MISSISSIPPI PAYMENT PROCESSING

Mississippi Interactive (MSI) will serve as the single point of entry for all e-commerce transactions. Awarded vendor will use Mississippi's official payment processor for any of the following services where payment is required.

- Web services
- IVR services
- Mobile services
- Over the counter payment processing services
- Kiosk services
- Lock Box services

The following payment methods accepted through MSI include: Visa, MasterCard, American Express, Discover, electronic check and subscription (monthly billed).

DFA Administrative Rule

The Department of Finance and Administration (DFA) established an administrative rule to be followed when agencies, in accordance with §27-104-33, Mississippi Code of 1972, Annotated, elect to accept payment by credit cards, charge cards, debit cards, electronic check (echeck) and other form of electronic payments for various services and fees collectible for agency purposes. See Attachment 1 for Final Rule.

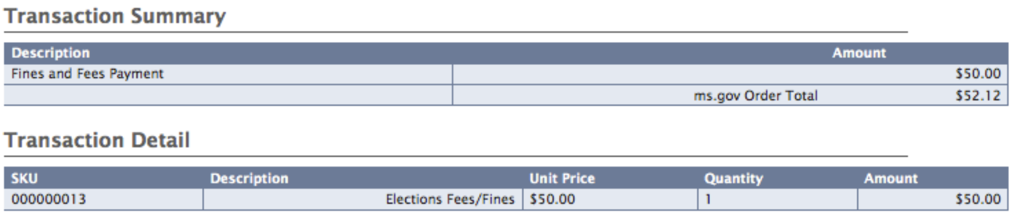
Payment Card Industry (PCI) Compliance

MSI will be responsible for Payment Card Industry (PCI) compliance on behalf of the State. MSI's Transaction Processing Engine (TPE) is certified compliant with the PCI Data Security Standard (DSS) and compliant with the Payment Application Best Practices (PABP) standards. It is also listed as a Validated Payment Application by VISA. TPE is hosted at NIC's Central Data Center in Ashburn Virginia and complemented with a backup facility in Allen, Texas. NIC is certified by PCI-DSS as a Level 1 Service Provider for this environment.

See Technical Requirements for notes to the PCI compliance responsibility of the awarded vendor.

Awarded vendor is prohibited from breaking out payment processing fees associated with any transaction. This includes all pages of the application and/or any receipt generated.

Acceptable fee breakout can include a "subtotal" for services and a "Total ms.gov Price" or "ms.gov Order Total" which includes the eGov processing fee. See image below for example.



Transaction Summary

Description		Amount
Fines and Fees Payment		$50.00
	ms.gov Order Total	$52.12

Transaction Detail

SKU	Description	Unit Price	Quantity	Amount
000000013	Elections Fees/Fines	$50.00	1	$50.00

Merchant of Record

In order to act as the single point of contact between the State, MSI, the payment processor, the merchant acquiring bank, and end users of ms.gov services, MSI will be the "Merchant of Record" for this RFQ. As the single point of contact for the State, MSI will work directly with the processor and the acquiring bank to request and set up merchant accounts and will be responsible for all areas of merchant services, including merchant fees.

eGov Transaction Fees

There will be standard payment processing fees associated with each payment transaction. Customer approval (electronic or otherwise) of MSI payment processing fees will be obtained prior to initiating payment.

Refunds, Chargebacks, Returns

As the merchant of record and official payment processor, MSI will handle all refunds, chargeback representments and returned echecks. However, MSI is not responsible for covering any monies that must be netted from the agency's account through refund, successful chargeback or returned echeck. Below are the processes for each.

Refunds

The refund process is initiated by either customer or agency request.

- Upon customer request MSI will contact the agency financial contact (established at project initiation) for approval prior to refund.
- Agency contacts have access to and are encouraged to use the MSI refund tool for their refund requests. This ensures adequate logs of all requested refunds.
- After agency request or approval MSI refunds the charge in TPE and notifies the requestor upon completion.
- Through MAGIC refunds are netted from the next day's deposits.

Chargebacks

A chargeback is a monetary dispute that is initiated by the Issuing Bank (issuer disputes the posting of the transaction) or the cardholder (a cardholder disputes a transaction).

- Customer or card issuing bank sees what appears to be a suspicious charge on their statement.
- The customer contacts the card company to dispute the charge and initiate the chargeback process. Note: depending on the company policies of the company that issued the card the company may initiate the chargeback without customer notification.
- MSI receives a chargeback email from our processor notifying us of the transaction details of the chargeback. Once this notification is received the processor pulls the funds back from the Portal account until supporting documentation is obtained. (MSI's processor has 45 days from the time the customer disputes the charge to contact MSI for additional information.)
- Based on the information provided in the chargeback notification MSI researches the charge internally first.
    - If the disputed charge is a true duplicate charge (same customer information, amount, etc), MSI allows the chargeback to process and it is automatically marked in TPE.
    - For all non-duplicate charges MSI contacts the appropriate agency contact(s) (financial contact gathered at project initiation) by email to explain the chargeback, provide charge details and verify with the contact that it is a valid charge. If needed MSI requests the agency provides any additional information they may have to support the claim.
- If the charge is valid MSI will provide the sales drafts (chargeback receipt, TPE receipts, agency support etc) back to the processor to support the charge validity.

- After the charge is verified through receipt of sales drafts the chargeback will be reversed and the funds will be deposited back to the agency.

Note: The chargeback process could take up to 60 days to resolve.

