

# VERSION NOT FINAL

## **Resource: Considerations When Accepting Payment Cards Credit Card Acceptance and Merchant Services**

### **Background**

Acceptance of credit and debit cards (herein referred to as 'payment cards') as a payment method has become widely accepted in the public sector. Many governments now accept cards for taxes, fines, user charges and fees. There are many benefits to accepting payment cards, including:

- Enhanced customer service and convenience
- Increased certainty of collection
- Accelerated payments and the availability of funds
- Improved audit trail
- Reduced cashiering costs
- Improved overall cash flow and forecasting
- Lessened delinquencies
- Reduced return check processing costs
- Reduced collection costs

There are also some considerations to accepting payment cards, including:

- Can be expensive
  - Security/Payment Card Industry-Data Security Standards (PCI) compliance
  - Fees on transactions
- Increases in budgets to cover credit card processing fees
- Settlement timing difference from cash/check and how to reconcile
- Time and processing to handle chargebacks

When governments look to accept payment cards or review their current policies and procedures related to payment card acceptance, there are many items that need to be considered. These include:

- Federal, state, provincial, and local laws
- Types of Cards to Accept
- Card Acceptance Process
- Accepting payment cards for various government charges
- Determining how / where payment cards will be accepted
- Merchant Services
- Merchant Identification Numbers (MID)
- Fees charged to governments when accepting payment cards
- Using third party services to accept payment cards
- Equipment needs for physical locations
- Online payments
- Understanding and Implementation of PCI compliance standards

Merchant Services provide the methodology a merchant (government) would need to accept card payments online and offline. Card payments may refer to credit cards, debit cards, e-checks, ACH payments, e-wallets and mobile payments. Governments will need to enter into an agreement for merchant services with one or more providers, depending on the services needed:

- Merchant Processors are the entities that settle the transactions accepted. They facilitate the transaction between the payer and the payee.

# VERSION NOT FINAL

- A Gateway is a service that securely collects, stores, authorizes, and transmits the transaction data to a payment processor for every transaction.
- It is common for a Merchant Processor and Gateway to be separate entities that are contracted with. However, there are some entities that offer both services under one umbrella. Not all merchant processors work with every gateway, the government should verify that any entities they are considering for these services are compatible and meet their needs.

## **Federal, state, provincial and local laws**

Governments should first review applicable laws to determine whether card acceptance is an option, and/or what criteria need to be followed to be in compliance.

## **Types of Cards to Accept**

- There are many different types of credit cards available. The most commonly used cards are Visa and MasterCard. Other cards that are frequently used include Discover and American Express. Each card type will have a different fee schedule attached and some cards are more expensive to accept than others.
  - If you accept Visa or MasterCard, or any other brand of card, all cards of that brand must be accepted.
    - This includes any branded rewards cards, such as those issued by airlines offering miles with a certain amount of card usage.
      - Note: Any card that has additional rewards, branded or otherwise, carries with it a higher fee to the merchant in order to pay for the additional rewards.
      - This means that as reward cards gain popularity, the cost to accept these cards increases.
- Governments are encouraged to review existing (or estimate potential) usage of each card brand (e.g., Visa, MasterCard, American Express, and Discover) and types (credit or debit cards), in order to determine which brands and types to accept.

## **Card Acceptance Process**

- Cards issued within the US generally contain both a chip and magnetic strip to prevent usability issues.
- Accepting a credit card by swiping the magnetic strip is the method most vulnerable to fraud and not a recommended practice.
  - Governments (merchants) are liable for fraud generated using a swipe.
  - Customers may file a claim to have their money refunded, whether legitimate or not, leaving the government (merchant) liable.
- Using the chip-enabled machines, where customers insert the chip into the card reader, allows for a more secure transaction that is less vulnerable to fraud.
  - The chip allows the data to be encrypted for one-time use.
  - Governments are generally not liable for fraudulent transactions if processed in this manner.
  - GFOA strongly recommends all governments upgrade their credit card terminals to be chip-enabled.
- Contactless Payments
  - Contactless payment systems are credit cards and debit cards, key fobs, smart cards, or other devices, including smartphones and other mobile devices, that use radio-frequency identification (RFID) or near field communication (NFC) for making secure payments.
  - There are multiple forms of contactless payments including a credit card issued with NFC capability, ApplePay, SamsungPay, and GooglePay, which are generally used on a mobile device.
  - These work by tapping the credit card or mobile device to the credit card terminal, which tokenizes as it passes through and processes the payment.

