STATE OF NEW MEXICO
PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS
GENERAL GUIDANCE DOCUMENT

The Payment Card Industry – Data Security Standards (PCI-DSS) Compliance Project is half-way through its scheduled work activities and a number of recurring themes have emerged. The PCI-DSS Steering Team would like to share some of the insights identified by RiskSense, the State's PCI-DSS contract partner, during their Gap Assessment process and more importantly highlight the actions you must take to minimize your PCI-DSS profile. It is the Steering Teams desire, that Agencies pursue the best practices describe below and the work on closing the gaps identified during the initial assessment phase of the project by year-end.

Whether highlighted in published articles or articulated by our consultants, the most cost effective strategy to meet PCI-DSS standards and to lower the cost of future compliance is to reduce in-scope payment card activities. Presented below are a few of the steps agencies should pursue to reach a compliant state faster and to drive the state toward more standardized card acceptance processes.

KEY INSIGHT - If your business process allows, keep cardholder data off the network!

SUGGESTED BEST PRACTICES:

E-mail DON'T. To prevent the state's e-mail servers from being pulled into scope for PCI DSS compliance, Agencies shall not request or accept credit card data via e-mail.

PCI DSS Requirement 4.2 states, "Never send unprotected PANs (primary account number) by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.)." The reason for this is, e-mail leaves trails of credit card numbers in inboxes, trashes, web browser caches, etc. and as with any end-user technology, it's extremely difficult to secure. Therefore don't use e-mail.

E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Therefore, do not utilize these messaging tools to send primary account numbers, find another way to transfer sensitive credit card data.

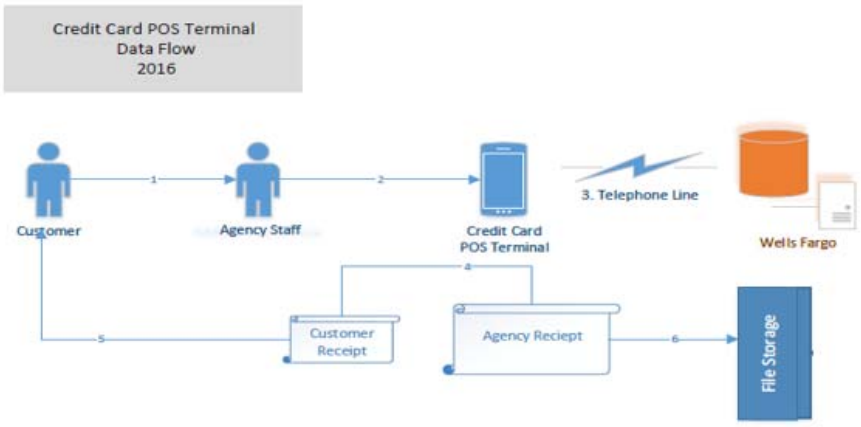
If you receive customer credit card numbers via e-mail by accident then

- Inform the sender to stop and educate them about the dangers of using e-mail to send credit card information.
- Make sure you don't respond by including the original e-mail.
- Delete the e-mail right away, this includes deleting it from the inbox, the deleted items file and the deleted items server. Can end users delete items from the deleted items server, or do they need to request technical assistance?

POINT OF SALE – Devices, Communication Network and Processes

Card present

- Transition to a standardized and approved commercial POS (point of sale) device that supports Point to Point Encryption (P2PE). This can be done by purchasing or renting the devices
    - Wells Fargo Merchant Services can assist – our preferred machine is a First Data chip reader enabled device. This will enable future creation of standardized anti-tampering process document.
- The preferred means of connecting the POS Device to the merchant service provider processing center is via a dedicated phone line
    - It is imperative that you do not bring cardholder data into the network which will necessitate network segmentation or total network compliance both costly endeavors.
    - Alternatively, POS devices may be connected wirelessly through a dedicated and separate (single activity) IPS connection
- Have your customers maintain control over card by letting them swipe or feed the card into the reader
    - If agency employees must handle make sure customer can witness the entire card transaction and not lose sight of their card.



1. Customer hands Agency employee their credit card to complete the purchase.
2. Agency employee has customer swipe card or scans the card into the POS Terminal.
3. The credit card POS Terminal dials Wells Fargo to process the card via a telephone connection and returns approval or reason for non-approval.
4. Upon approval, two receipts are printed showing only the last four digits of the credit card number.
5. The signed receipt is stored in a file cabinet with other sales with other sales documentation.

Card not present

- Same POS set-up
- Operator directly transcribes data into card reader
    - Card data is not to be captured anywhere else
        - Phone calls should not be recorded; do not use Interactive Voice Response (IVR) technology
- If you must take card number over the phone and store it until you have access to a POS devise
    - Capture it on paper, enter it into the POS device and cross-cut shred the document immediately. This process should always be completed in its entirety prior to the close of each business day.
    - Never type card data it into a computer connected to the network or onto any other electronic device.

