Merchant Intelligence™

Important Matters That Affect Your Card Processing Activity

WELLS FARGO

Fall, 2008

Protecting Cardholder Information

How to Keep Your Business Compliant with New Regulations

In the past 10 years, the value of purchases made on credit and debit cards worldwide has more than quadrupled. It is now estimated to exceed $5 trillion annually and that over 40% of this global spending is generated by American consumers[1]. As card payments have grown mainstream, thieves have continued to develop new and more sophisticated methods to steal payment card data from merchants. Protecting consumers' information and Cardholder data has therefore become an important concern.

To help keep Cardholder data secure and prevent identity theft, certain data security standards and regulations have been established and apply to all businesses that store, process, or transmit cardholder data. Wells Fargo Merchant Services knows that understanding and keeping up with new regulations can be complex and time-consuming for your business. This issue of *Merchant Intelligence* is an easy to read guide designed to help your business in its effort and obligation to protect Cardholder data and maintain its compliance with the Payment Card Industry Data Security Standard (PCI DSS), Card Associations' rules and applicable federal and state laws.

[1] Ronald J. Mann, "Prime Numbers: The Plastic Revolution", Foreign Policy, March/April 2008

Data security standards and regulations apply to all businesses that store, process, or transmit cardholder data.

Topics:

PCI DSS – 12 Fundamental Requirements to Protect Cardholder Data:

Objective 1: Build and Maintain a Secure Network

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

Objective 2: Protect Cardholder Data

- **Requirement 3:** Protect stored cardholder data
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Objective 3: Maintain a Vulnerability Management Program

- **Requirement 5:** Use and regularly update anti-virus software
- **Requirement 6:** Develop and maintain secure systems and applications

Objective 4: Implement Strong Access Control Measures

- **Requirement 7:** Restrict access to cardholder data by business need-to-know
- **Requirement 8:** Assign a unique ID to each person with computer access
- **Requirement 9:** Restrict physical access to cardholder data

Objective 5: Regularly Monitor and Test Networks

- **Requirement 10:** Track and monitor all access to network resources and cardholder data
- **Requirement 11:** Regularly test security systems and processes

Objective 6: Maintain an Information Security Policy

- **Requirement 12:** Maintain a policy that addresses information security

For more information or to view the detailed specifications of each requirement, please visit:
www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Rules and Regulations Protecting Cardholder Information

PCI Data Security Standard (PCI DSS)

The PCI Data Security Standard was developed by the Card Associations (Visa®, MasterCard®, Discover® Network, American Express and JCB) to help protect Cardholder information. It sets comprehensive requirements to assist businesses in securing their information network, as well as in establishing and maintaining procedures and policies to prevent threats and unauthorized access to their systems and applications.

The PCI DSS is managed by the PCI Security Standards Council, an independent committee founded in 2006 by the five major Card Associations. Its role is to develop and promote security standards to protect customer account information. However, the enforcement of the PCI DSS is led by the Card Associations (Visa, MasterCard and Discover Network) through Merchant Card Processors, like Wells Fargo Merchant Services.

Payment Application Data Security Standards (PA-DSS)

In 2004, Visa introduced the Payment Application Best Practices (PABP) program to help software vendors create secure payment applications that do not store sensitive data (such as full magnetic stripe, CVV, CVV2 or PIN data) and support compliance with the PCI DSS.

In April 2008, the PABP became an official global standard under the umbrella of the PCI Security Standards Council and were

(continued on inside)

Rules and Regulations Protecting Cardholder Information *(continued)*

renamed the Payment Application Data Security Standards (PA-DSS). To ensure that businesses do not use payment applications that are known to be vulnerable to security breaches, Visa has established a series of compliance mandates. Effective October 1, 2008, new merchants will not be able to use payment applications that are not compliant with the PA-DSS.

Merchants currently using payment applications that have not been validated to comply with the PA-DSS will need to upgrade their application by July 1, 2010. If you have purchased and are using a payment application developed by a third party vendor or software company, you should ensure that it has been validated with the PA-DSS. To view an updated list of compliant Payment Applications, please visit: http://usa.visa.com/download/merchants/validated_payment_applications.pdf

If you are using a payment application, you should ensure that it complies with the Payment Application Data Security Standards.

