WEST VIRGINIA STATE TREASURER'S OFFICE
JOHN D. PERDUE, STATE TREASURER

CREDIT CARD HANDLING HANDBOOK
FOR
WEST VIRGINIA SPENDING UNITS

Effective Date: April 11, 2018

TABLE OF CONTENTS

Section	Page
General	3
Definitions	5
Credit Card Processing Set Up	13
Transaction Processing	14
Card Present Best Practices	18
Card Not Present Best Practices	20
Refunds, Voids and Exchanges	23
Credit Card Disputes	24

Section	Page
Chargebacks	26
Fraud	29
Payment Card Industry Data Security Standards (PCI-DSS)	31
Personal Identifiable Information (PII)	35
Encryption and Tokenization	36
Merchant (Spending Unit) Responsibilities	37
State Treasurer's Office (STO) Contacts	40

GENERAL

- **Authority:** The State Treasurer's Office (STO) is statutorily and constitutionally charged with the responsibility to provide professional financial management for the collection, disbursement, management, and investment of public funds. The STO E-Government Program provides an electronic payment system for goods and services offered by a variety of state agencies and local governments. Payments are remitted with the use of credit cards or electronic fund transfers (EFTs). Additionally, the STO allows for credit card payments through Point of Sale (POS) transactions located at individual spending units.
- **Purpose:** This handbook has been prepared by the STO to provide guidance regarding the receiving, handling and acceptance of electronic payments by spending units and their employees. Strong internal controls for electronic payments are designed to safeguard and protect consumer information as well as to protect employees from inappropriate charges of mishandling transactions. The STO's goal is to guide the process for accurate and secure receiving and processing of electronic payments received at various locations throughout the State.

GENERAL

- **Overview:** Credit card transactions should be handled with the highest security. Spending units must ensure that they have the W.Va. Code authority to collect revenues. Each spending unit that has the authority to collect revenues must have policies and procedures detailing all required steps at each interval of the deposit transaction process. The procedures should give each employee a clear understanding of what is expected, what behavior is and is not acceptable and how to accurately accept, handle and safeguard credit card information. The procedures should also be clear as to which employees have access and the ability to perform each task required in the entire process. Employees should understand their accountability for all credit card transactions due the State of West Virginia. This Handbook establishes the minimum policies and procedures that are to be used, as well as best practice guidelines. Spending units may require stricter provisions than those specified in this Handbook. All spending units must follow their required procedures for credit card receipts, which procedures must meet the minimum standards in this Handbook.

DEFINITIONS

The following terms are defined for purposes of this handbook, unless a different meaning is clearly required by the context:

- **“Acquiring bank” (acquirer)** means the financial institution that administers payment processing services.
- **“Authorization”** means the process by which a transaction is approved or declined by the card issuer. An authorization indicates that sufficient funds are available on the cardholder's credit limit or account balance at the time the authorization request is made.
- **“Batch”** means a collection of credit card transactions that are saved for submitting at the end of the business day.
- **“Batch Close”** means the process of sending a batch to the financial institution for settlement.
- **“BB&T”** means the bank currently serving as the merchant services provider and contracts with the processor, gateways, and other payment service providers to deliver the payment services required by the STO and spending units.

DEFINITIONS

- **“Card present transaction”** means transactions that occur with the cardholder present. These transactions may require a clerk to swipe the mag stripe on the card through a POS terminal or the cardholder swipe or insert the card through the POS terminal.
- **“Card not present transaction”** means transactions that are generated without the card in view. They may be internet transactions or situations where clerks enter numbers that they receive by phone or mail.
- **“Cardholder”** means consumer to whom a payment card is issued to or any individual authorized to use the payment card.
- **“Clearing”** means the process of reconciling purchases and completing the movement of money between accounts.
- **“Credit card”** means a card issued by a financial institution giving the card holder the ability to borrow pre-approved funds.
- **“Debit card”** means a card used to purchase goods and services and to obtain cash, which debits the cardholder's personal checking account. During debit transactions, the cardholder must enter a PIN. Also known as PIN Debit.

DEFINITIONS

- **“End of day” (EOD)** means the time that indicates the end of a business day for a spending unit.
- **“EMV”** means the international industry standards that define the rules for processing chip cards, and originally named after the 3 organizations (Europay, MasterCard and Visa) that produced the specifications. The EMV standards and associated compliance processes are now managed by EMVCo.
- **“EMVCo”** means the company that owns and manages the EMV standards and which is jointly owned by Visa, MasterCard, JCB, UnionPay, Discover and American Express (www.emvco.com).
- **“E-Gov”** means the system developed by the STO to process eCommerce transactions for the STO and its spending units.
- **“ePay”** means the customer-facing payments page developed by the STO designed to accept payment information from any web service, whether developed by the STO, WV Interactive or on their own.
- **“Encryption”** means a method of utilizing cryptographic keys to encipher data to protect a cardholder's personal information.