# VERSION NOT FINAL

- These payment types are not EMV chip transactions so do not fall under the liability shift as there is no chip inserted into the terminal. Check with your merchant services provider as to the possible liability shift with contactless payment transactions
- 

## **Accepting Payment Cards for Various Types of Government Charges (fees, taxes, licenses, events, etc.)**

- Governments should consider whether they want to accept cards for mandatory charges (such as taxes and utility bills) or discretionary charges (such as recreation fees and performing arts admissions), or both.
- Consider the government's potential need to accept payment cards at special events (at different locations and for limited periods of time, and the staffing implications).

## **Determining How/Where Payment Cards will be Accepted (in-person, phone, kiosk, web)**

- **Card Present Transactions** - These types of transactions are the least risky for merchant providers as the card itself must be present. Types of Card Present Transactions include:
  - At a payment window
  - Kiosk
- **Card Not Present Transactions** – These types of payments are more risky as they only require the information to be typed in, and not dipped or swiped. They are more costly. Types of card not present transactions include:
  - Manually entered into the terminal
  - Phone / IVR system
  - Online payments

## **Merchant Identification Numbers (MID)**

- A Merchant Identification Number (MID) is a unique code provided to the merchant (government) by the Merchant Processor that identifies a specific merchant and location.
- Most major credit card companies require that the merchant name and location (address or site that accepts payments) be disclosed on transactions, which means a government should set up a MID for each specific department or area. Examples:
  - A government building may house multiple departments (treasury and licensing). A MID should be set up for each department to help with identification, reconciliation and chargeback issues that may arise.
  - A government parks operation may have multiple locations and depending on volume and organization of activities, it may make sense consolidate them under one MID, or have a MID set up for each location.

## **Fees Charged to Government When Accepting Payment Cards**

- Governments should be aware that different card processing service providers may have significantly different rates and fees depending on the methods they use to process payment card transactions. Fees may include:
  - ***Discount rate*** - The percentage of the sale that payment card service providers charge merchants for processing transactions. This involves all fees that are paid to card issuers and networks via interchange fees and assessment fees. The mode of presentation (card present, telephone, Internet) will impact the overall discount rate.
    - ***Assessment fee*** - a smaller fee that is paid directly to the card network (Visa, MasterCard, Discover, etc. for use of the network. Rates may vary between credit cards and debit cards.

# VERSION NOT FINAL

- *Interchange fees* - the largest component of the discount rate. It is paid by the merchant's bank to the customer's bank but is passed along to the merchant in the discount rate. These are the standard fees applied based upon merchant code by the merchant card companies (e.g. VISA, Mastercard).
  - *Merchant Service Provider Fees* - These are variable fees based upon the value of the transaction or fixed fee per transaction. Due to the complexity of the fee structure, governments should be prepared to monitor the billings on a regular basis in order to ensure that the government is not overcharged.
  - *Administrative fees* - Various fees that may be charged by the payment card provider or processor. Some of the more common are statement fees, PCI non-compliance fee, chargeback fees, terminal fees, and settlement fees.
- Three common Credit Card Processing Quotes from Merchant Providers are:
  - Interchange-Plus
    - This is the most commonly used fee structure of merchant providers.
    - Credit Card companies charge an interchange fee for each transaction
    - With this rate structure, merchant providers will mark up this amount and charge you the increased amount.
      - Ex. 2.75% + \$.10
      - \$.10 is the marked up price and the 2.75% is the credit card interchange fee. The 2.75% charge could be changed by MasterCard or Visa.
    - The type of card (debit, credit, or rewards card) will factor into the fee paid.
  - Flat Rate
    - Merchant provider charges business either a flat fee per transaction, a fixed percentage per transactions, or a mixture of the 2 each time a transaction is processed.
    - Very transparent fee structure.
  - Blended or Tiered Pricing
    - Least transparent of the fees
    - Tiers are based on cost structures.
  - Annual Rate Review – It is good practice to do an annual review with your provider in addition to the government's monthly review of each merchant statement. Governments will need to initiate the annual rate review and should be scheduled like any other audit to ensure the entity is receiving the lowest cost for merchant services.
- Merchants collect fees generally in the following ways:
  - Net – the gross settlement amount is reduced by fees each day.
  - Gross – the fee is paid through a separate, automatic debit from the government's bank account at the end of the month
  - Invoice to the government (very unusual)

