



BEST PRACTICE

Accepting Payment Cards and Selection of Payment Card Service Providers (1999, 2002, and 2009) (TIM)

Background. Acceptance of credit and debit cards (herein referred to as “payment cards”) as a payment method has become virtually universal within the private sector, and more common within the public sector. Many governments now accept cards for taxes, fines, user charges and fees. For a fee, a payment card processing service provider will work with a government to accept and process payment card payments.

While governments may have to absorb extra costs or citizens may have to pay an additional convenience fee for the transaction, establishing a payment card system may be an attractive addition to a government’s collection office, as long as it is executed properly.

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 cashing costs
- Improved overall cash flow and forecasting
- Lessened delinquencies
- Reduced return check processing costs
- Reduced collection costs

Recommendation. The Government Finance Officers Association (GFOA) recommends that governments evaluate whether accepting payment cards as a payment option is reasonable and appropriate for the type of charges or fees being paid, and the level of customer service desired.

In establishing a payment card acceptance program, governments should consider and evaluate the following:

- **Federal, state, provincial and local laws.** Governments should first review applicable laws to determine whether card acceptance is an option.
- **Scope.** Typically, in implementing a system to accept payment cards, governments should determine the required scope for the system and the services required from a payment card service provider. Governments should:
 - 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. Be sure to review seasonal use, such as park fees in the summer.
 - Consider payment type. 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.

- Inventory any hardware the government uses to accept payment cards. In some cases, the equipment may be easily and inexpensively reprogrammed for a new vendor, while in other cases, new hardware may be necessary.
 - 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).
 - Review and document existing processing procedures, focusing on the process used to receive cards.
 - Consider mode of presentation: office, Internet, lockbox processing facility, temporary or mobile location, telephone.
 - Evaluate internal system security capabilities to determine whether to contract directly with a payment processor or through a third party portal. It is the government's responsibility to be payment card industry (PCI) compliant.
 - Consider government's liability in the event of a security breach, loss of data, or default by the payment card service provider or third-party portal.
 - Consider intergovernmental cooperation arrangements and whether piggy-backing is an option.
 - Determine if changes are needed to the government's internal control system to the acceptance of payment cards.
- **Fees.** 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 fee that payment card service providers charge merchants for processing transactions. These are fees based upon the mode of presentation (card present, telephone, Internet).
 - **Interchange fees** - This is 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).
 - **Bank 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.

Governments should negotiate the lowest possible fee to minimize the financial impact to the government or to the consumer, whichever party will ultimately pay the fee.

- **Internal costs and benefits.** Governments should bear in mind their own costs in processing cards, such as:
 - **Administrative costs.** Governments have their own costs for equipment and associated personnel necessary to process card transactions, including costs associated in ensuring PCI compliance, which is the governments' responsibility.
 - **Cost savings.** Governments should measure their administrative cost savings and compare this against receiving and processing checks and cash transactions.
 - **Convenience fees.** Governments should consider charging a convenience fee for transactions. 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. In addition, card companies have strict regulations that limit the use of convenience fees (for example, payments made by telephone or via a third-party processor. In most instances, major card companies do not allow governments or businesses to pass on merchant fees directly to customers.

- **Request for Proposal.** GFOA recommends competitive procurement of card processing service providers. Governments should use the RFP process when selecting a vendor. This process allows a government to gather data necessary to make an appropriate selection.

Governments may consider issuing a joint RFP with other jurisdictions because larger card volumes generally result in lower fees. As well, governments may include a section on merchant services in their banking services procurement RFP. Third-party processors, such as commercial automated services capable of processing card transactions seven days per week, 24 hours per day, should be considered as part of the evaluation because they may prove to be essential in recovering discount fees. GFOA further recommends that a card acceptance agreement be made as a bank services agreement administered by the public official in charge of the treasury function.

In the RFP process, governments should evaluate:

- How funds are made available to the government. The funds' availability may range from same day, next day credit to next week credit. Depending on volume, this could be important in determining the profit/cost/benefit position of the program.
- The equipment that may be required. Differences in equipment requirements may affect the initial cost of the program as well as its the long term operating efficiency. For example, the cost of new equipment may be offset by a lower discount rate or per -item fee. A break-even analysis should be performed to evaluate the options. Consider leasing versus buying for equipment as leasing provides the flexibility to stay current with changing technology and security requirements.
- Whether the payment vendor fees and the actual payment to the government are considered two different and separate transactions, so that the tax/fee is automatically sent to the government and the processing fees are automatically sent to the payment vendor service for processing.
- The vendors' reporting capabilities. Each vendor's reporting capabilities should be evaluated. While most vendors provide the basic information, governments should evaluate the vendor's ability to provide customized reports and interfacing capability.
- The vendors' procedures and experience in maintaining security. This review should include the vendor's response to security breaches or loss of information. Service providers should provide a comprehensive review of their internal and external security procedures. Pay particular attention to the Internet sign-on and multi factor identification procedures. Standard protocols include passwords, tokens, fingerprint or bio-metrics.
- The government's liability in the event of a security breach, loss of data, or default by the payment card service provider or third-party portal.
- Experience with governments as the needs of governments differ from private sector entities. Governments should consider this and any special pricing arrangements the vendor has for governments.
- The training provided by vendor.
- The vendor's problem resolution, including the timely processing of chargebacks.

References.

- *An Introduction to Treasury Management Practices*, GFOA, 1998.
- *An Introduction to Electronic Commerce: Government Cash Management Programs*, GFOA, 1998
- *Banking Services: A Guide for Governments*; GFOA, 2004.
- *Treasury Management Newsletter* articles
 - Five Myths About the Payment Card Industry Data Security Standard May 2008
 - The Payment Card Industry Data Security Standard: Where to Begin January 2008
- PCI Security Standards Council, <https://www.pcisecuritystandards.org/>
- Payment Card Industry Standards: <https://www.pcisecuritystandards.org/>

Approved by the GFOA's Executive Board, October, 2009.