms, including any schedules.

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) SP 800-53 publications; Control Objectives for Information and Related Technology (COBIT); and national security best practices regarding protection of confidentiality, integrity, 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, Transport Layer Security (TLS), dedicated leased line or Virtual Private Network (VPN).

4. The Contractor must use data encryption techniques whenever data is transmitted to and from a remote site.

5. The Contractor shall process personal, confidential, and sensitive data as well as State customer metadata only for purposes described in the contract.

6. The Contractor shall not disclose or transfer metadata 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 State of Michigan as a result of this contract 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.

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 website , MasterCard's website , and the PCI Security Council website.

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

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.

3. 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.

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

5. In addition to the requirements set forth in the Contract terms, the Contractor will contact the Department of Treasury, Financial Services, CEPAS Program Manager or Office of Financial Services 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 Chief Privacy Officer, unless otherwise prohibited by law. In the event of a security intrusion, the Contractor agrees to cooperate with Payment Card Association requirements.

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

7. The Contractor will advise the Michigan Department of Treasury of all failures to comply with the PCI Data Security Requirements. The Contractor will provide a bridge letter for all lapses in compliance documents.

8 The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review. Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

C4. **Security User Monitoring Reports**

The Contractor shall have audit logs that assist in selecting pertinent information to create monitoring reports. This report can be ran by the State. The audit log fields include but are not limited to:

User Name
Application Name
User Role
Action taken
Date and time of action

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 by the State, for each user profile, 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 internally disseminated User Access Control document that address purpose, scope, roles, responsibilities and compliancy.

1. The Contractor shall periodically, but no less than annually, verify the legitimacy of Contractors employee 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.) Application Name(s)
c.) Role based Access Rights

3. The Contractor must allow the State to establish appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals through role based access rights.

4. The information system shall enforce the most restrictive set of rights/privileges or accesses granted to users (or processes acting on behalf of users) for the performance of specified tasks.

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.

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 if requested by the customer to prevent compromise of personal, confidential or sensitive information.

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

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. The information system security training plan must be documented and monitored.

a.) The Contractor shall develop, internally 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.

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

3. System protects audit information from unauthorized access

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

5. Audit logs are retained for a sufficient period of time, 2 years online and 5 years offline

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.

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.

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 internally 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.

J.) **Network Security**
The Contractor is responsible for the security of and access to the State's information. The Contractor and its sub-Contractor must have documented network security policies and procedures that address purpose, scope, roles and responsibilities.

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).
h.) Dynamic Application Security Testing (DAST) – Scanning interactive application for vulnerabilities, analysis, remediation, and validation (may include IAST). Contractor must dynamically scan the application source code of the deployed version of the solution using an industry standard application scanning tool, and provide the State a vulnerabilities assessment after Contractor has completed each such scan; further these scans and assessments i) must be completed quarterly and for each major release, and provided to the State upon request; ii) scans must be completed with verifiable matching source code and supporting infrastructure configurations.
i) Static Application Security Testing (SAST) – Scanning source code for vulnerabilities, analysis, remediation, and validation. For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete the scanning and the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code, and for all source code for each major release.
j) Software Composition Analysis (SCA) – Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation. For software that includes third party and open source software, all included third party software must be documented and the source supplier must be monitored for notification of identified vulnerabilities. SCA scans may be included as part

of SAST and DAST scanning or employ the use of SCA tool to meet the scanning requirements. These scans must be completed for all third-party code initially, for all updated third-party code, and for all third-party code in each major release.

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 44 minutes 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 with the State's site content or the State's programming errors;
c.) Problems caused by systems administration, commands, or file transfers performed by the State's representatives;
d.) Interruptions in third party networks that prevent users of the Internet from accessing the State Web site;
e.) Other activities the State directs, denial of service attacks, other regulatory actions or court orders.
f.) Lack of availability or untimely response by the State to incidents that require the State's participation for problem source identification and/or resolution.

When the accumulated monthly outage exceeds 44 minutes of outage per calendar month, the Contractor is subject to Monetary Assessments as defined in section **Schedule D**. 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 Contractor may perform maintenance weekdays after 8:00 pm ET, for updates that do not require system outages.** The maintenance window designated for the Contractor to perform system Maintenance that requires system down time 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 ten (10) 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 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 10-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.

