Table of Contents

1. Purpose

This document presents payment card retention and disposal method information.

2. Prohibition

Sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization can never be stored, even if encrypted.

3. Scope

Cardholder data refers to any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side. The front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization.

4. Procedure

4.1. Data Storage Systems

All data, except the operating system, will be stored on a networked accessible storage device such as a Storage Area Network (SAN) or a Network Attached Storage (NAS) device using a minimum RAID5 configuration. The data will be backed up or restored following the procedures in the IT Continuality, Backup and Disaster Mitigation-Recovery Plan.

4.2. Digital Cardholder Data

For ecommerce transactions, cardholder data will be entered (manually or via a magnetic strip reader), displayed, and processed in order to conduct a transaction with PayPal. Post transaction, the only cardholder data to be stored is the expiration date and the PnRef (a reference transaction variable from PayFlow) with the person's account information. The cardholder data is needed for refunding transactions.

For Point of Sales (POS) terminals, cardholder data is entered via swiping the card's magnetic strip or using the EuroPay, Visa, MasterCard (EVM) chip. No cardholder data is stored on the POS terminal nor sent to a department system.

4.3. Paper Cardholder Data

Paper containing cardholder data should only contain either Payment Account Number (PAN) masked except the last four digits or just the last four digits, expiration date, and the authorization number. Once the document containing this information is no longer needed for legal, contractual, or business needs and has met the retention period, it should be destroyed via a cross-cut shredder or using a secure shredding service. Paper awaiting destruction must be stored in containers secured with a lock to prevent access to the contents.

4.4. Data Retention

Best practices indicate data should only be retained for the time period it serves a legitimate business purposes. For credit cards, customers have as long as 18 months to dispute charges on their credit card bill. If you do not keep the credit card receipts from sales transactions, your business could be forced to return the money for the purchase to the customer's credit card company. If the credit card company sides with the customer and you do not have the receipt to validate the purchase, the company can debit your merchant account for a chargeback. This would suggest credit card data should be destroyed after 18 months. However, agencies should also consult their Records Retention and Federal and State data retention policies.