PIN Entry Device (PED) Security Requirements

PIN Entry Devices (PEDs) have often been hacked by criminals trying to gain access to card account data and PINs. Common attacks have included criminals posing as "service technicians" visiting merchants at their location and inserting a tapping device or tampering with the PED. Any merchant may be affected by this scheme, especially if the PED is not physically secured or if the merchant has an older PED on which it is hard to identify if tampering has occurred.

Also managed by the PCI Security Standards Council and enforced by the Card Associations through Merchant Card Processors, the PIN Entry Device Security Requirements set comprehensive specifications to ensure that PIN devices securely process and transmit PIN data. If your business processes PIN-based transactions, please ensure that your PED is compliant. To view an updated list of approved PEDs, please visit: http://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html

If your business processes PIN-based transactions, you must ensure that your PIN Entry Device is compliant.

Truncating Cardholder Information on Card Receipts

Federal and State Regulations

To protect Cardholder information and reduce identity theft, Federal law and certain State laws mandate that merchants truncate the account information on receipts provided to Cardholders. Under the Fair and Accurate Credit Transactions Act of 2003, merchants are prohibited from printing more than the last 5 digits of the Card account number and from printing the expiration date on any receipts "provided to the Cardholder at the point of sale or transaction". A few states also require merchants to truncate the copy that they retain for their records. Often referred to as "double truncation", this law has been in effect in Tennessee since January 1, 2007, and will take effect in California and Colorado on January 1, 2009 and in Alaska on July 1, 2009. Other states are in the process of evaluating bills mandating "double truncation". To find out about the most recent legislation in your state, please visit your state legislature's website or contact an attorney.

If your business also uses any type of POS application software from a Value Added Reseller (VAR) vendor, such as Aloha, Counterpoint, Monetra, or Squirrel, they are responsible for servicing your POS system and for configuring your software to the new industry standards. Contact your VAR directly to find out what updates are available for your system.

To verify whether your Point of Sale (POS) equipment is compliant, please contact Wells Fargo Merchant Services at 1-800-451-5817, 24 hours a day, 7 days a week.

Retrieving Cardholder data in states requiring double truncation

If you are doing business in a State which requires you to truncate your own merchant receipts, you may wonder how you will be able to retrieve Cardholder data and manage card disputes. The card associations no longer require a full account number to resolve a chargeback. You can use the transaction ID shown on receipts. You can also use our online reporting tool, *ClientLine*® to research Cardholder data and transaction information safely and easily, 24 hours a day, 7 days a week. Find out more at www.wellsfargo.com/biz/clientline or logon on to www.myclientline.net. *ClientLine* has no monthly fees and no set up fees.

Federal law mandates that merchants truncate account information on receipts provided to Cardholders. Tennessee extended this requirement to receipts kept by merchants in January 2007. California and Colorado will also require "double truncation" as of January 1, 2009 and Alaska, as of July 1, 2009.

Card Associations Rules

Today, Visa and MasterCard's rules are even more restrictive than Federal regulations as they prohibit merchants from printing more than the last 4 digits of the Card account number and from printing the expiration date on receipts provided to Cardholders. This requirement does not apply however to transactions in which the sole means of recording a customer's credit or debit card account number is by handwriting, imprinting or copying the Card.

Effective January 1, 2010, MasterCard will add a new requirement to merchants, mandating that they also truncate the expiration date on the payment card receipts they retain for their records. MasterCard also strongly recommends truncating the payment card number on the merchant copy. Receipts should only display the last four (4) digits of the payment card number and replace all preceding digits with non-numeric characters, such as "X", or "*", such as:

CARD NUMBER: **********1234**
EXP: **/**

If your POS terminal is not truncating the cardholder's information, please call our POS Help Desk at 1-800-622-0842.

Visa and MasterCard mandate that merchants truncate all but the last 4 digits of the Card account number and the expiration date on receipts provided to Cardholders. As of January 1, 2010, MasterCard will require merchants to also truncate the expiration date on the receipts they retain for their records.