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.

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 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 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.

D3. **TSYS Processing Connectivity:** The Contractor must work with the State to ensure that the connectivity solution obtains the lowest authorization cost with the State's credit card acquirer. The Contractor is responsible for all costs associated with ongoing maintenance of the connection.

A.) **Server-level Logs:** The Contractor must have the ability to maintain an electronic server-level log of all transactions to and from Michigan's credit card processor. Server logs are retained for a minimum of 14 days.

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.
- 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.

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 backup site must be physically separated from the primary site by a distance of at least 30 miles. The backup 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 (30) day notice. The Contractor is expected to perform functional testing to its Disaster Recovery site at 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 backup site must be completed in four hours or less from the time the primary site fails or the decision has been made to roll it over.

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.

D8. **Application Program Interface (API):** The Contractor must provide APIs to facilitate its payment processing functionality. 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 customizable generic Web and IVR hosted solution as described in requirement B14.

d.) 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 make the response file available so that the State can retrieve the file from the FTP server.

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.

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. Transaction data must be provided to the State upon request, for State transactions, to assist with problem resolution. Logs must be retained for 14 days.

D12. **Planned System Upgrades / Changes / New Releases:** The Contractor will:

a.) Notify the Contract Compliance Inspector or designee at least 60 calendar days in advance of when system changes (hardware/software) are planned.

b.) Provide detailed release notes that describes the changes at least 21 calendar days prior to implementation. The release notes must describe the existing process, the new process, what changed, and the reason for making the change.
E10
c.) Must provide updated merchant integration guide, best practice guide, consumer payment integration guide, merchant integration guide, and user guide at least 21 calendars days prior each new release.

d.) Place a testable version of the changes in the Test Environment at least 13 calendar days prior to implementation to allow for agency application testing.

D13. **Test Environments:** The Contractor will:

a.) Provide access to fully functioning test environment that has similar functionality as production.
b.) Ensure transactions processed in the Test environment will not be processed for financial settlement; a mock settlement will be completed in the Test environment to simulate settlement.
c.) Ensure test results for each testing application must be separate from other application test results.
d.) Provide a separate posting file that will be generated for transactions processed in the test environment.

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

,

A.) **Testing Environments:** The Contractor must make available one individual test environment for the State's use. This will be referred to as the User Acceptance Testing (UAT) environment.

B.) **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. UAT will support 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 Posting File (see D15 below) that contains the previous days test transaction detail for transactions processed in the UAT environment.

D.) **Repeatable Test Cases in Application Development:** The Contractor must supply a set of at least 6 repeatable test cases that validates make payment, refund, status call, and registration functions to ensure the API is properly integrated into an application in the Application Development Test domain. The test cases must be evaluated using pass or fail, yes or no logic.

D15. **Posting File:** The Contractor will supply a daily posting 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 Posting file:

A.) **Posting file Contents:**

a.) The file shall be in a straight or delimited ASCII format.
b.) The posting 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 posting file must equal the dollar value of the day's transactions in the settlement batches for each application.
e.) Refund transactions included in the posting file must contain enough information to allow for linking the refund back to the original transaction.
f.) 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 posting file must be available for five (5) or more calendar days after creation. It must be available in archive for a minimum of 30 calendar days on the PayPoint admin site.

B.) **Posting file Retrieval:** The Contractor must:

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 (encrypted) FTP method.
c.) Maintain the secure FTP server and the State will maintain the secure FTP client.
d.) Inform the State designated contact if the file is unavailable at the agreed time.

D16. **Data Retention:** Transaction data must be retained for a minimum of 24 months on-line, and 60 months off-line for a total of seven (7) years. Audit data which includes, but is not limited to, adding, deleting and modifying user accounts must be retained for a minimum of 7 years.

.

a.) In addition to the requirements set forth in the Contract terms, including any schedules, 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.

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 CSV or 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, registration/enrollment IDs, Agency Application IDs, customer address, reference data, 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 posting 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 to read only screens and reports, so that no new transactions can be authorized.

c.) At the end of the seven (7) year period 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 managers access to their system, upon request from the State. 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, upon request from the State.