DEFINITIONS

- **“Expiration Date”** means the date a credit, debit or pre-paid card expires.
- **“Issuer”** means an entity that issues payment cards or performs, facilitates or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as “issuing bank” or “issuing financial institution.”
- **“L-Gov”** means a system developed by the STO for use by local governments to accept payments.
- **“Merchant”** means a seller of a good or service. For the purpose of this handbook, a merchant refers to a State of West Virginia spending unit.
- **“Merchant Account”** means a bank account that allows a merchant to accept payments.
- **“Merchant Identification Number” (MID)** means an identification number that uniquely identifies a merchant to a bank, used for processing credit card payments.
- **“Method Of Payment” (MOP)** means the way a merchant (spending unit) chooses to accept payment for products or services. Examples include: MasterCard, Visa, American Express, Discover, Diners Club, JCB, and Electronic Check.

DEFINITIONS

- **“Payment Gateway”** means a service provider that facilitates payment transactions between a merchant (spending unit) and the payment processor for online payments.
- **“Payment Processor”** means a company responsible for processing payment transactions to the payment card brands. TSYS is the payment processor contracted by BB&T on behalf of the STO.
- **“PCI”** means Payment Card Industry.
- **“PCI DSS”** means Payment Card Industry Data Security Standard.
- **“Primary Account Number” (PAN)** means a 14 – 19 digit number that identifies a credit card account holder’s account.
- **“Personal Identification Number” (PIN)** means a numeric code (typically a four digit code) used as verification of the cardholder to complete a transaction via a payment card. The number is entered into a keypad and is encrypted and transmitted with the authorization.
- **“Point-of-Sale” (POS)** means the location at which a payment card transaction occurs, usually by way of a device such as a cash register as well as a debit/credit card reader.

DEFINITIONS

- **“Prepaid card”** means a card issued by a financial institution that is pre-loaded with funds and used by a card holder.
- **“Processing Fees”** means the fees associated with the processing of credit/debit card transactions.
- **“Reconciliation”** means the process used to compare two or more records to ensure the figures are in agreement and are accurate at a particular point in time. The merchant (spending unit) reconciles payment transactions and what is successfully settled by the acquirer. Merchants (spending units) reconcile data based on business need (frequency, level of detail, etc.).
- **“Refund”** means a transaction when the merchant (spending unit) rebates all, or a portion, of an original transaction amount to the cardholder. Refunds should be made to the same card that was used for the original transaction. May also be referred to as a credit.
- **“SAQ”** means acroynym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.
- **“Settlement”** means the process of finalizing a payment transaction so it can be cleared and the appropriate parties can be funded.

DEFINITIONS

- **“Spending Unit”** means any entity of the West Virginia state government for which an appropriation is requested or to which an appropriation is made by the Legislature.
- **“State Treasurer’s Office” (STO)** means the State entity that manages acceptance and transference of moneys for agencies involved in processing payments for state services provided online and at over 400 physical merchant (spending unit) locations.
- **“TID” (Terminal ID)** means a unique identification number assigned to a specific point of sale (POS) device by the Acquirer or E-Gov account by the STO.
- **“Tokenization”** means the replacement of sensitive data with a non-correlating unique identifier that cannot be derived or otherwise reengineered.
- **“Transaction”** means any action between a cardholder and a merchant (spending unit) or member that results in activity on the account, such as a purchase, cash advance or credit.
- **“Transaction Date”** means the actual date on which a transaction occurs.
- **“Trust Commerce”** means the eCommerce gateway contracted by BB&T on behalf of the STO.