Returns

Electronic checks (echeck)/ACH payments (where a user enters an account and routing number) may be returned unpaid for any reason, including non-sufficient funds (NSF), stop payment, online data entry error or closed account. A full list of return codes is listed below:

- R01 - Insufficient Funds - Available balance is not sufficient to cover the dollar value of the debit entry.
- R02 - Account Closed - Previously active account has been closed by customer or RDFI.
- R03 - No Account/Unable to Locate Account - Account number structure is valid and passes editing process, but does not correspond to individual or is not an open account.
- R04 - Invalid Account Number - Account number structure not valid; entry may fail check digit validation or may contain an incorrect number of digits.
- R05 - Improper Debit to Consumer Account - A CCD, CTX, or CBR debit entry was transmitted to a Consumer Account of the Receiver and was not authorized by the Receiver.
- R06 - Returned per ODFI's Request - ODFI has requested RDFI to return the ACH entry (optional to RDFI – ODFI indemnifies RDFI).
- R07 - Authorization Revoked by Customer - Consumer, who previously authorized ACH payment, has revoked authorization from Originator (must be returned no later than 60 days from settlement date and customer must sign affidavit).
- R08 - Payment Stopped - Receiver of a recurring debit transaction has stopped payment to a specific ACH debit. RDFI should verify the Receiver's intent when a request for stop payment is made to insure this is not intended to be a revocation of authorization.
- R09 - Uncollected Funds - Sufficient book or ledger balance exists to satisfy dollar value of the transaction, but the dollar value of transaction is in process of collection (i.e., uncollected checks) or cash reserve balance below dollar value of the debit entry.
- R10 - Customer Advises Not Authorized - Consumer has advised RDFI that Originator of transaction is not authorized to debit account (must be returned no later than 60 days from settlement date of original entry and customer must sign affidavit).
- R11 - Check Truncation Entry Returned - used when returning a check safekeeping entry; RDFI should use appropriate field in addenda record to specify reason for return (i.e., "exceeds dollar limit," "stale date," etc.).
- R12 - Branch Sold to Another DFI - Financial institution receives entry destined for an account at a branch that has been sold to another financial institution.

Typical Return Process

- User enters echeck information in the ms.gov common checkout page
- TPE captures the information and sends to payment service provider
- The service provider submits a request to the payer’s bank to retrieve the funds
- Payer’s bank reports back one of the aforementioned return codes to the services provider
- Service provider notifies MSI and the return is marked in TPE
- Funds are electronically pulled from the agency through the daily SAAS payment interface file. MSI contacts the individual(s) responsible for agency funds (contact obtained during project initiation) by email to let them know of the return and reason.

Hardware Acquisition

Due to the payment key injections required for hardware to be compatible with MSI’s PCI compliant payment processor, any hardware must be acquired through MSI’s existing eGov contract. This includes, but is not limited to, kiosks, pin pad/card swipe, mobile devices etc.

Application Testing

For all new services DFA requires a test transaction to be run for flow of funds and processor verification. After MSI receives confirmation the awarded vendor is satisfied with the integration, one test must be run through production TPE and confirmed by MSI.

It takes three (3) business days (excluding bank holidays) for the transaction to be confirmed by DFA. Awarded vendor should take this time frame into consideration when anticipating launch date.

Reporting

TPE provides reporting and auditing tools useful for streamlining and accommodating various back-office procedures. TPE's financial reporting is comprehensive, flexible, and robust. Within TPE all payment processing data is made available via a wide variety of reporting features. Reports are real-time, up-to-the-minute transaction reporting ranging from summary reports to detail reports showing line-item level data. A comprehensive users guide and applicable training will be provided to agency contacts during integration.

Payment Support

Mississippi Interactive will provide support for all user payment inquiries. MSI is located at 2727 Old Canton Rd., Suite 100, Jackson, MS 39216 and customer payment support is available during normal business hours (Monday – Friday 8am – 5pm CST). MSI's toll free support number (1-877-290-9487) is listed on the ms.gov Common Checkout page and is accessible to all users. For payment emergencies a technical support cellular number will be provided to the State contact.

MSI will work directly with the awarded vendor and/or the agencies to identify, report, track, monitor, escalate, and resolve any technical issues with TPE or CCP. It is MSI's policy to notify all awarded vendors and agencies of planned maintenance windows or system updates to avoid any payment issues.

State entities and/or awarded vendors will not be charged for MSI's efforts during payment implementation or any training/support.

Technical Requirements

Mississippi's payment solution is designed to provide two methods of integration: CommonCheckout (where the user clicks on a "Pay Now" button and is transferred to a set of common checkout pages branded for ms.gov), and DirectConnect (where the application has self-contained checkout pages and will call TPE for verification and capture once all payment information has been entered). In both of these instances, the awarded vendor will utilize standard web services protocols.

The CommonCheckout integration is required by ITS and DFA. Should special circumstances arise where the CommonCheckout is not applicable and/or the DirectConnect option is required, approval from both State agencies is mandatory.

High level descriptions of the integration requirements are included in this section. For detailed documentation please contact Brandon Ward, Mississippi Interative's Director of Technology, at brandon@msegov.com.
CommonCheckout (CCP)