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.

E. CONTRACTOR SUPPORT

E1. **Dedicated (Single Point of Contact) Business and Technical Contacts:**

a.) The Contractor must provide a dedicated business and technical contact 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 backups. 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.

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 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).

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.

E4. **System Business Documentation:** The Contractor must provide the State with detailed documentation describing the Contractor's PayPoint application/system. , Business documentation must include:

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

E5. **System Technical Documentation:** The technical documentation must describe the PayPoint system in detail to foster complete technical understanding of the Contractor's entire product in all its environments utilized by the State and must include:

a.) **Data Dictionary:** A complete data dictionary describing every data item used in the Contractor's system must be documented in the PayPoint guides. Naming conventions used in the Contractor's system must be thoroughly documented within the PayPoint guides, for example the term CVV2 is explained as Card Verification Value 2 for Visa.

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.

k.) **Unique Software Requirements:** 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.) **User Guide:** Contractors must provide a detailed user guide on use of the PayPoint system.

E6. **Best Practices:** The Contractor will provide a best practice guide containing discussions of technical best practices to assist agencies in integrating with the Contractor's system.

E7. **Training:** If changes to the PayPoint system necessitate additional training, the Contractor will work with and train Treasury staff on the new functionality. The State will be responsible for passing the training down to the Agencies. The Contractor will provide detailed and comprehensive training that covers all aspects of the new functionality of the Contractor's system. Training will include support documents as required to explain or provide detail of the new functionality. The Contractor will provide a training session(s) to train the Office of Financial Services

CEPAS Agency Liaisons and management (see Section 19, State Resources/Responsibilities). 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.

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.

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.

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.

E10. **New PayPoint Application Set-Up:** The Contractor must complete set-up of new credit card applications within 5 business days and E-Check accounts within 10 business days of request from the State.

F. **BANKING**

F1. **ACH Application Deposit Identification:** At agency application set up for ACH debit programs, CEPAS 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.

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.

F3. **Company Name and Entry Description:** Per NACHA specifications and at agency application set up for ACH debit programs, CEPAS 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.

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).

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.

G. **SOFTWARE MODIFICATION**

a) Contractor 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 the mutually agreed upon change request will be used for all software modification provided either on a fixed-price or T&M basis.

b) Contractor 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 Contractor and MDTMB.

c) The Change Management process may be modified as mutually agreed by Contractor and MDTMB.

SCHEDULE B – PRICING

Compensation and Payment

A. **Firm Pricing:** All prices will be firm for the term of the Contract. If the Contract is extended beyond the initial term of the Contract, the State and the Contractor may negotiate price.

B. **Unit Price Contract:** This is 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 (with the exclusion of NACHA or card association passthrough fees):

- an authorization
- an ACH return
- communication failures
- errors
- chargebacks
- duplicate transactions attributable to the Contractor
- refunds of duplicate transactions attributable to the Contractor

C. Pricing

Transaction Fee Pricing: The transaction fees include all costs for providing the system defined in the Statement of Work. The State expects volume discounts in the transaction fee pricing based on a monthly review of the transaction volume processed

Bank of Hours: This bank of 1000 hours is to be used for customized enhancements that the State may request.

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). The 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 also must 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, Office of Financial Services Division.

