Primer on
GSA SmartPay® Charge Card Program EMV "chip" Transition and Other Enhanced Security Considerations

Pursuant to section 1(b) of the Presidential Executive Order (EO) on "Improving the Security of Consumer Financial Transactions," also known at the "Buy Secure" initiative, the United States General Services Administration's (GSA), Office of Charge Card Management (OCCM), is transitioning the Federal Government's GSA SmartPay commercial charge card program to higher security EuroPay MasterCard Visa (EMV) standard "chip " type charge cards. The EO requires the Federal government to adopt "enhanced security features" on its commercial payment programs. This transition was undertaken to reduce program exposure to external fraud, as well as to show Federal leadership in moving to this technology. Among other issues, actions to enhance charge card transaction security involve both charge cards issued to Federal government agencies and other authorized organizations as well as merchant terminals used by these organizations to process charge card payments. This primer deals exclusively with the former (known as "card issuance") considerations, as opposed to matters related to card acquiring (wherein merchants accept cards as payment).

Chip or EMV charge card products contain a microprocessor which is embedded into the card. The chip creates a code known as a "cryptogram" for each transaction when inserted into a payment terminal while making a purchase. As a result, it is much harder to counterfeit these cards compared to traditional magnetic stripe cards, since a unique cryptogram is generated for each transaction and fraudsters have yet to be successful in counterfeiting the chip technology. These cards therefore offer significant protection against "card present" fraud, where the card is physically inserted into a payment terminal. These chip cards have already been deployed in many countries around the globe, and demonstrated their effectiveness in reducing card present fraud.

Card data from the face of the card or from the magstripe (which will also be present on chip cards as a back-up capability for the foreseeable future), can still be captured and used in online fraud, so it is important to remind cardholders to continue to monitor their transactions and monthly statements. As an added layer of security and to facilitate overseas acceptance, OCCM is requiring the issuance of Personal Identification Numbers (PINs) as one of the cardholder verification methods for every GSA SmartPay purchase and travel charge card. Within the U.S. PIN prompting may be very limited, however there are countries where PIN use is more prevalent, particularly at unattended kiosks such as those often located within public transit stations. We hope to encourage the payment industry in the United States to move towards further use of PIN-preferring corporate charge cards over time.

State and local government commercial charge card programs may face many challenges similar to those experienced by the Federal Government in making the transition to chip charge cards. Some organizations may even be unaware of the liability shift (described below), or the benefits of transitioning to chips cards. Although the GSA SmartPay program currently is not available for State and local government use, OCCM prepared this primer to share our lessons learned in dealing with the transition from a card issuance perspective.

As discussed in greater detail in the following paragraphs, we made certain changes to our issuer contracts to address chip card products/services in the wake of the EO. We also developed reports to track chip card issuance and activation, as well as to obtain data on chip-enabled transactions at the point of sale. Note that the attached contract documentation may be redacted to protect procurement-sensitive information, and that the capabilities and/or service offerings available from State/local issuers may vary from that available to the Federal Government. This primer is provided for informational purposes only, with no warranties, either actual or implied. Any mention of brand names in this primer is for descriptive reasons only, and is in no way to be construed as an endorsement of any particular product or service.

Contracts for charge card issuance products/services are generally commercial in nature, meaning that the products/services acquired are widely available from commercial sources. As a result, these products are affected by developments in the commercial marketplace. In the charge card industry, a significant driver in the move to chip card technology in the United States is what is known as the "liability shift," which is being instituted by the major payment card networks/brands. In essence, it makes the party who constitutes the weakest security link in the transaction processing chain liable for the cost of any external fraud associated with a transaction. The effective date of this liability shift for most point of sale transactions, with the exception of fuel dispensers and ATMs, is October 2015. As card present fraud rates for transactions within the United States are increasing, card issuers have a significant incentive to replace the magnetic strip cards they have in circulation with higher-security chip cards and merchants are incentivized to upgrade their terminals to utilize this chip capability.

When considering the **transition to chip technology** for your State/local card issuance program, consider the following:

1. Be familiar with what charge card products/services your current charge card issuing contractor offers and the terms & conditions of any contracts your organization has in place with these issuers. This includes information on pricing and your organization's existing liability, if any, for external fraud.
2. Discuss with your issuing contractor their current plans to address the "liability shift," and if they plan to issue chip cards.
    a. If so, request information on the schedule for replacing your program's cards with chip cards, and if any added costs are involved. Ensure you understand how your organization's liability for external fraud may change as a result of this transition. Be aware that many issuers are moving to chip cards to reduce their external fraud liability exposure, and are therefore issuing the chip cards at no additional cost. Also, ask about the Card Verification Method (CVM) for the chip cards -- Will these cards be "signature

preferring" or "Personal Identification Number (PIN) preferring?" Note that most of the chip cards being issued in the United States are of the "chip and signature" CVM variety. If your organization prefers to have the added security of a PIN, ensure you understand: (i) if your issuer can provide such a product, (ii) whether or not cardholders will be able to self-select a PIN and (iii) the conditions under which the cardholder will and will not be prompted for a PIN. Also ask about the issuer's strategy for issuing PINs (mailers, through a voice response unit when activating, etc.) and how PINs will be re-set in the event a cardholder forgets it. Please review the GSA SmartPay contract modification language, at the link provided below, for further information.