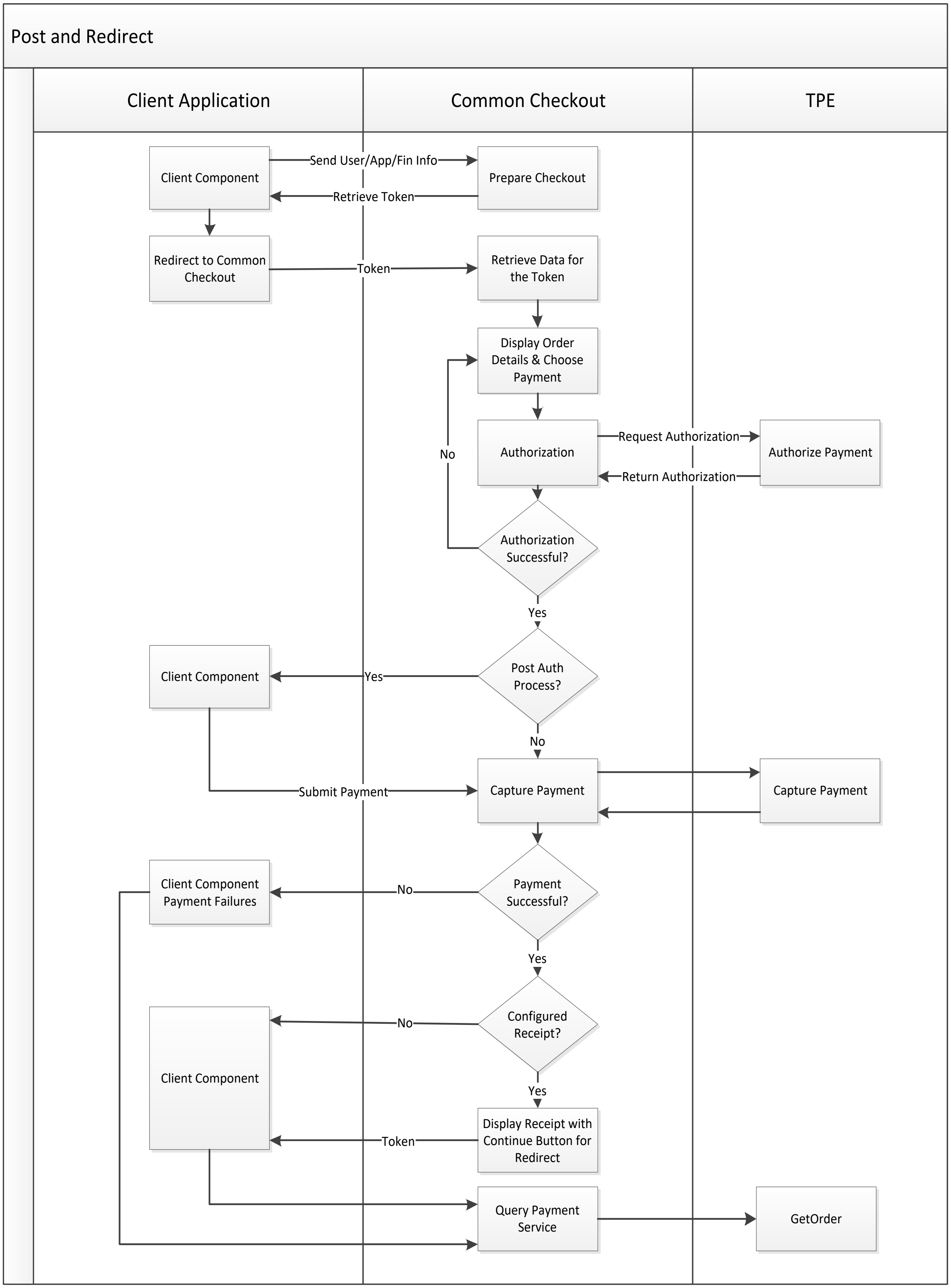
When utilizing CommonCheckout, the calling application is not responsible for collecting the credit card or banking information. Instead, the application sends the transaction data to the CommonCheckout interface which collects and processes all payment information. The CommonCheckout interface will then return to the calling application all transaction status details and information related to the transaction.

CCP Option 1: Server-side Web Service Calls and Browser-side Redirect

The partner application is required to invoke Prepare Checkout Operation on the Common Checkout web service that is passing along the financial/customer/application information.

- The Web Service operation returns a token back in the SOAP response. The token is required as a hidden field on the form post to the Common Checkout web application or a redirect.
- The Prepare Checkout Service returns the token back. This token is required as a hidden field on the form post or query string to the Common Checkout web application.
- When the customer chooses to continue with the payment by clicking a form button on the partner screen, the browser redirects to the Common Checkout web application.
- The Common Checkout web application retrieves the customer/financial/application data associated with the token and displays it on the payment page.
- Upon submission of the payment, Common Checkout redirects to the partner application or displays a receipt page, based on the configuration. In the latter case, the redirect to the partner application happens when a customer clicks a button on the receipt screen.
- The partner application is required to do a call back to the Query payment web service by sending the token. The service will return the transaction information back in the SOAP response. This ensures authenticity of the payment.

The following figure outlines a typical process flow for a CommonCheckout transaction.


Post and Redirect
Client Application
Common Checkout
TPE
Client Component
Send User/App/Fin Info
Prepare Checkout
Retrieve Token
Redirect to Common Checkout
Token
Retrieve Data for the Token
Display Order Details & Choose Payment
Authorization
Request Authorization
Authorize Payment
Return Authorization
No
Authorization Successful?
Yes
Client Component
Yes
Post Auth Process?
No
Submit Payment
Capture Payment
Capture Payment
Client Component Payment Failures
No
Payment Successful?
Yes
Client Component
No
Configured Receipt?
Yes
Display Receipt with Continue Button for Redirect
Token
Query Payment Service
GetOrder

CCP Option 2: Server-side Name-Value-Pair HTTPS Posts and Browser-side Redirect

The partner application is required to send the financial/customer/application information as multiple name/value pairs using HTTPS POST to the Prepare Checkout Post URL.

- The Prepare Checkout Service returns a token-based transaction identifier, which is required as a hidden field on the form post or query string to the Common Checkout web application.
- When the customer chooses to continue with the payment by clicking a form button on the partner screen, the browser is redirected to Common Checkout web application.
- The Common Checkout web application retrieves the customer/financial/application data for the transaction identified by the associated token and displays it on the payment page.
- Upon submission of the payment, Common Checkout redirects to the partner application or displays a receipt page, based on the configuration. In the latter case, the redirect to the partner application happens once a customer clicks a button on the receipt screen.
- The partner application requires a call back to the Query payment HTTP service by sending the token. The service returns the payment detail back as name value pairs. This ensures authenticity of the payment.

<u>DirectConnect</u>

The second scenario is to use the Application Programming Interfaces (“API’s”) that are available to developers. In this scenario, agency or third party developers write applications that include the checkout pages. Customers fill out all payment information within the application, and once captured, the application communicates with TPE using a standard API. TPE processes the payment, based on payment type, and returns either a success or failure code back to the calling application. Based on the code, the calling application displays either a receipt back to the customer or the reason for the failure. TPE supports multiple API’s including:

- Java
- .NET
- Perl
- PHP

Note: If the DirectConnect method is approved by ITS and DFA the awarded vendor must provide MSI and the State proof of their software’s (and any applicable hardware) PCI compliance.