<table>
<tr><th>Billing #</th><th>Element</th><th>Description</th><th>Price (USD $)</th><th>Per Unit</th></tr>
<tr><td>5243</td><td>GATEWAY FEES FOR CARD TRANSACTIONS</td><td>This element identifies the charge for processing PayPoint transaction for One-time Card transactions and Recurring Card Transactions.</td><td><table><tr><th>Unit Price</th><th>Range of Monthly Transactions</th></tr><tr><td>0.150</td><td>0 - 150,000</td></tr><tr><td>0.140</td><td>150,001 - 250,000</td></tr><tr><td>0.130</td><td>250,001 - 300,000</td></tr><tr><td>0.130</td><td>300,001 - 350,000</td></tr><tr><td>0.120</td><td>350,001 - 400,000</td></tr><tr><td>0.110</td><td>400,001 - 450,000</td></tr><tr><td>0.095</td><td>450,001 - 500,000</td></tr><tr><td>0.095</td><td>500,001 - 550,000</td></tr><tr><td>0.085</td><td>550,001 - 600,000</td></tr><tr><td>0.085</td><td>600,001 - 650,000</td></tr><tr><td>0.080</td><td>650,001 - 700,000</td></tr><tr><td>0.080</td><td>700,001 - 750,000</td></tr><tr><td>0.080</td><td>750,001 - 800,000</td></tr><tr><td>0.080</td><td>800,001 - 850,000</td></tr><tr><td>0.080</td><td>850,001 - 900,000</td></tr><tr><td>0.080</td><td>900,001 - 950,000</td></tr><tr><td>0.080</td><td>950,001 - 1,000,000</td></tr></table>
Note: Transactions for Element 5243 only are Pick the Tier above.</td><td>/transaction</td></tr>
<tr><td>5245</td><td>GATEWAY FEES FOR ACH TRANSACTIONS
(With TeleCheck ACH processing)</td><td>This element identifies the charge for processing One-Time eCheck Transactions and Recurring eCheck Transactions.

This includes successful, declined, and cancelled eCheck payments with standard eCheck processing.

Standard eCheck processing includes basic processing through TeleCheck. Additional TeleCheck services are priced and contracted separately.

For applications that charge convenience fees separately, two transaction fees will be incurred- one for the primary payment and a separate fee for the convenience fee.</td><td><table><tr><th>Unit Price</th><th>Range of Monthly Transactions</th></tr><tr><td>0.150</td><td>0 - 150,000</td></tr><tr><td>0.140</td><td>150, 001 - 250,000</td></tr><tr><td>0.130</td><td>250,001 - 300,000</td></tr><tr><td>0.130</td><td>300,001 - 350,000</td></tr><tr><td>0.120</td><td>350,001 - 400,000</td></tr><tr><td>0.110</td><td>400,001 - 450,000</td></tr><tr><td>0.095</td><td>450,001 - 500,000</td></tr><tr><td>0.095</td><td>500,001 - 550,000</td></tr><tr><td>0.085</td><td>550,001 - 600,000</td></tr><tr><td>0.085</td><td>600,001 - 650,000</td></tr><tr><td>0.080</td><td>650,001 - 700,000</td></tr><tr><td>0.080</td><td>700,001 - 750,000</td></tr><tr><td>0.080</td><td>750,001 - 800,000</td></tr><tr><td>0.080</td><td>800,001 - 850,000</td></tr><tr><td>0.080</td><td>850,001 - 900,000</td></tr><tr><td>0.080</td><td>900,001 - 950,000</td></tr><tr><td>0.080</td><td>950,001 - 1,000,000</td></tr></table>
Note: Transactions for Element 5245 only are Pick the Tier above.</td><td>/transaction</td></tr>
<tr><td></td><td>ACH Validation for NACHA Web Debit Rule</td><td></td><td>0.05</td><td>/transaction</td></tr>
<tr><td>5246</td><td>CONSUMER PAYMENTS</td><td>This element identifies the per transaction surcharge for a payment using Consumer</td><td>0.07</td><td>/transaction</td></tr>
</table>

<table>
<tr><td></td><td></td><td>Payments Web in addition to the Gateway Fees.