DEFINITIONS

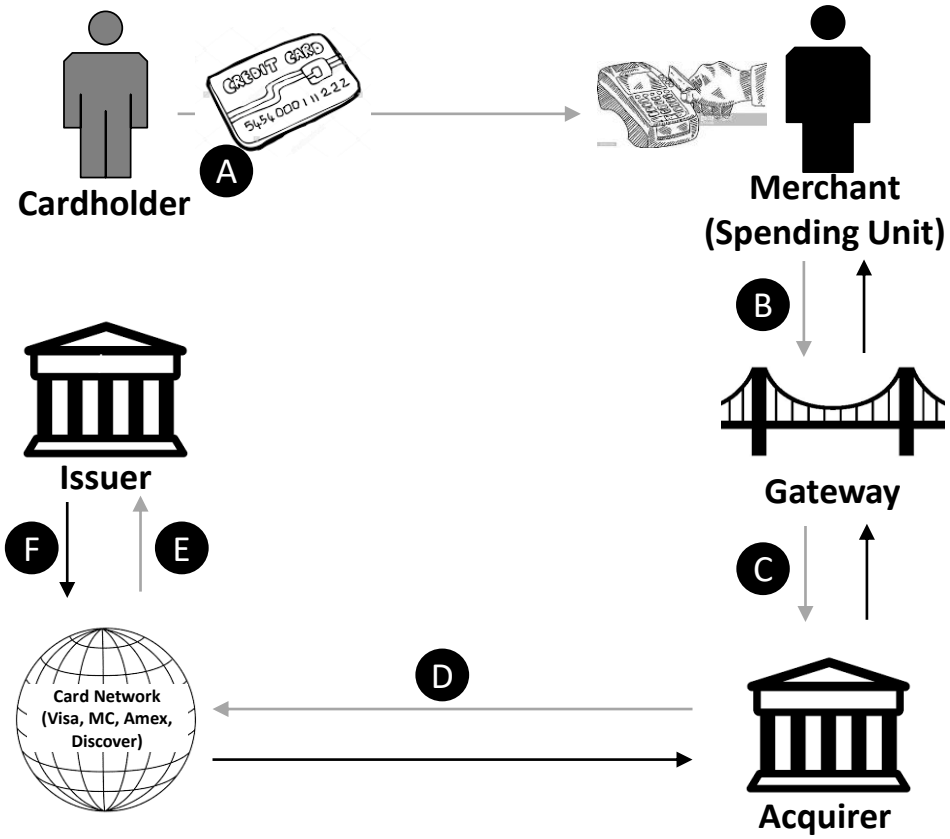
- **“TSYS”** means the payment processor contracted by BB&T.
- **“WV Interactive”** means the current statewide contract holder for web based portal management.
- ***“wv*OASIS”** means the State Enterprise Resource Planning (ERP) system with a comprehensive suite of integrated modules that provide end-to-end support for statewide administrative functions such as Financial Management, Procurement, Asset Management, Payroll, etc.

CREDIT CARD PROCESSING SET UP

- **E-Gov Set Up**
  - For assistance setting your spending unit up to accept online payments through the STO's E-Gov system, please contact the E-Government group by calling the STO Check Hotline at 304-558-3599 or submitting an email to egovernmentCM@wvsto.com.
- **Point of Sale Set Up**
  - For assistance setting your spending unit up to accept in-person credit card payments or adding additional locations to accept in-person credit card payments, please contact the Cash Accounting Department by calling the STO Check Hotline at 304-558-3599 or emailing the ReconGroup@wvsto.com.

TRANSACTION PROCESSING

Credit card authorization process



Authorization Process

A. Customer provides their card information either in person (card present) or online or over the phone (card not present).

B. Merchant (spending unit) submits the transaction and credit card details provided for authorization to the gateway*.

C. If used, the gateway routes the transaction to the acquirer.

D. Acquirer forwards the transaction to the credit card network.

E. Credit card network requests payment authorization from the customer's issuing bank.

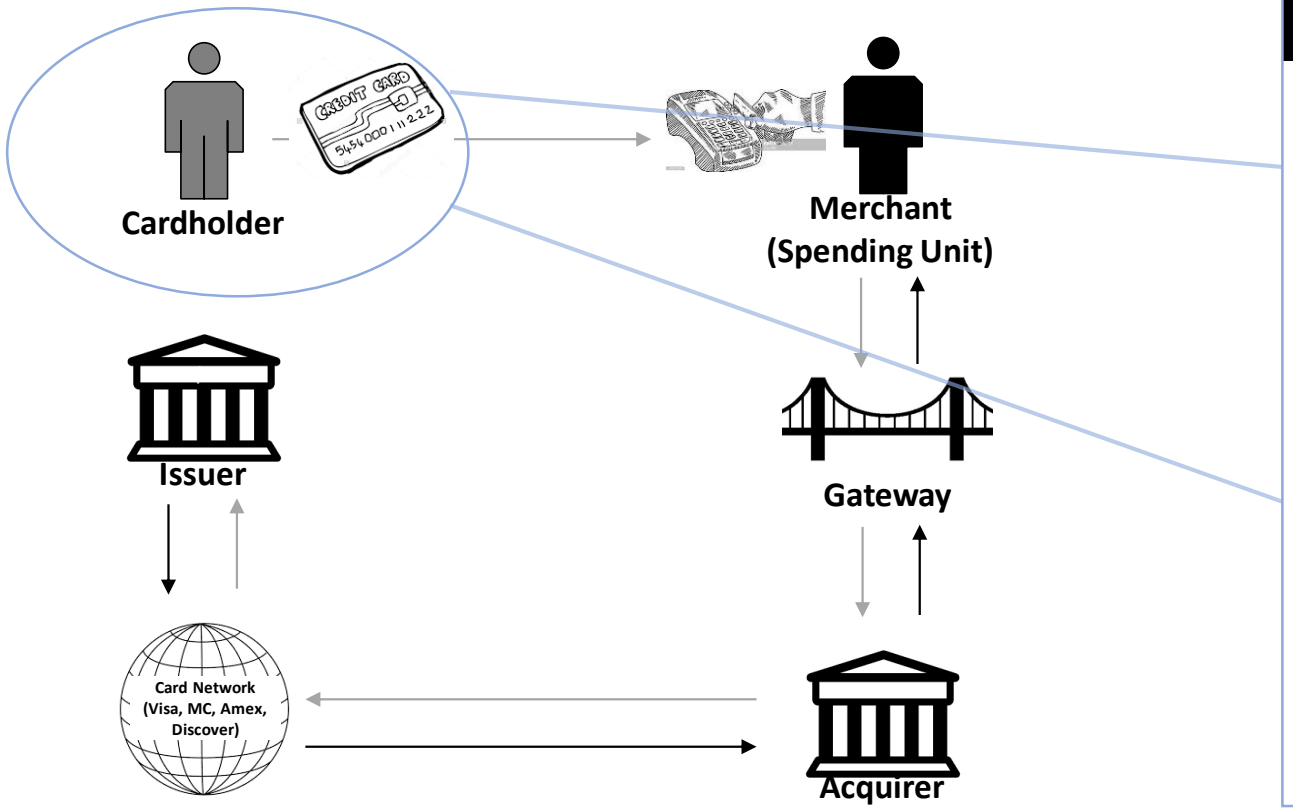
F. The issuing bank:
   A. Authenticates the card by checking information such as the Address Verification Service (AVS) and the card security codes (such as CVV, CVV2, CVC2 and CID).
   B. Confirms available funds in the account.