DirectConnect Integration Outline

Before a payment can be processed inside of TPE, an *Order* must be established. An Order is the basic transaction container in TPE. It is a detailed request for certain goods or services and represents all the instructions and information needed from the customer for the merchant to collect money. An order contains information about the customer, items purchased, fees and taxes, payment information, billing address, shipping address, and so forth.

TPE uses the term *order*, along with the terms *payment* and *credit* to represent payment data for all electronic payments. An order is created by the client application while the customer is placing an order for goods or services. Transactions flow between the merchant and the financial institution during the life cycle of the order. These transactions can be broken into two broad categories: *payments* (monies transferred to the merchant from the customer) and *credits* (monies returned to the customer, such as when goods or services are returned and payment is refunded). As order processing continues, payments and credits are created and modified.

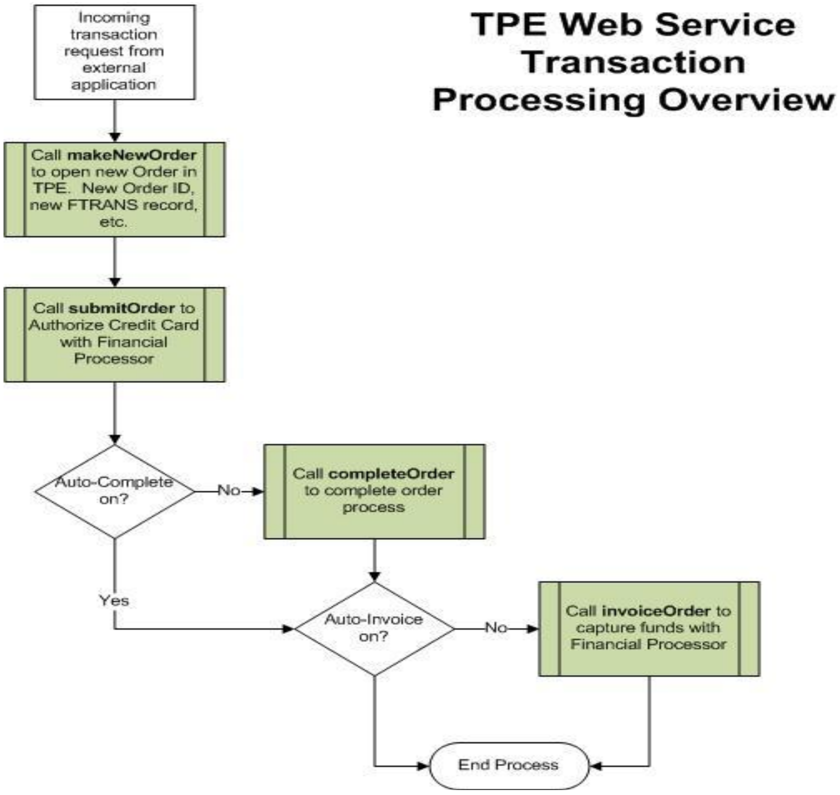
The basic steps for creating an Order and processing a payment are as follows:

1. Submit a new Order Request to TPE. The client application will create a request that includes a Merchant Id, a Merchant Key, and a Service Code. These are pre-defined security parameters

that are configured within TPE. If the request is successful, TPE will return an empty order container to the client application.

2. Inside of this container, the application will set the Payment Implement (Credit Card, ACH, Cash, etc.), customer payment information, billing information, transaction line items and amounts, and any other information necessary for processing the payment.
3. Submit the Order. Once the Order container has been filled by the calling application, it will be submitted for authorization. TPE will do preliminary validations on the Order before submitting it to the Merchant Service Provider for authorization. If there is an error with the Order, TPE will return that information back to client application, or it will return back that the authorization was successful.
4. Complete the Order. This call to TPE informs the system that the order is complete and ready to be invoiced.
5. Invoice the Order. This step is where money transfer (i.e., Capture) is initiated. The invoice takes the information from the Order, and is then submitted to the Merchant Service Provider for Capture/Settlement.

The following figure outlines a typical process flow for a Direct Connect transaction.


TPE Web Service Transaction Processing Overview
Incoming transaction request from external application
Call makeNewOrder to open new Order in TPE. New Order ID, new FTRANS record, etc.
Call submitOrder to Authorize Credit Card with Financial Processor
Auto-Complete on?
No
Call completeOrder to complete order process
Yes
Auto-Invoice on?
No
Call invoiceOrder to capture funds with Financial Processor
End Process

Charges Table Connection

The Mississippi Department of Information Technology Services (ITS) has developed the Mississippi Charges Web Service to supply application programs with data from the charges table. This data is required by the Agency application to build a valid MSI electronic payment request. The item type, item description, and item cost, for each item sold, must be submitted in the transaction request for payment authorization.

Service Use

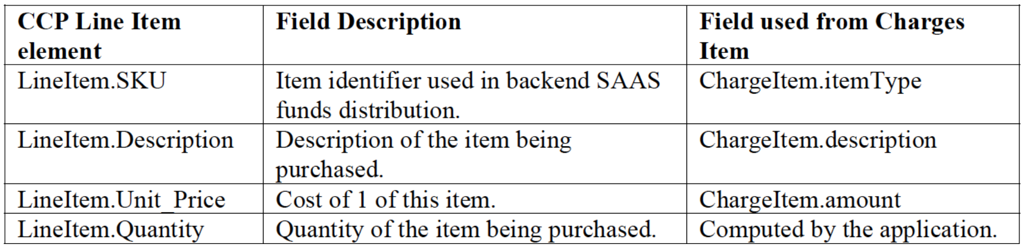
The primary purpose of the web service is to provide the charges data for a requested application. The method that performs this function is getCurrentCharges and requires a chargesInput object as the input parameter. A getCurrentChargesResponse object is returned.