Excludes applications that “redirect” to Consumer Web pages.</td><td></td><td></td></tr>
<tr><td>5247</td><td>CONSUMER PAYMENTS SUMMARY PRESENTMENT</td><td>This element identifies the per transaction surcharge to use summary presentment feature – includes uploading summary billing data and displaying it to a consumer using the Consumer Payments interface in addition to the Gateway Fees.</td><td>0.07</td><td>/transaction</td></tr>
<tr><td>5244</td><td>IVR MINUTES</td><td>This element identifies the charge for telecommunication fees for using Consumer Payments IVR.</td><td>0.10</td><td>/transaction</td></tr>
<tr><td>5249</td><td>DEVELOPMENT SURCHARGE</td><td>This element identifies the custom project charges, including but not limited to: consultation, project management, development, and testing. Custom projects beyond the scope of standard initial onboarding will be quoted separately.</td><td>150/hour</td><td>One-time</td></tr>
<tr><td>5275</td><td>NACHA UNAUTHORIZED RETURN FEES</td><td>This element applies only to Clients who use PayPoint/TeleCheck services and identifies the charge for each eCheck return received for one of the following NACHA Unauthorized Return Codes:
<table><tr><th>Return Code</th><th>Return Description</th></tr><tr><td>R05</td><td>REQUIRED PRENOTIFICATION NOT RECEIVED</td></tr><tr><td>R07</td><td>AUTHORIZATION REVOKED BY CUSTOMER</td></tr><tr><td>R10</td><td>CUSTOMER ADVISES NOT AUTHORIZED</td></tr><tr><td>R29</td><td>CORPORATE CUSTOMER ADVISES NOT AUTH</td></tr><tr><td>R51</td><td>ITEM IS INELIGIBLE, NOTICE NOT PROVIDED, SIGNATURE NOT GENUINE</td></tr></table></td><td>5.00</td><td>/eCheck Return</td></tr>
</table>

Monthly Invoice: The Contractor must provide a monthly invoice no later than 10 calendar days of the next month.

SCHEDULE C - INSURANCE SCHEDULE

Required Coverage.

1.1 **Insurance Requirements.** Contractor, at its sole expense, must maintain the insurance coverage identified below. All required insurance must: (i) protect the State from claims that arise out of, are alleged to arise out of, or otherwise result from Contractor's or subcontractor's performance; (ii) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (iii) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Personal & Advertising Injury $2,000,000 Products/Completed Operations $2,000,000 General Aggregate	Policy must be endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
If a motor vehicle is used in the performance of the Contract, Contractor must maintain motor vehicle liability coverage for bodily injury and property damage, as required by law.	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Annual Aggregate	Policy must cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.
Crime (Fidelity) Insurance	
Minimum Limits: $1,000,000 Employee Theft Per Loss	Policy must: (1) cover forgery and alteration, theft of money and securities, robbery and safe burglary, computer fraud, funds transfer fraud, money order and counterfeit currency,

	and (2) be endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as Loss Payees.

1.2 If any required policies provide claims-made coverage, the Contractor must: (i) provide coverage with a retroactive date before the Effective Date of the Contract or the beginning of Contract Activities; (ii) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (iii) if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

1.3 Contractor must: (i) provide insurance certificates to the Contract Administrator, containing the agreement or delivery order number, at Contract formation and within twenty (20) calendar days of the expiration date of the applicable policies; (ii) require that subcontractors maintain the required insurances contained in this Section; (iii) notify the Contract Administrator within thirty (30) business days if any policy is cancelled; and (iv) waive all rights against the State for damages covered by the minimum insurance limits above. Failure to maintain the required insurance does not limit this waiver.

1.4 This Section is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

SCHEDULE D - SERVICE LEVEL AGREEMENT
DOWNTIME

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 16, the State may assess Monetary Assessments against Contractor as specified in this Section. "Monetary Assessment" is an amount agreed to by the Parties with respect to any delay or failure by Contractor to timely perform its obligations in accordance with the Contract.

The Contractor is expected to meet a service level objective of 99.9% availability, less than 10 minutes 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 the following;

- Periods of scheduled or emergency maintenance activities or a scheduled outage;
- Problems with the State's site content or the State'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, other regulatory actions or court orders.
- Lack of availability or untimely response by the State to incidents that require the State's participation for
- problem source identification and/or resolution.

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.

Disaster Recovery

Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan satisfactory to the State in order to maintain a Tier 1 application (the "**DR Plan**"),and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. An overview of Contractor's current DR Plan, revision history, and relevant reports or summaries relating to past testing of or pursuant to the DR Plan is included as part of Contractor's Security Assurance portfolio. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE D - SERVICE LEVEL AGREEMENT

SYSTEM RESPONSE TIME

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 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 16** of the Contract Terms, the State may assess Monetary Assessments against the 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 matter 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 describe 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 2.2 of the Statement of Work. 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 the slow payment response time the Contractor will ne 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 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 will reimburse the State for costs incurred as the result of the Contractor system issues (e.g. staff time to resolve the issue, NSF charges, chargeback fees, additional interchange/processing costs).