If all data is confirmed, the issuing bank sends an approval code to the merchant (spending unit) via the same channels.

** The gateway typically applies to card not present transactions (i.e. E-Gov transactions), however could apply to card present transactions depending on the spending unit's point of sale system.*

TRANSACTION PROCESSING

Payment Acceptance



** Spending unit dependent*
*** Not all spending units accept PIN Debit*

Current Payment Types Accepted

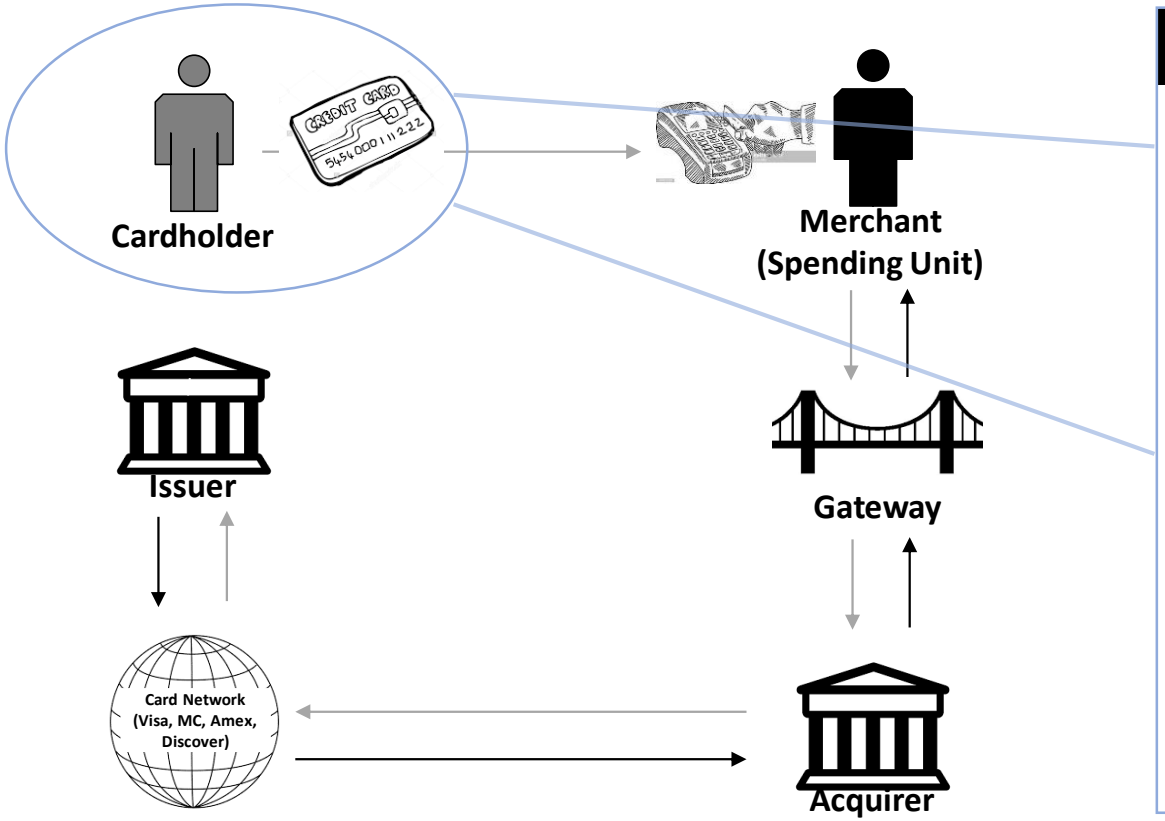
- Payment types currently accepted within West Virginia State spending units:

Payment Type	Card Present	Card Not Present
US Credit Visa MasterCard American Express* Discover	Yes	Yes
PIN Debit	Yes**	No

- Other payment types accepted include ACH, check and cash.