- getCurrentCharges(chargesInput)

DFA updates the charges table each night just before midnight. The agency application is responsible for obtaining and using the current charges information. Good practice is to obtain the charges data at least daily.

Charges Use in MSI Common Checkout

The ChargeItem data will become the basis for a line item that is sent to the CCP in the Prepare Checkout call. The table below maps the line item fields referenced in the CCP interface to their related ChargeItem value. In the CCP Prepare Checkout service call, line items are sent in as an array of lineItems.



CCP Line Item element	Field Description	Field used from Charges Item
LineItem.SKU	Item identifier used in backend SAAS funds distribution.	ChargeItem.itemType
LineItem.Description	Description of the item being purchased.	ChargeItem.description
LineItem.Unit_Price	Cost of 1 of this item.	ChargeItem.amount
LineItem.Quantity	Quantity of the item being purchased.	Computed by the application.

ATTACHMENT I

FINAL RULE
MISSISSIPPI DEPARTMENT OF FINANCE AND ADMINISTRATION
ADMINISTRATIVE RULE
PAYMENTS BY CREDIT CARD, CHARGE CARD, DEBIT CARDS OR OTHER FORMS OF ELECTRONIC PAYMENT OF AMOUNTS OWED TO STATE AGENCIES

The Department of Finance and Administration (DFA) has established the following Administrative rule to be followed when agencies, in accordance with §27-104-33, Mississippi Code of 1972, Annotated, elect to accept payments by credit cards, charge cards, debit cards, electronic check and other forms of electronic payment for various services and fees collectible for agency purposes.

I. Definitions

A. Electronic payments: Consumer and business initiated payments, whether made through the Internet or in person, for various services and fees using any of the following payment instruments: credit cards, bank cards, charge cards, debit cards, electronic checks, or direct debits via electronic funds transfer.

B. ACH: Automated Clearing House. Affiliated with the U. S. Treasury and the Federal Reserve System and used as the conduit for electronic payments and collections. The ACH is the settlement vehicle for electronic payments. The ACH is also used to transport direct debit and credit transactions to consumer bank accounts.

C. Application Service Provider (ASP): An application service provider (ASP) provides computer-based services to customers over a network. The most limited definition is that of providing access to a particular application program (such as license renewals, registrations, etc.) using a standard protocol such as HTTP. ASP applications for purposes of this rule are those which accept electronic payments either through a browser-based application, or other revenue input sources.

D. DFA: Mississippi Department of Finance and Administration.

E. EOC FEE: Electronic Government Oversight Committee (EOC) Fee. This fee is used to offset the costs associated with providing electronic services and operating the electronic portal (www.mississippi.gov) at ITS. §25-53-151 (2) of the Mississippi Code defines the EOC. All transactions must include an EOC fee unless ITS has granted express written exemption of this fee for a specific Agency application or has granted approval for the Agency to absorb and directly remit the EOC fees associated with transactions for a specific application to DFA payable to State Treasury Fund 3126.

F. Consumer: Consumer, for purposes of these rules, may be any individual person or business representative who initiates a transaction involving electronic payment.

G. Convenience Fee: Convenience fee is the payment-processing fee as calculated and approved by the Department of Finance and Administration (DFA). No other fees, including the EOC fee, will be defined as convenience fees. All transactions must include a convenience fee unless DFA has granted express written approval for the

Agency to absorb the payment processing costs associated with the transactions for a specific transaction and for the agency to remit those fees to DFA payable to State Treasury Fund 3126.

H. ITS: Mississippi Department of Information Technology Services.

I. Point of Sale: Point of Sale (POS). Payments made "over the counter" for fees for services. For the purposes of electronic payments in Mississippi, agencies desiring to accept "over the counter" electronic payments must have a POS application. POS applications may be: A web-based system where all payment information is keyed into the application by the client or a "card swipe" application similar to those found in commercial enterprises. POS applications must be certified to meet PCI Compliance Standards.

J. SAAS: Statewide Automated Accounting System.

K. SPI: SAAS Payment Interface. The SPI defines the accounting entries used to record all electronic payment transactions.

L. Record Keeping: An agency must establish and maintain financial records and keep them available for the purposes of audit. The record keeping procedures must include the capture of the details of the electronic payments, associated fees, and supporting reconciliation documentation.

M. Payment Card Industry – Data Security Standards: PCI-DSS is the result of collaboration between the major credit card brands to develop a single approach to safeguarding sensitive data. PCI-DSS defines a series of requirements for handling, transmitting, and storing sensitive data. The PCI-DSS standards can be found at https://www.**pci**securitystandards.org.

N. Self-Assessment Questionnaire (SAQ): The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

O. Payment Application Approved Scanning Vendor (PA-ASV): Organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers.

P. Payment Application Qualified Security Assessor (PA-QSA): Companies or employees that have been certified by the Payment Card Industry Security Standards Council to validate an entity's adherence to the PCI PA-DSS.

Q. Cardholder Data: Data that includes cardholder full name, full account number, expiration date, service code, full magnetic stripe, PIN/PIM Block or Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card). Card Validation Code is also known as the CVV2 or CVC2 code.

R. Sensitive Cardholder Data: Data includes Card Validation Code (e.g., three-digit or four digit value printed on the front or back of the payment card (e.g., CVV2 and CVC2 data)).

S. Payment Application Data Security Standards (PA-DSS): A program managed by the Payment Card Industry Security Standards Council (PCI SSC). PA DSS is a set of standards designed to assist software vendors in developing secure payment applications that comply with PCI-DSS requirements.

The PA-DSS standards can be found at https://www.**pci**securitystandards.org/.

T. Revenue Input Source: Electronic transactions from Web-based, Point of Sale (POS), Interactive Voice Response (IVR), Over the Counter Sales, etc.

U. §27-104-33. Payment by credit card, charge card, debit card, or other form of electronic payment amounts owed to state agencies.