b. Ask what type of chips will be provided in the cards. They should be a recent version of Dynamic Data Authentication (DDA) or Combined Dynamic Data Authentication (CDA) type chips which meet applicable industry specifications and standards. Your servicing bank or associated networks/brands (MasterCard, VISA, etc.) can provide information on the chip specification versions which are acceptable/usable.
c. Request and review for acceptability the issuer's proposed schedule for replacing your cardholders' cards. The GSA SmartPay reporting requirements, mentioned below and appropriately tailored to your program's specifics, may help you in monitoring card issuance and activation rates as well as chip-involved transaction activity.
d. There are two main approaches to charge card issuance: "natural" and "forced." Natural reissue means that your issuer will issue the new (chip) cards as your cardholders' existing magstripe cards approach their expiration date. A forced approach issues new cards earlier, regardless of the expiration date of existing cards. If your issuer plans to employ a forced reissue approach (usually to get the chip cards issued more rapidly), ask if and when the issuer will cancel the existing magstripe cards, as our experience is that only approximately 30 to 50% of cardholders activate their new cards upon receipt under a forced reissue (because their existing card is not about to expire). Awareness of this issue is important as call center volume tends to spike when those cardholders who have not activated and begun using their new cards experience the impact of the cancelation of their existing cards prior to the date embossed on the card itself.
e. Inquire as to your issuer's customer service call center(s) preparedness to handle the expected level of chip card-related customer calls. To date during the GSA SmartPay transition, no significant increase in call center volume has occurred except when existing mag strip cards are cancelled under a forced reissue. Despite that fact, it is advisable to be aware of your issuer's ability to handle such calls, especially if PIN-preferring cards are to be issued.
f. Ask about your issuer's plan to train cardholders in the use of chip cards request. Review their planned approach, as well as any associated training materials for suitability.
g. Based on the response to item 2c above, consider if the contract with your issuer needs to be modified to include a schedule for the issuance of chip cards.
h. If your issuer is not planning a near-term transition to chip cards, ask how they intend to deal with the liability shift and if/how their plans will affect your organization's liability and costs for external fraud.

Example documentation on how the Federal GSA SmartPay Program approached the chip card conversion issue is provided below:

- *Contract Modification:* A modification to GSA SmartPay Master Contract was developed to make chip cards the standard card issued under the Federal Government-wide GSA SmartPay charge card services program. (Attachment 1, Redacted Contract Modification PDF)
- *EMV Issuance and Activation Status Report*: This report is designed to track contractor bank issuance of chip cards, and cardholder activation of those cards. (Attachment 2, Issuance and Activation Report)
- *EMV Transaction Report*: The EMV Transaction Report is designed to capture the total number of card present transactions and those that actually utilize the chip in processing the transaction, to the extent this information is available from the issuing banks and their associated brands/networks. (Attachment 3, EMV Transaction Report)

In other countries around the world, once chip cards are issued, fraudsters typically shift their strategy to increase their focus on card not present (on-line) transaction activity. It is therefore important that government commercial charge card issuing programs not only consider the implications of chip cards, but also other fraud mitigating technologies to help further secure their transactions.

Here are examples of **other products and services** which your organization could consider exploring:

- Discuss with your issuer and their associated networks/brands what measures they are taking "behind the scenes" to increase card not present security.
- Ask if your issuer intends to offer tokenization for corporate cards in the near future. Card-related payment systems which use tokenization include: Apple Pay, Google Wallet and Samsung Pay (formerly Loop Pay). These systems provide a higher level of security and can generally be used for both card present and card not present transactions, but note that as of this writing these services are generally not yet available for commercial charge card accounts. Note that these systems require employees to use a smartphone to complete a transaction, which may raise another set of issues regarding employee access to a phone, etc.
- Ask if your issuer offers Single Use Accounts (SUAs). SUAs are an electronic cardless solution that is currently available from certain issuers which can be used to enhance the security of card not present transactions. SUAs can be customized for large ticket transactions, payments to vendors not traditionally accepting cards, one-time supplier payments or recurring transactions with a single vendor. They can offer a cost effective alternative for streamlining payment processes and earning refunds:
    - 100% electronic payments help payees meet sustainability goals and eliminate manual payment processing;
    - Seamlessly integrates with existing Accounts Payable (AP) or Enterprise Resources Planning (ERP) systems;

- Increased security in that a unique, 16-digit virtual account number is generated for each payment
- Transactions are payment-specific:
    - Only active for a defined time period (e.g., 5 or 50 days)
    - Credit limit equals the exact payment amount due
    - Only authorized for specific merchant category codes

Often improves reporting and reconciliation when compared to other payment methods

Other examples of and ideas for alternative payment solutions that your organization could consider exploring can be found in the GSA SmartPay Payment Solutions Brochure located on our website.