TRANSACTION PROCESSING

Differentiation between Magnetic Stripe and EMV Card Entry



Magnetic (Mag) Stripe vs EMV

- Terminals may accept cards using a magnetic swipe and/or EMV if enabled for chip acceptance (see the approved list of terminals published by the acquiring bank for more details). Key differentiators between these two entry methods include:

EMV:

- Account information stored on embedded microchips as well as on the mag stripe
- Chips have dynamic authentication capabilities and EMV-enabled terminals communicate with the chip and transmit data that is unique to each transaction
- The card may be inserted into the terminal (contact EMV) or the card/mobile device is tapped against terminal (contactless EMV)

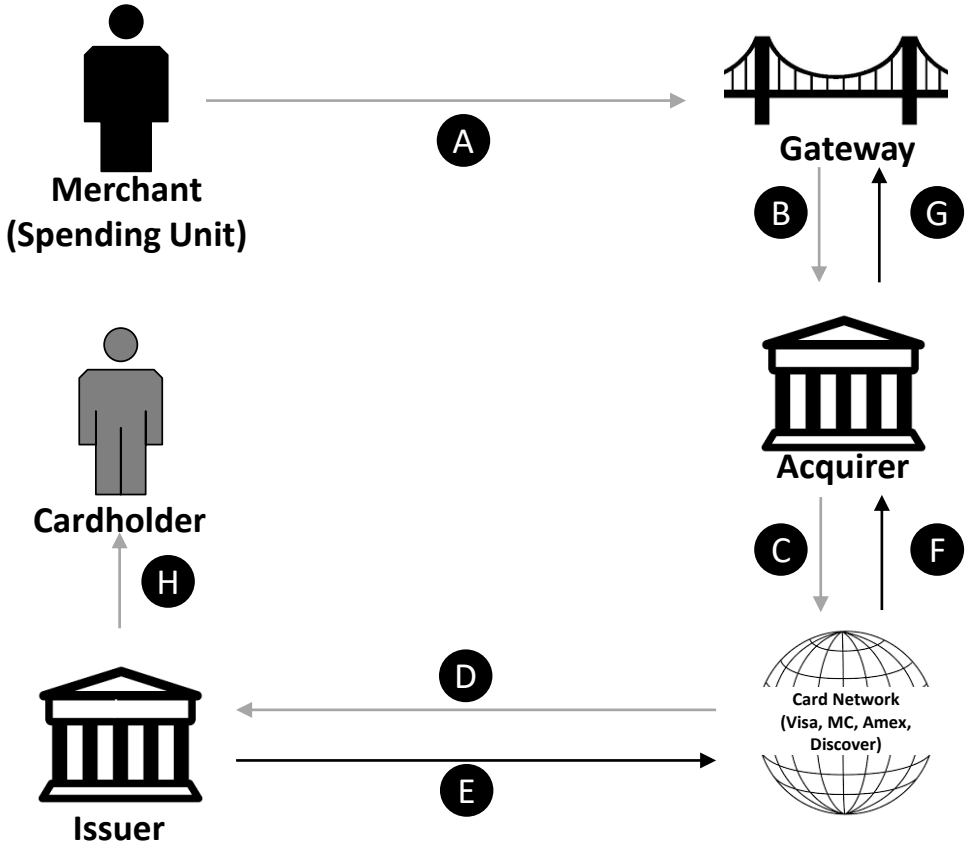
Mag Stripe:

- Account information is stored on mag stripe
- Data is static and consistent on every transaction, making it more susceptible to fraud
- Card is swiped in the terminal (contact) or card or phone is tapped against the terminal (contactless)

Note: *It is the preference of the STO to accept EMV whenever possible in order to reduce liability on the spending unit.*

TRANSACTION PROCESSING

Clearing and settlement process



Clearing and Settlement Process

A. Upon end of day, merchant (spending unit) sends the batch of approved transactions (typically at the end of the day) to the gateway (if terminal batch capture applies).
B. Gateway validates the batch and routes it to the acquirer.
C. Acquirer aggregates merchant (spending unit) batches and submits to the credit card network for clearing.
D. Credit card network sends each approved transaction to the appropriate issuing bank.
E. Issuing bank transfers funds to the payment brands.
F. Card network pays the acquirer.
G. Funds are deposited in the STO bank account by the acquirer.
    - All processing fees are charged on a monthly analysis/invoice from the acquirer to each spending unit.
H. Issuing bank posts transaction to the cardholder's statement. This is known as the clearing step of the process and occurs simultaneously with the settlement process (step E).