The State Department of Finance and Administration shall establish policies that allow the payment of various fees and other accounts receivable to state agencies by credit cards, charge cards, debit cards and other forms of electronic payment in the discretion of the department. Any fees or charges associated with the use of such electronic payments shall be assessed to the user of the electronic payment as an additional charge for processing the electronic payment.

Agencies with the approval of the Department of Finance and Administration may bear the full cost of processing such electronic payment if the agency can demonstrate to the department's satisfaction that they are able to assume these costs and provide the related service for the same or lesser cost.

II. Approvals for Internet-based Applications and Services for State Agencies

A. E-government applications and services require additional review and approval by ITS and by DFA (in contrast to traditional software applications.) Because of the multiple costing models used by vendors for e-government applications, as well as the necessity for ensuring appropriate security for all public-facing applications, the normal ITS procurement delegations to agencies do not apply for these types of acquisitions. In addition, DFA must approve and schedule any implementations that involve payments. See 001-025 Approvals for Internet-based Applications and Services in the ITS Procurement Handbook. http://dsitspe01.its.ms.gov/its/procman.nsf/TOC4?OpenView

III. Payment Applications - Fees Paid By Consumer

A. Agency applications accepting payments shall use the third party electronic payment processor designated by DFA to accept electronic payments for various services and fees collectible for agency purposes unless express written approval is given by DFA for the use of an alternate payment processor.

1. Designated payment processor is to be used regardless of where the application is hosted (agency, ITS, third-party).

2. Rules for obtaining approval of an alternate payment processor are found in Section V.

B. The services provided by the processor and the fees for such services shall be set forth in the contract approved by the State. All such agreements are considered e-government agreements and are under the purview of ITS (see 001-020 Acquisitions within ITS Purview, item 3, in the ITS Procurement Handbook).

C. Funds will be deposited in the account designated by the State Treasurer and transferred to the designated agency funds in SAAS once the bank deposit is balanced.

D. The payment processor will support, as a separate line item on the transaction payment summary presented to the customer, the convenience fee for the service and fee payment due the agency.

E. DFA will provide the software components to be used by agency applications in calculation of the convenience fee associated with a particular fee or services payment.

   1. The standard calculation used by the software ensures the total cost to process the electronic payment is passed to the consumer.

   2. The software components are collectively known as the “charges client”.

F. The application must inform the consumer of the total amount of the convenience fee that will be added to the fee or service billing before such charges are assessed. The consumer must be able to cancel the transaction at this point without any fee being assessed.

G. The convenience fee and EOC fee shall be plainly included and identified on the electronic receipt provided to the consumer.

H. The convenience fee charged to the consumer and noted in the financial records for verification purposes:

   1. Will be recorded in SAAS as a revenue receipt in DFA fund 3126 (known as the Mississippi.Gov Portal fees Fund).

   2. Will not flow through agency accounting journals.

I. The portion of the convenience fee owed the electronic payment processor shall be directly withheld by the processor, then aggregated with other fees for that application and recorded appropriately as an expenditure transaction against the Mississippi.Gov Portal Fees Fund.

J. Any rejected items returned to DFA by the designated third party processor will be forwarded to the appropriate agency for handling after being netted out of the settlement for the day.

K. Revenues for all fees and services shall be recorded at gross in SAAS as revenue, as specified by the agency on the SAAS electronic payment distribution tables.

L. Actual processing costs to include fees for authorization, settlement, and Electronic Government Oversight fees, will be recorded as expenditures as specified by the Agency on the SAAS electronic payment distribution tables.

IV. Payment Applications - Fees Paid By Agency

A. Agencies desiring to pay all fees associated with electronic processing of payments must demonstrate to DFA their ability to do so and receive express written approval from DFA. Requirements for requesting approval are outlined in section VI of these rules.

B. Agency applications accepting payments shall use the third party electronic payment processor designated by DFA to accept electronic payments for various services and fees collectible for agency purposes unless express written approval is given by DFA for the use of an alternate payment processor.

1. Designated payment processor is to be used regardless of whether the particular application is a POS application, an application hosted through the Mississippi.gov infrastructure, or an application hosted through other ASPs.

2. Rules for obtaining approval of an alternate payment processor are found in section V.

C. The services provided by the processor and the fees for such services shall be set forth in the contract approved by the State. All such agreements are considered e-government agreements and are under the purview of ITS (see 001-020 Acquisitions within ITS Purview, item 3, in the ITS Procurement Handbook).

http://dsitspe01.its.ms.gov/its/procman.nsf/TOC4?OpenView

D. Funds will be deposited in the account designated by the State Treasurer and transferred to the designated agency funds in SAAS once the bank deposit is balanced.

E. Revenues for all fees and services shall be recorded at gross in SAAS as revenue as specified by the agency on the SAAS electronic payment distribution tables.

F. Actual processing fees to include fees for authorization, settlement, and Electronic Government Oversight fees, will be recorded as expenditures as specified by the agency on the SPI distribution tables. These fees will be applied against the day's settlement for the agency.

G. Any rejected items returned by the designated third party credit card/or other electronic processor to DFA will be forwarded to the appropriate agency for handling after being netted out of the settlement for the day.

V. Approval of an Alternate Payment Processor

A. An agency wishing to use an alternate payment processor must submit a written request to the Department of Finance and Administration, Office of Fiscal Management, Attn: Portal Transactions, 501 North West Street, Suite 701 B, Jackson, MS 39201.

B. The written request must state:

   1. The reason(s) the State-approved payment processor is not suitable for the agency application.

   2. The impact if the request is not granted.

C. The application must be approved by DFA prior to entering into the procurement process for the alternate payment processing services.

D. The agency must state what payment processors are available that meet their needs.

E. The agency must describe the agency application including:

   1. The agency program supported.

   2. The items (services and fees) offered for sale.

   3. The individual item costs.

   4. The estimated usage of the processor (i.e., the number of transactions that will occur per fiscal year).

   5. An estimate of the processing costs "per transaction" for the items to be sold.

   6. The costs associated with the use of an alternate payment processor including, but not limited to, purchased and leased equipment, training, and contractual services.