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.

SCHEDULE E – DATA SECURITY REQUIREMENTS

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract.

"**Contractor Security Officer**" has the meaning set forth in **Section 2** of this Schedule.

"**FedRAMP**" means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

"**FISMA**" means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014.).

"Hosted Services" means the hosting, management and operation of the computing hardware, ancillary equipment, Software, firmware, data, and other services (including support services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

"Hosting Provider" means any Permitted Subcontractor that is providing any or all of the Hosted Services under this Contract.

"**NIST**" means the National Institute of Standards and Technology. "**PCI**" means the Payment Card Industry. "**PSP**" or **"PSPs"** means the State's IT Policies, Standards and Procedures. "**SSAE**" means Statement on Standards for Attestation Engagements.
"**Security Accreditation Process**" has the meaning set forth in **Section 6** of this Schedule

2. Security Officer. Contractor will appoint a Contractor employee to respond to the State's inquiries regarding the security of the Hosted Services who has sufficient knowledge of the security of the Hosted Services and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**").

3. Contractor Responsibilities. Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to:

(a) ensure the security and confidentiality of the State Data;

(b) protect against any anticipated threats or hazards to the security or integrity of the State Data;

(c) protect against unauthorized disclosure, access to, or use of the State Data;

(d) ensure the proper disposal of any State Data in Contractor's or its subcontractor's possession; and

(e) ensure that all Contractor Representatives comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor's data privacy and information security program be materially consistent with NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in IRS Publication 1075.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the contracted solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

4. Acceptable Use Policy. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred. Contractor access to State's IT environment is not anticipated at the time of contracting.

5. Protection of State's Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause pursuant to **Section 17.1** of the Contract;

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit. based on State required NIST Special Publication 800-53 MOD Controls.

5.3 ensure that the Software and State Data is securely hosted, supported, administered, accessed, and backed up in a data center(s) that resides in the continental United States, and meets the Service Availability set forth in Exhibit [D] – Service Level Agreement;

5.4 maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State Data that is materially consistent with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in IRS Publication 1075

5.5 provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data, consistent with best industry practice and applicable standards (including, but not limited to, compliance with HIPAA, ACH, PCI and applicable law, and materially consistent with FISMA, NIST, CMS, IRS, FBI, SSA, and FERPA requirements as applicable);

5.6 take all reasonable measures to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "malicious actors" and others who may seek, without authorization, to destroy, disrupt, damage, encrypt, modify, copy, access or otherwise use Hosted Services or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) State Data from being commingled with or
contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State Data;

5.7 ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.8 ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities

using Security Assertion Markup Language (SAML), Open Authentication (OAuth) or comparable State approved mechanisms;

5.9 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

6. Security Accreditation Process. Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State's automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor's security controls within two weeks of the State's request. From time-to-time, State may utilize third party hosted SaaS services platform (**Third Party SaaS**) to perform vendor oversight and assess the processes, procedures, and systems of Contractor deliverables provided Third Party SaaS vendor cannot access or use Contractor documentation provided for the Security Accreditation process and uploaded to the third party SaaS solution. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system's controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to create or assist with the creation of State approved POAMs and perform related remediation activities. The State will make any decisions on acceptable risk, Contractor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk. Failure to comply with this section will be deemed a material breach of the Contract.

7. Unauthorized Access. Contractor may not access, and shall not permit any access to, State systems, in whole or in part, whether through the Hosted Services or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this Section. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

8. Security Audits.

8.1 During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.

8.2 Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract. State shall be entitled to perform or to have its authorized agent perform audits to verify Contractor's compliance with this contract. Audits shall: a) take place no more than once per calendar year, b) The scope of any such audit shall be agreed to by the parties not less than 60 days in advance and otherwise in accordance with the audit related terms and conditions set forth in this Section, c) take place during normal business hours, d) allow documents pertaining to audit to be reviewed, however no cameras or electronic recording equipment is allowed, e) allow Auditors to conduct inquiry and limited observation based testing. To the extent that Contractor has undergone a SOC1 Type 2 audit, SOC2 Type 2 audit or PCI-DSS certification, State shall reasonably leverage audit reports and certifications to consolidate and condense requisite testing. The Contractor must make available third party Penetration Testing summary results upon request. Scanning of systems is prohibited. Contractor may, in its sole discretion, withhold any confidential or proprietary information from the Penetration testing results, where disclosure may directly impact client confidentiality or contractual agreements, or where disclosure would jeopardize the safety and

security of Contractor applications or systems.