CARD PRESENT BEST PRACTICES

- **Swipe/insert or enter the card through the point of sale (POS) system.** Avoid manually keying card information whenever possible. This helps reduce the chance of errors. Cards swiped/inserted directly into the POS typically have lower interchange fees than those manually keyed.
- **Validate the card.** Check the expiration date, ensure the payment brand emblem is present and the card is not altered.
- **Obtain a signature.** Obtain a signature on the receipt or invoice – especially on larger transactions.
- **Prohibit storage of cardholder data.** Spending units that do not store cardholder data help protect the spending unit and the State of West Virginia against becoming targets of theft.
  - All card present related documents must be kept in accordance with the spending unit record retention policy. All spending units must have a record retention policy approved by the Department of Administration.

CARD PRESENT BEST PRACTICES

- **Properly authorize the transaction.** Confirm the authorization response provided and take the appropriate action. Visa provides the following guidelines for responding to the response codes provided on an authorization request.

Authorization Response	Meaning[1]
Approved	Card issuer approves the transaction. This is the most common response.
Declined or Card Not Accepted	Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account.
Call, Call Center, or Referrals	Card issuer needs more information before approving the sale. You should call your authorization center and follow whatever instructions you are given. In most cases, an authorization agent will ask to speak directly with the cardholder or will instruct you to check the cardholder's identification.
Pick Up	Card issuer wants to recover the card. Do not complete the transaction. Inform the customer that you have been instructed to keep the card, and ask for an alternative form of payment. If you feel uncomfortable, simply return the card to the cardholder.

- **Settle the transactions daily.** Transactions not settled within a day are subject to higher interchange rates. Settling daily also helps ensure any issues can be addressed more quickly.

[1] ***Source:*** *https://usa.visa.com/dam/VCOM/global/support-legal/documents/card-acceptance-guidelines-visa-merchants.pdf*

CARD NOT PRESENT BEST PRACTICES

- **Utilize the E-Gov system for card not present transactions.** Unless required, it is recommended to not accept credit cards over the phone but to direct customers to use the E-Gov system to help reduce merchant's (spending unit's) liability and to be consistent with PCI DSS.
  - If a spending unit determines they must accept credit card information over the phone in order to be able to complete a transaction, they should adhere to the following:
    - Enter payment details provided directly into the terminal.
    - Do not write down any cardholder information or payment details provided.
    - If any payment details must be captured, ensure they are securely deleted as soon as the transaction has been completed.
    - Report any incidents of storage, misuse or breach of cardholder information to spending unit management and the STO.
    - Use a cross-cut shredder when destroying any transaction information.

CARD NOT PRESENT BEST PRACTICES

- **When available, verify the cardholders address using the Address Verification Service (AVS).** This service helps validate pieces of the cardholder's billing address with the card issuer.
- **Maintain records of supporting information to help complete research and disputes when needed.** Maintaining internal records of receipts and/or invoices (where applicable) can assist staff in investigating fraud if suspected and provides historical documentation in the event a chargeback occurs.
- **Confirm the purchase with the customer.** Especially on large ticket items, incorporate into the customer service process to validate the transaction with the customer. Keep a record of the conversation for documentation backup purposes.

CARD NOT PRESENT BEST PRACTICES

- **Clearly communicate the return, refund and cancellation policy.** Display the policy clearly for customers when they're completing their purchase and have staff outline the policy for customers (see also the *Chargebacks* section on p. 26).
- **Provide email confirmations.** Following a sale or return, send the customer an email confirmation. For returns, indicate to the customer that it may take a billing cycle for the return to appear on their billing statement.

REFUNDS, VOIDS AND EXCHANGES

- **Refunds** are settled funds that are transferred from a merchant's (spending unit's) account back to the customers for goods or services purchased.
- **Voids** cancel the transfer of funds from a customer to the merchant (spending unit) before the payment transaction is settled.
- **Exchanges** allow for a transfer of the goods or services provided to the customer for funds settled; depending on the value of the exchanged goods/services, a balance of funds may be due to either the customer or the merchant (spending unit).

State of West Virginia spending units are responsible for developing, training employees and properly communicating any policies relating to refunds, voids and exchanges both for online and in person transactions.

CREDIT CARD DISPUTES

- Below are the steps involved in handling a dispute for payments through the STO's E-Gov system:
  - **Discover/Visa/MasterCard disputes**
    1. Fax is received from the acquiring bank Merchant Service's department with dispute information.
    2. E-Government staff member verifies the transaction in the E-Gov system.
    3. E-Government staff member will reach out to the spending unit that corresponds with the transaction to verify the transaction was a legitimate purchase.
    4. If the spending unit deems the transaction to be legitimate and wants to fight the dispute, they supply the STO with any information they have to prove the transaction should have taken place.
    5. E-Government staff member will fax all documentation to the acquiring bank's Merchant Services for their review.
    6. The acquiring bank's merchant's services will either accept the State's rebuttal or deny it. If accepted, no further action is needed. If denied, then an E-Government staff member will refund the transaction in the E-Gov system and inform the spending unit that the money was refunded to the customer.