F. The agency must acknowledge that if DFA approves the agency's request to pursue alternate payment processing services:

   1. Funds will be deposited in the account designated by the State Treasurer and transferred to the designated agency funds in SAAS once the bank deposit is reconciled and balanced by the agency. DFA will not perform this reconciliation and will not approve the transfer of funds to SAAS until proof of reconciliation is provided.

   2. Any request for an exception to the above reconciliation requirement must be clearly documented in the request for the alternate payment processor.

G. The service must be legally procured following the rules for technology procurement. All such services are considered e-government services, and are within the purview of ITS even if those services are offered at no cost to the agency. (See 001-020 Acquisitions within ITS Purview, item 3, in the ITS Procurement Handbook):

   http://dsitspe01.its.ms.gov/its/procman.nsf/TOC4?OpenView

1. DFA will be an active participant in the procurement, implementation, and acceptance of the alternate payment processor before the application supported is certified for production operations.

2. DFA, at its discretion, may require that DFA be a party to the contract.

H. The alternate payment processor and/or 3rd party vendor must work with DFA to interface daily settled transactions and any associated fees into SAAS via the Cash Receipts (CR) interface or the SPI.

I. Agencies are required to collect any State required fees, such as EOC fees.

J. Approval under this section shall not relieve an agency of its responsibility concerning other sections of this rule.

VI. Approval for All Fees to Be Paid By Agency

A. An agency wishing to obtain approval to bear the full cost of processing electronic payments should address the written request to the Department of Finance and Administration, Office of Fiscal Management, Attn: Portal Transactions, 501 North West Street, Suite 701 – B, Jackson, MS 39201.

B. The request must state whether the application is web-based or of another type (example: submission of a file of EFT debits for mortgage payments).

C. The agency must describe the agency application including:

1. The agency program supported.

2. The items (services) offered for sale or collections.

3. The individual item costs.

4. An estimate of the processing cost “per transaction” for the items (services) to be sold.

D. The agency must state whether the agency or the consumer will pay the EOC fee.

E. The agency request must clearly:

1. Document whether the request is for an application where the consumer can purchase only a single item or service at a time (example: drivers’ license renewals) or a shopping cart model where multiple items may be purchased (example: hunting and fishing licenses).

2. Demonstrate a dollar neutral cost or cost saving to the agency when absorbing the processing fees rather than having the consumer pay the fees projected over a fiscal year. All assumptions must be documented.

3. Demonstrate that the funds to defray the total cost of electronic processing will be available projected over a fiscal year. All assumptions must be documented.

F. The agency must acknowledge that it will be required to set aside cash/authority at a specified minimum limit in a specified fund to cover expenses (debits) associated with the agency's transactions for the following:

1. Authorization and settlements fees
2. Refunds
3. Chargebacks
4. Voids
5. Returned items charges

G. Approval under this section implies that the agency accepts and understands that the application will not be certified for production until such time as complete end-to-end testing is approved by DFA.

1. Testing will include financial settlement testing of all payment types.
2. Testing will include refunds and chargebacks.
3. Testing will include full reconciliation using the procedures developed by the Agency for that purpose.

VII. Waiver of the EOC Fee

A. All requests to waive EOC fees must be addressed to Department of Information Technology Services, Attention: E-government Oversight Committee, 301 North Lamar Street, Suite 508, Jackson, MS 39202.

VIII. Third Party Processing and Fulfillment Costs

A. §7-7-9, Mississippi Code (Laws of 1972) states the following:

"*The Mississippi General Accounting Office shall maintain a complete system of general accounting to comprehend the financial transactions of every state department, division, officer, board, commission, institution or other agency owned or controlled by the state, except those agencies specifically exempted in Section 7-7-1, whether at the seat of government or not and whether the funds upon which they operate are channeled through the State Treasury or not, either through regular procedures having to do with the issuance of the State Fiscal Officer receipt warrants and disbursement warrants or through controls maintained through reports filed periodically as required by the State Fiscal Officer in accordance with the reporting provisions contained in said Section 7-7-1.*

All Transactions in public funds, as defined in Section 7-7-1, shall either be handled *directly through the State Fiscal Officer and the State Treasury, or shall be reported to the State Fiscal Officer at the times and in the form prescribed by the State Fiscal Officer and the Legislative Budget Office, so that a complete and comprehensive system of accounts of the fiscal activities of all state governmental agencies shall be made available at all times in the General Accounting office.*

B. This policy is established by the Department of Finance and Administration, Office of fiscal Management (OFM) for direct or indirect payment to vendors to support internal business functions in the fulfillment of orders and completion of transactions initiated in person or through the Internet. These transactions may include, but are not limited to, the collection of taxes, issuance of licenses, production of reports, and other collections or payments for services that are conducted by agencies in their normal course of business.

C. Any cost incurred directly (by an agency) or indirectly (passed directly to the consumer) for a party to complete agency business transactions must be reflected as a cost of doing business for this agency. To do otherwise would not fully disclose costs of the State to conduct business or reflect revenue generated by a vendor who is providing services under contract for the State of Mississippi. Likewise, any charge to the consumer for processing these transactions should be recognized by the agency as revenue.

D. Agencies will report revenues and expenses on a Journal Voucher (JV) according to the Mississippi Agency Accounting Policy and Procedure (MAAPP) Manual, Section 16. The JV will be created within 5 workdays of the end of the fiscal quarter.

IX. Payment Card Industry – Data Security Standards (PCI-DSS)

A. State agencies accepting credit and/or debit cards will comply with Payment Card Industry – Data Security Standards (PCI- DSS) to safeguard cardholder and sensitive cardholder data, regardless of revenue input source.

B. To assist agencies in complying with PCI–DSS mandates, state agencies will use Project Number 37081, a Professional Services Agreement Between Coalfire Systems, Inc. and the Mississippi Department of Information Technology Services on Behalf of the Agencies and Institutions of the State of Mississippi. To request services under this agreement see http://www.its.ms.gov/PCI.shtml.

