Customer Service Center Operations Manual

CSC Payment Card Industry (PCI) Data Security Standards (DSS) Responsibilities-Safeguard the Card CSCOM-001

Original Date: 08/25/2015
Revision Date: 04/25/2016

DEFINITIONS

Payment Card Industry Data Security Standards (PCI DSS) - A widely accepted set of policies and procedures developed by Visa, MasterCard, Discover, and American Express credit card companies to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

VeriFone MX925 Card Swipe Terminal – New card swipe point of sale (POS) terminal used in Customer Service Centers, and other work areas in DMV to help ensure customer payment card security. The terminal has smart card reader capabilities that allow for processing all magnetic-stripe cards, including credit, debit, and other payment card types. The terminal also has touch screen and signature capture capabilities with a hooded keypad for greater customer privacy.

Return to top of page

DESCRIPTION

The Payment Card Industry (PCI) Data Security Standards (DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and payment card transactions, and protect cardholders against misuse of their personal information.

PCI DSS standards are administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

DMV is required to comply with all PCI DSS standards when handling and processing major credit, debit, and payment cards. Consequences of non-compliance include fines, fees, lawsuits if breached, and possible loss of privilege to accept credit/debit cards from customers.

Protecting customer payment card data is a DMV core responsibility. DMV staff, regardless of work location, is responsible for ensuring the security and proper handling of all customer data, including payment card information received by DMV, regardless of if payment cards are processed by their work area or not.

Payment card data to be protected includes all printed information on the payment card as well as authentication data contained in the card’s magnetic stripe or chip.

- Customer name and address
- Payment card account numbers
- Security verification codes
- Expiration dates

<<<<<REVISION
Customer Service Center (CSC) management and staff, as identified in CSCOM-000.1, are responsible to protect any form of payment card information (debit, credit, or other payment card type) used in any CSC, whether stored, collected or transmitted by, or on behalf of DMV in accordance with PCI DSS standards and DMV’s Safeguard the Card policies (refer to the Financial Management Services (FMS) Customer Payment Policy). **END REVISION>>>>>**

DMV has changed how it handles sensitive payment card data:

- Payment card data is processed and stored by Elavon, a third-party processor, instead of on a DMV server.
- Payment card data cannot be accepted via mail, email, fax, or voicemail.

  NOTE: Specified areas in DMV still accept payment card information online, by unrecorded phone in certain work centers, and via fax only in designated Headquarters work centers.

- OnBase encryption and redaction capabilities are updated to ensure the security of incoming data, data storage and data retrieval.

For more information, refer to DMV's Safeguard the Card: Payment Card Security at DMV.

Return to top of page

SAFEGUARD THE CARD-PCI DSS RESPONSIBILITIES

CSR Safeguard the Card Responsibilities:

<<<<<REVISION

All CSC employees, as identified in CSCOM-000.1, who receive, or come into contact with, payment card information (credit, debit, and other payment card types) in any format, whether digital or non-digital (including but not limited to paper, portable drives, stored recordings, document imaging, microfiche/film, audio/video or any other media that may hold data) is responsible to protect that information at all times. **END REVISION>>>>>**

DMV policy requires that CSC staff:

- **DO NOT** write payment card information such as the primary account number, expiration dates, or verification codes for debit, credit and/or other payment card types in any way on Post-it notes, DMV forms, publications, or other transaction or non-transaction documents when customers request to pay using a payment card.
- **DO NOT** provide payment card information, verbally over the phone or otherwise anywhere it could be overheard, to anyone unless it is in accordance with DMV Safeguard the Card policy and is approved by the CSC manager and that the person receiving the information has a need to know the information in order to process, or assist in processing the transaction for the customer.
- **DO NOT** key payment card information into any location on the computer (i.e., email, a Word document, etc.) except those areas in mySelect specifically intended for the collection of payment card information.
- **DO NOT** share payment card information with anyone in any way (electronic, verbal, or written) unless it is authorized by the Safeguard the Card policy and procedures for your work area and when it is necessary to allow for the processing of the transaction.

Return to top of page

CSC HANDLING OF PAYMENT CARD INFORMATION SUBMITTED USING IMPROPER CHANNELS

CSCs do NOT accept payment card (debit, credit, and other payment card) information sent through the **mail**, **by email**, **fax**, or **voice mail**. In the rare event a customer provides payment card information to a CSC through a non-secure path (improper channel), the CSC will contact the Customer Service Management Administration (CSMA) at Headquarters (HQ) to provide the customer information and receive instructions for handling the transaction.

CSMA HQ will maintain, update, and review an improper channel log of all customers who have submitted payment at a CSC through improper channels and the actions taken in order to:

- Safeguard the customers' payment card,
- Determine customer repeat violations,
- Track actions taken and customer follow-up.

Whenever payment is received by debit card, credit card, or other payment card via mail, email, fax, or voice mail, CSCs must follow the procedure below:

a. Notify the CSC manager that payment was submitted through a non-secure path.
b. The CSC manager or designee contacts CSMA HQ that payment card information has been received from a customer using improper channels and provides:
    - Customer name,
    - Customer number,
    - Email address or fax number (if applicable), and
    - Mailing address

   NOTE: DO NOT forward any payment card information.

c. CSMA HQ will:
    1. Update the customer information to the improper channel log for tracking,
    2. Research and determine if the customer has submitted payment card information via improper channels in the past (repeat offender),
    3. Notify the CSC to:
        - ○ Process the transaction,
          OR
        - ○ NOT process the transaction.

4. Instruct the CSC how to properly dispose of improperly submitted payment card information, to include, but not limited to the following steps:
    - Shred any mailed documents not required to be scanned into OnBase that display credit, debit or other payment card information.
    - Redact any credit, debit, or other payment card information on documents prior to scanning into OnBase
    - Delete any emails in which payment card information was improperly recorded immediately by emptying the "deleted items" recycle bin as follows:
        i. Right click on the "Deleted Items" folder in Outlook,
        ii. Select "Empty Deleted Items folder", and
        iii. Click "Yes".
    - Delete any voice mails with payment card information.
5. Send a follow-up letter to the customers advising of DMV's secure payment card policy.

IMPORTANT: It is essential that all CSCs adhere to the process above for credit card, debit card or other payment card payment information received improperly by mail, email, fax, or voice mail to ensure the integrity of the improper channel log maintained, updated, and reviewed by CSMA for tracking of repeat offenders and customer follow-up in compliance with PCI standards.

Return to top of page

CSC RESPONSIBILITY- ELECTRONIC DATA STORAGE – REDACTION IN ONBASE

Although DMV does not accept payment card information recorded on paper, documents, or in any other form, there may be rare instances when a document stored in OnBase will display debit/credit card information.

IN EVERY CASE, when a document in OnBase displays sensitive payment card information and must be printed for review, the document MUST be redacted in OnBase **before being printed**, in accordance with guidelines in the Redacting a Document (ONB-135).

OnBase will not overwrite the existing document with the redaction after being printed UNLESS you save it as a separate redacted document.

Return to top of page

POINTS TO REMEMBER

- CSCs accept payment by debit card, credit card or other payment cards **in-person only** for DMV products and services.
- CSCs notify CSMA HQ for guidance any time debit or credit card payment is received by mail, email, fax, or voice mail.
    - When authorized, payment information taken by phone must be keyed directly to the payment screen and not written in any way on Post-it notes, DMV forms, publications, or other transaction or non-transaction documents.

Return to top of page

REFERENCES

- OnBase Documents with Payment Card information
- ONB-135 - Redacting a Document in OnBase
- Safeguard the Card
- Payment Card Security EZ Guide

Return to top of page