CREDIT CARD DISPUTES

7. Even after acquiring bank accepts the State's rebuttal, there is an opportunity for the cardholder's bank to open a second dispute or the cardholder to enter into arbitration via their card brand.
8. The State does not enter into arbitration. If arbitration is requested by the customer, then an E-Government staff member will refund the payment in the E-Gov system and notify the spending unit.

- **American Express disputes**
  - For American Express disputes, the same steps are followed as above except the dispute comes directly from American Express.

- The only difference in the E-Gov process and point-of-sale transactions is that dispute notices are sent directly to the merchant (spending unit). Please refer to #1 for information.

CHARGEBACKS

- **Process**
  - Total processing time for retrieval requests for Visa, MasterCard and Discover is 27 days from the time the request is filed. Total processing time for chargebacks for Visa, MasterCard and Discover is 38 days. Total time for both retrieval requests and chargebacks for American Express is 17 days.
  - The number of days for merchants (spending units) to respond varies, but could be limited to 7 to 10 days. If the merchant (spending unit) does not respond within the number of days stated on the request, the card brand or issuing bank will make the final decision without the response. Responding within the allowed timeframe does not guarantee a decision in favor of the merchant (spending unit). Not responding within the allowed timeframe does not guarantee a decision in favor of the consumer.
  - If a chargeback is filed against a merchant (spending unit), the acquiring bank's chargeback team will fax the merchant (spending unit) the documentation. If the merchant (spending unit) does not have a working fax number, the system will generate the chargeback/retrieval request information into a letter that will be mailed to the merchant (spending unit). The merchant (spending unit) then has the above mentioned timeframes to respond.

CHARGEBACKS

- Credit Card disputes for online purchases that process through the STO's E-Gov system are received by the STO. The STO will contact the spending unit for which the disputed payment is for to submit a reply by the deadline.

- **State Spending Unit Responsibility**
  - State spending units/agencies are responsible for truncating all but the last four digits of consumer credit card numbers on any documentation. Please contact the acquiring bank/vendor for any questions regarding such documentation.
  - Credit Card disputes for online purchases that process through the STO's E-Gov system are received by the STO. The STO will contact the spending unit for which the disputed payment is for to submit a reply by the deadline.

CHARGEBACKS

- Strategies that can help merchants (spending units) reduce the risk of receiving chargebacks include:
  1. **Follow policies and guidelines for processing credit cards.** Follow guidelines and best practices outlined by processors, card brands, the State of West Virginia and the STO.
  2. **Clearly communicate return/exchange policies and handle any customer issues promptly.** At the time of the transaction, clearly display any return or change policies. Respond quickly to any customer call or complaints made to your organization/spending unit to help reduce the potential number of customers who file chargebacks.
  3. **Train employees.** Train employees to handle credit card information correctly, potential ways to prevent fraud and chargebacks (e.g. validating signatures, card expiration dates, etc.) and completing the appropriate documentation.
  4. **Maintain proper records.** Maintain records with order or contract information, along with customer signatures (if available).
  5. **Fight chargebacks (when appropriate).** Fighting chargebacks takes time and resources, but it may be worth pursuing if a merchant (spending unit) thinks they can win.

FRAUD

- If fraud is suspected, spending units should:
  - If fraudulent credit card payments are suspected through the STO's E-Gov system,
    - Notify the STO immediately of the suspected fraudulent activity.
    - The STO will contact the State's acquiring bank to report the suspected fraud, and
    - The acquiring bank will contact the appropriate card brand to report the suspected fraud to have the card brand investigate.
  - If fraud is suspected with the credit card terminal and/or the terminal has been tampered with,
    - The merchant (spending unit) should contact the acquiring bank and local law enforcement immediately,
    - The acquiring bank would notify Loss Prevention, and
    - Loss Prevention would send a request to have the v# (terminal ID) closed and a replacement terminal sent out if desired.
  - If it is suspected that that merchant account or merchant terminal was compromised, the merchant account will be closed, a new merchant account (MID) will be opened and a replacement terminal will be sent.

FRAUD

- If a card is presented that has been coded as “fraudulent/lost/stolen,” the terminal will decline the transaction.
  - The merchant (spending unit) should ask the customer for another form of payment. If the customer has questions, they should be directed to call their bank.
  - The merchant (spending unit) and acquiring bank should notify the STO of the problem and the resolution.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)

- **Payment Card Industry Data Security Standards (PCI-DSS)** applies to protecting cardholder data. Compliance is determined through a security assessment and reported through Self-Assessment Questionnaires (SAQs) or Report on Compliance (ROC). See page 32 in this handbook for additional information on completing SAQs to ensure PCI-DSS compliance.
- State spending units who accept credit card payments must do so in accordance with PCI-DSS. All technology and business processes implemented in association with transmitting, storing or processing credit cards must be in accordance with the PCI-DSS. The cost of equipment or other related business processes will be the responsibility of the agencies.
- In accordance with PCI-DSS, agencies are prohibited from storing sensitive cardholder data on any systems, databases, spreadsheets, email or paper files. PCI-DSS classifies the following as sensitive card data:
  - Security codes (CVV2, CVC2, CID).
  - PIN/PIN block.
  - Full magnetic stripe data or equivalent data on a chip.
  - Full Personal Account Number (PAN)

