Credit Card Processing Overview

Megan De Freitas - 2024-12-02 - Miscellaneous

Important Notice

After October 29, 2019, SalesPad will no longer be supporting CardControl. Additionally, the application will cease to be a PA-DSS validated solution as of this date, and therefore CardControl customers would no longer be PCI compliant.

Instead, SalesPad Desktop now offers built-in credit card processing via Nodus PayFabric. If you have questions or want more information on our credit card processing services, please contact your sales rep.

Overview

Credit card processing is a very complex and important system for anyone that sells goods. This guide will hopefully help educate and inform new and old merchants that are working towards being more secure with the use of credit card information, ultimately leading to PCI-DSS compliance.

Definitions

In most places CardControl and SalesPad use the terms Processor and Gateway interchangeably. They are distinctly different entities. These are some definitions to better understand the process a transaction goes through to capture funds.

Card Issuer

Bank that issued the card. Could be the customer's bank, (ex. Bank of America) or one of the payment brands.

Card Not Present

When a credit card is processed without the card stripe information being sent to the Processor or Gateway. A swipe can still be used for card entry. This is typical for online or transactions processed over the phone.

Card Present

When a credit card is processed via a credit card swipe in the United States or a Chip and Pin transaction in other parts of the world. The track data from the mag strip is sent to the processor or gateway.

Card Security Code

An embossed number typically shown on the back of a credit card. This code is used to verify the physical presence of a credit card at the time a transaction is processed.

The different payment brands have different names for this code, such as the following:

- MasterCard - Card Validation Code (CVC2)
- Visa - Card Verification Value (CVV2)
- Discover - Card Identification Number (CID)
- American Express (Amex) - Unique Card Code (CID)

Chip and Pin

Also known as EuroPay, MasterCard, Visa (EMV) cards, or smart cards. Cards that contain integrated circuits. The word chip refers to a computer chip embedded in the smartcard; the acronym PIN refers to a personal identification number that must be supplied by the customer. Chip and PIN is also used in a generic sense to mean any EMV smart card technology which relies on an embedded chip and a PIN. Chip and Pin is not commonly used in the United States.

CardControl does not support Chip and Pin.

Credit Card Number

Also known as the Primary Account Number (PAN), The 13, 15, or 16 digit number representing the credit card account.

Data Security Standard (DSS)

Also known as PCI-DSS, Security requirements for any merchant that chooses to process credit cards. There are several different versions of the DSS standard. CardControl is validated under DSS 2.0, DSS 1.2 is retired and DSS 3.0 is set to go into general use mid-2014.

Gateways

Application Programming Interfaces (APIs) for connecting to processors. These companies add various services on top of the processors that they connect with such as tokenization.

Level 1, 2, & 3 Data

There are differing levels of data that can be sent to a payment processor / gateway. What each level constitutes is different for each setup.

The general guidelines are:

- Card info only – the bare minimum information needed to charge a credit card
- Card info + Order Info – Level 1 plus including information about the order such as order number, shipping and billing address information, etc.
- Card Info + Order Info + Order Detail – Level 2 plus including Line item details, Tax, duty, commodity codes, etc. Level 3 is required for US federal government transactions.

Merchant

The company taking payment via a credit card. CardControl is the merchant’s interface to the credit card processing world.

Payment Application DSS (PA-DSS)

Security validation that states that an application can help a merchant achieve PCI-DSS compliance. An application must be validated before being certified as PA-DSS Validated.

Payment Brand

Major Credit Card companies, Such as Visa, Discover, MasterCard, etc.

Payment Card Industry (PCI)

Trade group for credit card payment brands.

Point of Sale (POS) Terminal

A hardware device that will take a credit card swipe or chip and pin entry.

Processors

Also called acquirers, these are the companies that actually contact the Card Issuer / Payment Brand to get funds for a transaction.

Tokenization

A way of storing a credit card number for later use. Instead of storing the card information in the merchant's database. The card is stored at the Gateway or Processor level.