The government should evaluate the fee payment structure to determine the best fit for managing their program. Be aware that you as the government are in control of the process of payment and should push for gross settlement, not net, even though the vendor may request that.

## **Governments Using Third Party Service Providers to Accept Payment Cards**

- Governments can use third party service providers to accept payment cards. These can be especially helpful if there are laws surrounding what types of fees governments can charge. These arrangements often involve a web portal where a constituent is redirected from the government's website to the third party to make their payment. Often the third party will charge the constituent a fee, flat or percentage, and then remit the full bill amount back to the government. This way the government does not touch the fee nor do they charge the fee to the constituent.

# VERSION NOT FINAL

## **Governments Charging Customers When Using Payment Cards**

- *Convenience fees.* Governments may consider charging a convenience fee for transactions. Convenience fees can be charged when the government is offering an alternative method of payment that is nonstandard for the government. If the norm is accepting payment in person, then convenience fees may be charged for online payments. The constituent is paying for the convenience of not paying in person.
  - The advantage of convenience fees is that they can recoup the cost of merchant fees.
  - A disadvantage of convenience fees is that they may deter some users from paying with a card.
  - These types of fees are available to all types of merchants.
- *Service fees.* Governments may consider charging a service fee for transactions. Service fees are fees which only higher education and governments may charge. These types of fees may be charged on all credit card payments whether online or in person.
  - In the US, Service Fees may be charged on:
    - Tax Payments – Merchant Category Code (MCC) 9311
    - Government Services (Not classified elsewhere) – MCC 9399
    - Fines – MCC 9222
    - Court Costs – MCC 9211
    - Colleges, Universities, Professional Schools, and Junior Colleges – MCC 8220
    - Elementary and Secondary Schools – MCC 8211
    - Business and Secretarial Schools – MCC 8244
    - Vocational and Trade Schools – MCC 8249
  - To charge Service Fees, the government must follow these guidelines (in consultation with the merchant services provider):
    - Disclose fee clearly to cardholder before transaction is completed and provide them an opportunity to cancel the transaction without a penalty.
    - Not represent fee as being a fee charge by the credit card provider but by the entity.
    - Ensure the Service Fee amount is:
      - A reasonable reflection of costs, and possibly capped
      - A flat, fixed, banded or ad valorem amount regardless of the value of the payment
      - Assessed only on the final amount, net of all discounts and rebates applied during the transaction.
      - May not be charged in addition to a Convenience Fee.
- Any fees charged must be in compliance with state and local laws

## **Equipment Needs at Physical Locations**

- A variety of equipment exists to aid in accepting credit cards at physical locations
  - Physical locations may generally include the following:
    - Standalone terminals
    - Terminals connected to a Point-of-Sale (POS) system
    - Kiosks (e.g., parking garage)
    - Mobile payment unit used for events or offsite payments
  - The equipment will require at a minimum:
    - Chip Reader (EMV Compliant)
    - Data Connection – phone line, internet connection (IP address), or wireless capability
    - Some environments may require:
      - A dedicated server – necessary for many kiosk systems or POS systems.
      - Special extensions to fit in a secure environment (glass or other barrier)
      - A dedicated PC hooked into a network (e.g., kiosk).
      - Wireless terminal for offsite events or field operations (e.g. parks or inspections activity)
        - Wireless terminals should not be connected to an unsecure Wi-Fi network, as that is not PCI compliant.