The Benefits of Being Compliant

Not only is it mandatory for businesses to adhere to federal and state laws relating to the protection of Cardholder information and to remain compliant with the PCI Standards, it is also good business practice. Protecting your business from a data security breach is essential to protect your customers' personal data, their confidence in your business and brand, and your revenues. A study conducted by Javelin Strategy and Research in April 2007 revealed that "85% of consumers would be likely to increase their shopping at a store if they knew it was a leader in protecting (their) account information. 78% of consumers also said they would be unlikely to continue to shop at a retailer that had suffered a security breach in which account information may have been compromised"[2].

Unlike popular belief, 70% of compromises occurred at brick and mortar merchant locations and 92% affected smaller businesses.

Consequences and Penalties for Non-Compliance

Often businesses are unaware of the consequences of an account data security breach. It is also often wrongly assumed that only large retailers and Internet merchants are prone to a data compromise. In March 2008, Trustwave compiled statistics from more than 400 cardholder data compromise investigations performed in over 20 different countries. Its results showed that, unlike popular belief, 70% of compromises occurred at brick and mortar merchant locations and that 92% affected smaller businesses[3].

The consequences and costs of non-compliance and of a data compromise can be devastating for any merchant. While businesses who are not PCI DSS compliant risk losing their ability to process card payments, they are also very likely to lose customer confidence and revenues in case of a compromise and will potentially face fines, penalties and expenses to repair the damages done.

In situations of non-compliance with federal account truncation laws, merchants can be liable for actual damages suffered by Cardholders and attorneys' fees. In cases of willful non-compliance, Cardholders may even be able to recover statutory damages in the amount of $100 to $1000 for each act of willful non-compliance. Several U.S. states have passed account truncation legislation which can expose merchants to financial and criminal penalties. Finally, the Card Associations may also impose considerable fines for non-compliance which range from $5,000 per violation to $500,000 a month for willful and flagrant violations.

According to a study conducted by Forrester Research, costs associated with a data security breach can range from $90 to over $300 per lost credit Card record. In one high profile security breach where more than 45 million payment Card numbers may have been stolen, reports estimate that the victimized retailer could pay between $100[4] to over $180[5] per lost record (an estimated $4.5 to $8 billion loss).

[2] Javelin Strategy and Research, Retailers & Card Data Security, April 3, 2007

[3] Trustwave, Trustwave Global Compromise Statistics, Quarterly Report, March 2008

[4] Source: IPLocks study, as reported in Information Week on 05/02/07

[5] Source: Ponemon Institute LLC study, as reported in Information Week on 05/02/07

Validating Your PCI Compliance

All businesses that store, process, or transmit cardholder data must validate that they comply with the PCI DSS. The volume of transactions annually processed by a merchant determines its PCI Level and therefore its compliance validation requirements. The table provided below will help you identify your PCI level and validation requirements.

PCI Levels	Visa and MasterCard	American Express	PCI DSS compliance validation requirements
1	• Over 6,000,000 Visa or MasterCard transactions per year • Businesses that experienced a data compromise • Businesses meeting the Level 1 criteria of another payment card brand	• Over 2,500,000 American Express transactions per year • Businesses that experienced a data compromise	• Annual onsite review by a Qualified Security Assessor • Quarterly network security scan by an Approved Scanning Vendor • Annual submission of a compliant "PCI Report On Compliance" • Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only
2	• 1,000,000 to 6,000,000 Visa or MasterCard transactions per year • Businesses meeting the Level 2 criteria of another payment card brand	• 50,000 to 2.5 million American Express transactions per year	• Annual Self assessment questionnaire must be submitted to Wells Fargo Merchant Services • Quarterly network security scan by an Approved Scanning Vendor • Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only • Annual signed "Attestation of Report Accuracy"
3	• 20,000 to 1,000,000 e-commerce Visa or MasterCard transactions per year • Businesses meeting the Level 3 criteria of another payment card brand	• All other businesses	• Annual Self assessment questionnaire must be submitted to Wells Fargo Merchant Services • Quarterly network security scan by an Approved Scanning Vendor • Annual signed "Attestation of Report Accuracy"
4	• All other businesses	• N/A	• Annual Self assessment questionnaire • Quarterly network security scan by an Approved Scanning Vendor strongly recommended

The Self Assessment Questionnaire (SAQ) is a document available for download from the PCI Security Standards Council which helps you self-assess your compliance with the PCI DSS, gain a better understanding of your risk level and may provide you with the steps you will need to take to comply with the PCI DSS. To download the SAQ, please visit: www.pcisecuritystandards.org/saq/index.shtml