Difference between PCI Compliance and PA-DSS Validation

PA-DSS v2.0 is the standard against which CardControl has been tested, assessed, and validated. PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining PCI Compliance is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that CardControl will help you achieve and maintain PCI Compliance with respect to how CardControl handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment, which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed, or transmitted.

The 12 Requirements of the PCI DSS: Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

1. Use and regularly update anti-virus software
2. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

1. Restrict access to data by business need-to-know
2. Assign a unique ID to each person with computer access
3. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

1. Track and monitor all access to network resources and cardholder data
2. Regularly test security systems and processes

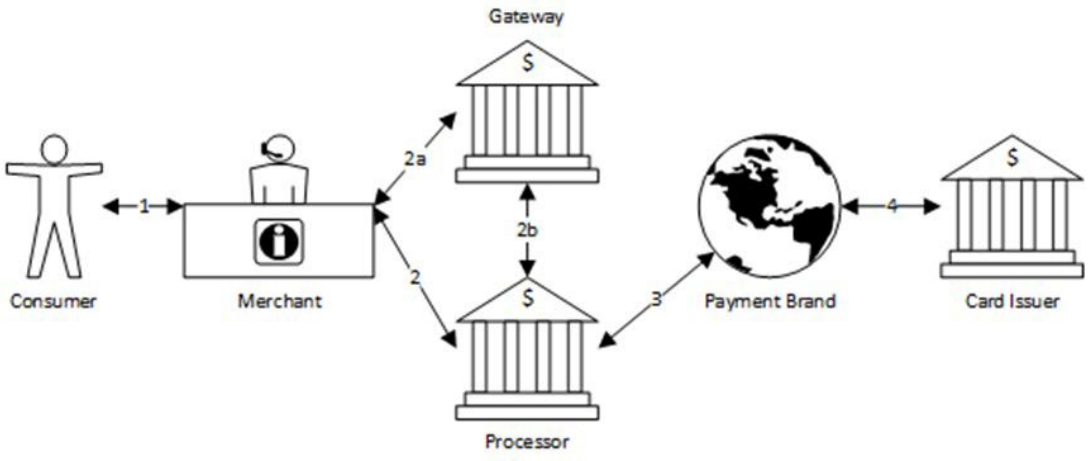
Maintain an Information Security Policy

1. Maintain a policy that addresses information security

The Payment Process

The payment process is the most complex process of taking payments. Understanding of this process can allow merchants to save money once their setup is optimized.

Process Diagram



1. The consumer chooses the credit card they would like to use to pay for their order.
    1. This process may involve swiping their card at a POS terminal, typing their card information into a web application, or reading the card information to a Customer Service Rep over the phone.
    2. At this point the sensitive information PAN, Expiration date, card security code, etc. are sent
2. The Merchant sends the sensitive credit card information to their Processor or

Gateway to process the transaction
    1. If the merchant is using a gateway then the data is sent to the gateway.
    2. The gateway sends the data to the processor the merchant has configured in the account with the gateway.
3. The processor contacts the Payment brand based on the type of card provided.
4. The payment brand contacts the issuing bank to determine if there is enough balance available to process the transaction.
    1. If the issuing bank approves the transaction, that approval is sent back along the chain back to the merchant.

Notes

- While a transaction has been approved the money does not instantly transfer from the Consumer's bank account to the merchant's.
    - The processor, gateway, and issuing bank must all run settlement before the money can be transferred.
    - For this reason, it may take a day or two for money to show up in the merchant's accounts.
- Each step in this process requires resources. Each step also increases the percentage of the payment the merchant pays to process the transaction.
- If a merchant can reduce the number of steps then their rate will be lower. (I.e. it is better to go directly to a processor than use a gateway, the tradeoff is that is extremely difficult to integrate with a processor.)
- The more information that is sent & supported by a gateway or processor the more secure a transaction will be considered. When more information is sent rates are typically lower. See Level 1, 2, & 3 data.

Useful Links

Find Applications and Companies that are PA-DSS Validated

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Payment Applications Data Security Standard (PA-DSS)

https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Payment Card Industry Data Security Standard (PCI DSS)

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Open Web Application Security Project (OWASP)

http://www.owasp.org