1. Agencies will attend a Self-Assessment Workshop when scheduled by DFA and ITS.

2. Agencies will complete a Self-Assessment Questionnaire (SAQ) and participate in interviews to evaluate their current operations and network. If an agency accepts credit cards via mail, manually or other non-Internet means, the Self-Assessment Questionnaire is still required. Additionally, there may be other operational security issues the agency will need to address.

3. All agencies will have quarterly scans on all Internet-facing Internet Protocol (IP) addresses used in the processing and storing of credit card data under the Professional Services Agreement between Coalfire Systems, Inc. and ITS.

4. Agencies will make a good faith effort to correct deficiencies identified in the remediation plan and provide status or remediation tasks as requested by DFA and ITS.

H. Agencies that do not participate in PCI-DSS cannot accept credit cards/debit cards as a form of payment. If an agency is found accepting credit/debit cards as payment and has not completed the steps for PCI compliance, DFA under the authority of §27-104-33, will issue the agency a cease and desist letter to close the system down. To request an appeal see Section XII.

X. Development/Hosting Options and Ultimate Responsibility for PCI-DSS and Fines and Penalties

A. Agencies are responsible for ensuring their vendors are PCI-DSS compliant. Vendors will use Payment Application Data Security Standards (PA-DSS) to develop applications. The PA-DSS standards can be found at https://www.pcisecuritystandards.org/.

B. Should an agency wish to move the hosting of their applications to Mississippi Department of Information Technology Services (ITS), the agency will bear the responsibility and cost to bring the application into PCI compliance before it is transferred to ITS. The agency will ensure the transfer takes place no later than 90 days after the last PCI scan. Another scan will occur after the transfer to ITS and the agency will be responsible for all PCI non-compliance items.

C. The following table is a general guideline for PCI-DSS responsibility and liability:

System Type or Web Development/Hosting	**Responsible Entity**
ITS Developed/ITS Hosted	State is responsible for PCI compliance, fines and penalties
Agency Developed/ITS Hosted	State is responsible for PCI compliance, fines and penalties for state network infrastructure. The agency is responsible for PCI compliance, fines and penalties for the agency application and internal agency business practices
Agency Developed/Agency Hosted	The agency is responsible for PCI compliance, and all fines and penalties
3rd Party Vendor Developed/Agency Hosted	The agency is responsible for PCI compliance, and all fines and penalties
3rd Party Vendor Developed/ITS Hosted	State is responsible for PCI compliance, fines and penalties for state network infrastructure. The agency is responsible for PCI compliance, fines and penalties for the agency application
3rd Party Vendor Developed/3rd Party Vendor Hosted	The agency is responsible for PCI compliance and all fines and penalties
Non-Web based systems, Point of Sale (POS), Interactive Voice Response (IVR), Over the Counter Sales, Telephone Sales, Mail in, etc.	The agency is responsible for PCI compliance and all fines and penalties

XI. Security Breaches and Notifications

A. In the event of a security breach, credit card or debit card data could be compromised. Agencies will immediately terminate the application/services to preserve evidence and notify:

1. DFA's Chief Systems Information Officer at 601-359-6570.

2. Mississippi Department of Information Technology Services, Information Security Director at 601-432-8080 and E-Government at (601) 432-8146.

3. Mississippi State Attorney General's Office, Consumer Protection Division at (601) 359-3680 or 1 (800) 281-4418 and the Cyber Crimes Division at (601) 359-3817.

B. The agency shall notify their customers of the breach once law enforcement informs the agency that customer notification will not impede an investigation.

1. Agencies may notify customers using written notices or electronic notices. As a last resort, telephone notices can be given. Documentation that notices were provided, to whom they were provided, and when such notices were provided must be maintained by the Agency.

2. The notice shall be clear and conspicuous and include:

   a. A description of the incident in general terms.

   b. The type of personal information subjected to unauthorized access or acquisition.

   c. The general acts the agency has taken to protect the information from further unauthorized access.

   d. A telephone number that the customer can call for further information.

   e. Advice that directs the customer to remain vigilant by reviewing account statements and monitoring free credit reports or close an account.

XII. Appeal Process

A. An agency wishing to appeal a cease and desist letter must submit a written request to the Department of Finance and Administration, Director, Office of Fiscal Management, 501 North West Street, Suite 701 -B, Jackson, MS 39201.

B. The agency must provide the following information in the written request:

1. The agency program supported.

2. The items (services) offered for sale or collections.

3. The individual item costs.

4. An estimate of the processing cost “per transaction” for the items (services) to be sold.

5. The number of items sold per year and the total cost of those items.

6. A detailed description of how the system works.

7. A detailed list of software operating on the system.

8. A detailed list of equipment, including the name, model number, and purposed of the equipment.

9. A detailed description of accounting entries made to account for revenue and processing and other fees.

C. The agency must state whether the agency or the consumer pays the EOC fee. The agency request must clearly:

1. Document whether the consumer can purchase only a single item or service at a time (example: drivers' license renewals) or a shopping cart model where multiple items may be purchased (example: hunting and fishing licenses).

2. Demonstrate a dollar neutral cost or cost saving to the agency when absorbing the processing fees rather than having the consumer pay the fees projected over a fiscal year if the agency is to pay the processing fees. All assumptions must be documented.

3. Demonstrate that the funds to defray the total cost of electronic processing will be available projected over a fiscal year if the agency is to pay the processing fees. All assumptions must be documented.

D. If the agency is paying processing fees, the agency must acknowledge that they will be required to set aside cash/authority at a specified minimum limit in a specified fund to cover expenses (debits) associated with the agency's transactions for the following:

3. Authorization and settlements fees

4. Refunds

5. Chargebacks

6. Voids

7. Returned items charges

E. The agency will also submit their PCI Self-Assessment Questionnaire, Remediation Plan, and cost estimates to correct deficiencies identified in the Remediation Plan. Once the agency information is reviewed, the agency will be given a written response to the appeal request.