A Quarterly Network Security Scan is a non-intrusive test of all your network, hosts and applications, which provides a real-time snapshot of your system to find vulnerabilities and recommend improvements. The report generated helps determine if your business is in compliance with the PCI DSS. A list of Approved Scanning Vendors (ASVs) can be found at www.pcisecuritystandards.org/pdfs/asv_report.html

Annual onsite reviews (for level 1 merchants only) must be performed by a Qualified Security Assessor (QSA), who will assess your organization's compliance with the PA-DSS. A list of QSAs may be downloaded from the PCI website at: www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Level 4 Merchants
Assess Your Data Security Risk with Trustwave's Risk Profiler Tool

As a Wells Fargo Merchant Services customer and to assist you in measuring your risk, we have made arrangements for you to have access to Trustwave's Risk Profiler. It is at **no additional cost to you.**

Trustwave is a Qualified Security Assessor and their online tool, Risk Profiler, uses a brief questionnaire to gather information on your payment card processing environment (such as your POS system, terminal set-up, and/or payment software). It can also perform a vulnerability scan if you require one. Risk Profiler will help you determine whether or not your payment card systems are at an elevated risk for a compromise.

To take advantage of this service, please visit: www.wellsfargo.riskprofiler.net

WELLS FARGO

Information Security Tips and Best Practices

To reduce the threat of a data security breach, the following best practices should be followed:

- ✓ **Never store full-track magnetic- stripe data, PIN block data and CVV2** once a transaction has been authorized. Only the account number, expiration date and Cardholder name can be stored, in accordance with the PCI DSS requirements.
- ✓ **Change the default settings and login credentials** supplied by your vendor when you install a payment application system.
- ✓ **Establish and maintain a data retention and destruction policy.** Only store data necessary to conduct your business and ensure that the stored data is secure. We also recommend moving the retention of data from an online to an offline environment and destroying data after the retention period expires. A common misconception is that if a merchant does not store cardholder data, the PCI DSS do not apply. This is inaccurate as the PCI DSS also apply to the environment that transmits or processes cardholder data. This includes any service providers that a merchant uses. However reducing the amount of data stored will help reduce your exposure if a compromise occurs.
- ✓ **If you are using a third party provider and/or card processing software,** you are required to advise Wells Fargo Merchant Services of any third party that engages in or proposes to engage in, the processing or storing of transaction data on your behalf. Only use third parties that are registered with Wells Fargo Merchant Services and are PCI compliant. Any violation by third parties may result in unnecessary financial exposure and inconvenience to your business, including the assessment of substantial fines and/or penalties.
- ✓ **If you outsource your IT infrastructure or allow remote access,** you should:
  - Allow dual factor authentication
  - Only allow access during scheduled maintenance windows when possible
  - Disable remote access accounts when not in use.
- ✓ **If you use Voice over Internet Protocol (VoIP)** to transmit transactions over the Internet through your terminal, you should ensure that your VoIP solution is secure. You must use a Secure Socket Layer (SSL) IP converter to ensure that the Cardholder data transmission is safe. Currently, Wells Fargo Merchant Services is aware of three solutions that use an SSL IP converter. They are offered by:
  - Precidia Technologies www.precidia.com
  - Systech Corporation www.systech.com
  - TechTrex USA Inc. www.techtrex.com

Protecting Cardholder Data Additional Resources

- ➢ **Wells Fargo Merchant Services:**
  www.wellsfargo.com/biz/merchantsecurity
  or email: WFMSPCICompliance@wellsfargo.com
- ➢ **PCI Security Standards Council:**
  www.pcisecuritystandards.org/
- ➢ **Visa Inc. (USA):**
  www.visa.com/cisp/
- ➢ **MasterCard:**
  www.mastercard.com/sdp/
- ➢ **Discover Network:**
  www.discovernetwork.com/resources/data/data_security.html
- ➢ **American Express:**
  www.americanexpress.com/datasecurity
- ➢ **JCB:**
  www.jcb-global.com/english/jdsp/index.html
- ➢ **Your State Legislature**
- ➢ **Your Attorney**

WF MI 08/08