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)

- PCI compliance for spending units is likely assessed using Self-Assessment Questionnaires (SAQs). The required SAQ is dependent on the type of organization and how credit card payments are processed.
  - All spending units that take credit card payments must complete a yearly Self-Assessment Questionnaire (SAQ) to maintain PCI compliance.
  - The STO offers spending units a service to help with completion of their SAQs.
    - The spending unit should identify an internal staff member to serve as the PCI contact.
    - Once the PCI contact has been established, they will be setup with access to the SAQ service.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)

- The PCI-DSS identifies twelve basic security requirements for merchants (spending units) processing credit card payments in order to protect cardholder information.

Goals	Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall and router configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications

Source: *https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf*

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)

Goals	Requirements
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

- For more information, please see the PCI Security Standards Council website: https://www.pcisecuritystandards.org/.

Source: *https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf*

PERSONAL IDENTIFIABLE INFORMATION (PII)

- **Personal Identifiable Information (PII)** is data that can be used to identify an individual's identity such as social security numbers, date of birth, email address, bank account number, etc. Merchants (spending units) have responsibility to ensure their customers' PII is safeguarded.
- Rules and regulations govern protection of PII. Best practice is to have an audit completed at the spending unit's discretion to ensure PII compliance at both an organization's governance, procedural and operational levels. Spending units are responsible to protect all customer PII when processing payments.

ENCRYPTION AND TOKENIZATION

- Two methods often used to help protect cardholder information and help protect the State of West Virginia and its spending units include:
  - **Encryption**, which scrambles data so it is unreadable to anyone but those who have an 'electronic key' to decrypt the data.
    - Spending units have access to terminals that are capable of encrypting card information for payments made in person. See the approved list of terminals for more information.
    - Encryption services are also available by the STO's gateway provider for payments made through E-Gov.
  - **Tokenization**, or the process of replacing sensitive data with a non-sensitive data equivalent (called a token) that has no useable meaning or value. Tokens are only reversible to those who have the original key used to create the token.
    - The STO recently developed the ability to tokenize credit cards that are processed through the E-Gov system. Please contact the STO for more information.

MERCHANT (SPENDING UNIT) RESPONSIBILITIES

- With regards to processing credit card payments, West Virginia spending units are responsible for:
  - Completing the required process with the STO to accept credit card payments.
  - Adherence to Federal and State of West Virginia policies and laws and complying with PCI-DSS requirements.
  - Validate PCI compliance annually, which includes the completion of the Self Assessment Questionnaire (SAQ) and associated processes, where applicable.
  - Work with the STO and authorized partners in the initial setup for payment processing and ongoing operations.
  - Ensure with internal IT Division any new equipment will connect properly to current network.
  - Designating an individual to hold primary responsibility and authority for payment processing.
  - Designing and maintaining security policies and procedures for processing payments, handling devices and handling credit card information. Any policies and procedures need to be developed taking into account PCI requirements. Policies should include approval from spending unit finance/business office as well as the STO.

MERCHANT (SPENDING UNIT) RESPONSIBILITIES

- Providing training to all employees regarding proper payment processing and cardholder information protection protocols. Limit use of equipment to authorized personnel who have been trained to process credit card payments.
- Ensure proper segregation of duties, which includes transaction processing, reconciling and reporting. The individual processing the payment should not also prepare the deposit in *wv*OASIS.
- Accepting payments using the systems and devices approved by the STO.
- Keep any physical terminals in a safe and secure location with limited physical access. Equipment should be checked at the beginning of work day for any suspicious activity and/or skimmers.
- Maintain an up-to-date list of devices and ensure all devices utilized are in good condition and have not been tampered with or substituted by another device.
- Paying the required costs and fees associated with processing payments and implementing solutions and processes for securing cardholder data.
- Limit access to payment and cardholder data to appropriate staff. Maintain appropriate hierarchies of access to fit individual roles and responsibilities.

MERCHANT (SPENDING UNIT) RESPONSIBILITIES

- Monitor chargeback and fraud activity and respond in a timely manner, as required.
- Batch payment transactions daily. This will ensure deposit is made at the bank within one business day as required by W.Va. Code §12-2-2.
- Address any questions or inconsistencies with batch settlements in a timely manner. Notify the STO of any discrepancies found.
- Perform daily reconciliation of receipts and deposit entries. This should be done by an employee other than the staff member that processed the payment transaction.
- Keep needed internal documentation safe and secure for documentation and reference purposes.

STATE TREASURER'S OFFICE (STO) CONTACTS

- West Virginia State Treasurer's Office

  Check Hotline: 304-558-3599

  Email: checkhotline@wvsto.com

- For E-Government specific questions please contact the Check Hotline number above or send email to egovernmentCM@wvsto.com