Mobile Devices

- Use a commercially available mobile POS devices using cellular technology and that applies Point to Point Encryption (P2PE).
    - Wells Fargo Merchant Services can assist. These devises may be obtained from Wells Fargo on a temporary basis to meet short-term event needs or acquired for long-term operating activities
- We are currently working with Wells Fargo and VISA to obtain direction on the use of POS devices tied into cell phone, I-Pads and other multi use machines. These devices go by the name Clover and Square. Depending on the results of the review these devices may be deemed acceptable, however global POS handling documentation will be tailored to the First Data card reader.

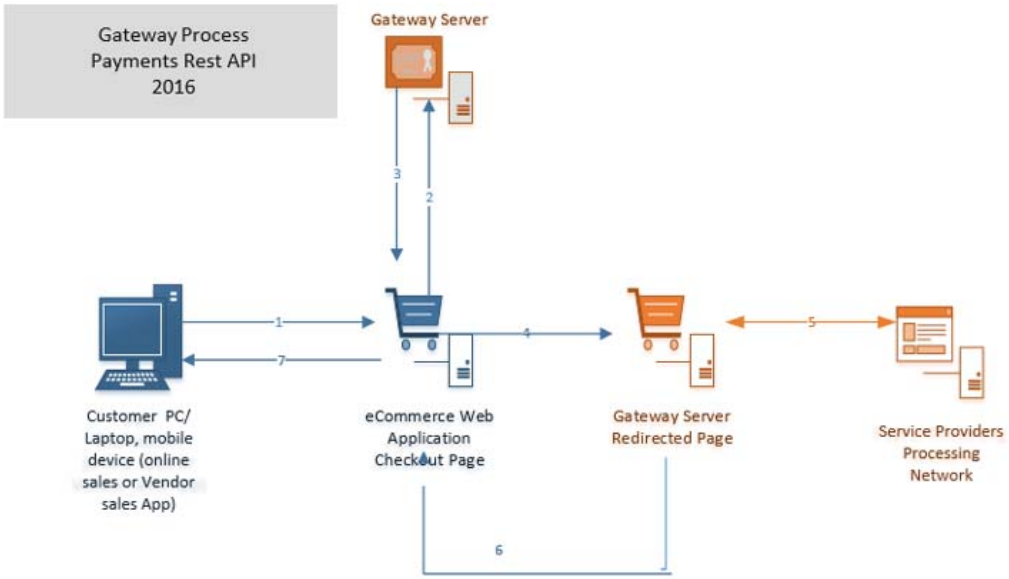
KIOSK

- To prevent your network from coming into scope, the Kiosk should be connected to the processing network using a dedicated phone line.
    - A wireless connection through a separate / independent network is an acceptable alternative
- Kiosk functionality should be limited to the specific purpose of card payment. This can be achieved via configuration and available software.

e-COMMERCE

For e-commerce the preferred payment processing method is using “redirect” technology. Redirects are when the e-Commerce site sends their customer to the payment processor’s site for the processing of the payment.

The payment window/frame/page does not belong to the e-Commerce site and the redirect method is driven by code developed, managed and maintained by the processor, not the e-Commerce organization. In the case of a new window or page, it is the processor’s responsibility to ensure the windows/page is PCI compliant and protects cardholder information.



1. Customer/Vendor Clicks buy via Credit Card on Agency website
2. A request for a secure token is sent via a token ID to the Service Provider Gateway Server
3. The Gateway Server returns a secure token and token ID
4. The web application redirects the customer to an Agency page hosted on the Gateway server via the secure token and token ID. Using the secure token, the Gateway Server retrieves the transaction amount and other transaction data. The customer enters their credit card number, expiration date, CVV on the redirected page.
5. The Gateway Server connects to the Service provider's processing Network and processes the transaction. The Processing Network returns a successful completion or any errors to be corrected by the customer.
6. The Gateway server returns PNRef, last four digits of the credit card, and any other information.
7. The customer receives confirmation of their completed transaction.

If you initiate these steps now, you should be well positioned to show significant improvement in your agency's state of PCI-DSS readiness and more importantly be able to reach full compliance sooner.

Future communications will provide among other topics, tips on contracting terms that should be written into future agreements to ensure your business partner is aware of their responsibility and so the state may have reasonable assurance that our customer's data is protected. If document on contract clauses is released at the same time, this paragraph can be eliminated.

Finally, if your agency feels that the effort required to comply with PCI-DSS outweighs the benefit of acceptance, discontinuing acceptance of payment cards is a viable option to become compliant.