During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's FedRAMP System Security Plan(s) or SOC 2 Type 2 report(s) to the State within two weeks of the State's request. The System Security Plan and SSAE audit reports will be recognized as Contractor's Confidential Information.

With respect to State Data, Contractor must implement any required mutually agreed upon safeguards as identified by the State or by any audit of Contractor's data privacy and information security program

8.3 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8.**

9. Application Scanning. During the Term, Contractor must, at its sole cost and expense, scan all Contractor provided applications, and must analyze, remediate and validate all vulnerabilities identified by the scans in compliance with Contractor policy and procedures.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Scanning interactive application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST).

(a) Contractor must dynamically scan a deployed version of the Software using an industry standard scanning tool and provide the State a summary assessment report upon written request. These scans and assessments i) must be completed quarterly and for each major release; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

(a) For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code prior to use in a production environment and for all source code for each major release and Contractor shall provide the State a summary SAST report upon written request.

9.3 Software Composition Analysis (SCA) – Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation.

(a) For Software that includes third party and open source software, all included third party and open source software must be documented and the source supplier must be monitored by the Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. These scans must be completed for all third party and open source software initially, for all updated third party and open source software, and for all third party and open source software in each major release and Contractor shall provide the State a summary report upon written request.

9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

(a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programing interface (API).

(b) Penetration Testing – Simulated attack on the application and infrastructure to

identify security weaknesses.

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must ensure the infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements in compliance with PCI and Contractor's policies and standards.

11. Nonexclusive Remedy for Security Breach.

11.1 Any failure of the Services to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

PCI Compliance.
Contractors that process, transmit store or affect the security of credit/debit cardholder data, must adhere to the PCI Data Security Standard. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

The Contractor must notify the State's Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, and Discover) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.
Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

The Contractor must provide the State's Contract Administrator with an annual Attestation of Compliance (AOC) if or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

SCHEDULE F - DISASTER RECOVERY PLAN

Fiserv supplies an overview of its Disaster Recovery / Business Continuity Plan as part of its Security Assurance portfolio. The actual plan can be discussed onsite at data center(s) or via secure virtual video conference.

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 Schedule A, Statement of Work..

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.

CONTRACTOR INFORMATION TRANSITION

Contractor will provide transition assistance as a billable item; using the hourly rate in Schedule B. Contractor will draft a Statement of Work outlining the project purpose, scope, and cost associated with the migration.

RESERVED

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.

SCHEDULE H – 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 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 postdating 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	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 ACH payment. Used to select appropriate SEC code.		Y	
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

SCHEDULE I – ESCALATION PROCESS

MI CEPAS

PayPoint Support Interaction and Escalation Process

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 conduct 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 Jesse Wees 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 Terrance Cherry

In the event is not available, we have assigned your second point of contact as:
PayPoint Support Manager Ryne Weaver

When Terrance and Ryne 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 Terrance or Ryne 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 services 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 is necessary. Support technician will notify the merchant of the expected timeframe for resolution and no escalation will take place.
- Our PayPoint 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 sire 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, ACH services provider, 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
Terrance Cherry 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 eServices Account Management will be the owner of the formal Incident Report response process.

Contacts:

Terrance Cherry, Senior Problem Analyst and Primary PayPoint Support contact.
303.967.5833 direct
303.799-3621 fax
Terrance.Cherry@Fiserv.com

Ryne Weaver, PayPoint Support Manager and Secondary contact

PayPoint Support
877.869.0860
PaySupport@FirstData.com

Ryan Kelsey**, Relationship Manager**
303.967.5833 direct
Ryan.Kelsey@fiserv.com