# VERSION NOT FINAL

- Wireless terminals should connect to a cellular network and that a proper cellular signal can be obtained at the location
- Leasing vs Buying – two options available for acquiring equipment
  - Lease – usually a monthly payment per piece of equipment, can sometimes come free with overall service package, maintenance/replacement usually covered by provider.
  - Buy – payment up front is required, government owns equipment which is subject to manufacturer's warranty only.
  - Warranties – verify the beginning and end of the warranty period and verify that the equipment meets PCI Compliance standards and is compatible with your merchant (if you buy through a 3<sup>rd</sup> party or re-use old equipment).

## Online Payments

- Online payments – It is important that online transactions are safe and secure. The following steps outline some important precautions to take:
  - GFOA recommends governments do not take credit card payments directly on their organizations website, as it increases data risk under Payment Card Industry (PCI) Compliance Standards. For more information on PCI Compliance, visit <https://www.pcisecuritystandards.org/>
  - Many online portals use a “redirect” from the government's website to the payment provider's site
    - The site is usually branded to your government, so the customer does not realize they have been re-directed.
    - It is recommended that you verify that your provider's **portal is PCI Compliant, and that the credit card information is stored directly on their site, therefore mitigating the government's risk. Note: the credit card data should never be entered or stored on the government's computer network.**

## Understanding and Implementing PCI Compliance Standards

- These standards are a set of rules established by the Payment Card Industry (not a law)
- The standards apply to everyone who accepts payment cards
- The standards were instituted to prevent payment card fraud.
- They are regulated and updated by the PCI Security Standards Council (<https://www.pcisecuritystandards.org>)
- Not complying with PCI-DSS Standards may result in:
  - Financial losses and penalties
  - Termination of ability to accept payment cards
  - Legal costs
  - Loss of customer trust / negative effect on customer information security (ID theft)
  - Additional costs assessed by the merchant services provider for non-compliance
- PCI DSS Requirements – See table below:

# VERSION NOT FINAL

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect cardholder data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
Protect Cardholder Data	<ol style="list-style-type: none"><li>3. Protect stored cardholder data</li><li>4. Encrypt transmission of cardholder data across open, public networks</li></ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"><li>5. Use and regularly update anti-virus software or programs</li><li>6. Develop and maintain secure systems and applications</li></ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"><li>7. Restrict access to cardholder data by business need-to-know</li><li>8. Assign a unique ID to each person with computer access</li><li>9. Restrict physical access to cardholder data</li></ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes</li></ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security for employees and contractors</li></ol>

- To be PCI Compliant, each government is required to:
  - Fill out an annual Self-Assessment Questionnaire (usually one per tax ID per merchant services provider used, if more than one)
  - Adopt a formal policy on credit card acceptance
  - Provide annual training to staff that accept payment cards
  - Provide training to new staff that accept payment cards
  - Perform quarterly computer network scans using an Approved Scanning Vendor (ASV)
  - Perform additional network scans as needed (e.g. when new equipment is placed or there is a change in the computer network).
  - Maintain documentation on all processes, changes, training, etc.
  - Maintain a high level up to date network diagram and data diagram.
- Governments should evaluate their processes and determine if they are able to manage PCI Compliance in house, or contract with a vendor to aid in the process.

## **Chargebacks**

- A chargeback is a dispute by the cardholder identifying a transaction that they believe was processed on their account inappropriately.
- There are many reasons for chargebacks, including fraudulent transaction, duplicate transaction, or ineffective service.
- Governments need to understand the chargeback process of their merchant vendor and set up appropriate procedures for managing chargebacks and disputing them, when appropriate.