


**FIFTH THIRD
PROCESSING SOLUTIONS**

**Blueprint for
Cardholder Data Security**

October 14, 2009

Confidential and Proprietary | For Internal Use Only
© Fifth Third Processing Solutions | All Rights Reserved

Blueprint for Cardholder Data Security




How Secure is Your Cardholder Data?

- Building Your Foundation Through PCI DSS Compliance
- Having Protection in the Event of a Card Data Compromise
- Ongoing PCI Compliance, Protection, Education

Confidential and Proprietary | For Internal Use Only
© Fifth Third Processing Solutions | All Rights Reserved

PCI DSS Compliance



**Payment Card Industry Data Security Standard
(PCI DSS)**

PCI DSS is comprised of 12 high level requirements designed to:

- Build and maintain a secure network
- Protect cardholder data
- Ensure maintenance of vulnerability management programs
- Implement strong access control measures
- Regularly monitor and test networks
- Ensure the maintenance of information security policies.

Confidential and Proprietary | For Internal Use Only
© Fifth Third Processing Solutions | All Rights Reserved

PCI DSS Compliance



Payment Card Industry Data Security Standard (PCI DSS)

- The card associations aligned to support these standards
- Applies to ALL organizations, systems, networks and applications that process, store or transmit at least the cardholder number
- Never store any cardholder data other than the cardholder name, number, expiration date and service code
- **All merchants are required to comply**

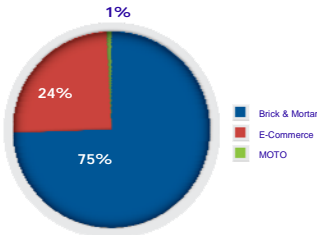


Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

The Reality of Card Data Compromise



Card Data Compromise Statistics



- In contrast to common belief, Card Present merchants are twice as likely to be compromised than Card Not Present merchants.
- As a consumer, you are more likely to have your card stolen making a face-to-face transaction, than when shopping online.

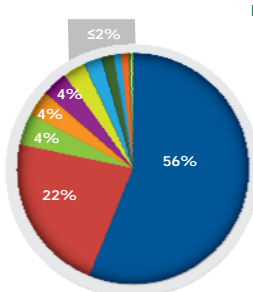
Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

Source: Trustwave

The Reality of Card Data Compromise



Card Data Compromise Statistics



Food Service Industry represents the majority of the compromises (56%).


Retail Industry is the next largest industry seeing compromises (22%).



Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

Source: Trustwave

PCI DSS Compliance – Merchant Levels




- **Merchant Level 1**
 - Any merchant, regardless of acceptance channel, processing 6 million Visa® or MasterCard® transactions per year, or identified by Visa as Level 1, or suffered a hack or attack that resulted in an account data compromise
- **Merchant Level 2**
 - Any merchant, regardless of acceptance channel, processing 1 million to 6 million Visa or MasterCard transactions per year
- **Merchant Level 3**
 - Any merchant processing 20,000 to 1 million e-commerce Visa or MasterCard transactions per year
- **Merchant Level 4**
 - All other merchants regardless of acceptance channel

Level 4 merchants are impacted!!

Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

PCI DSS Compliance – Merchant Validation




Merchant Levels	Validation Actions		
	On Site Assessment	Self – Assessment Questionnaire	Network Vulnerability Scans
Level 1 <small>(see note below)</small>	Report on Compliance (ROC) <small>(Submitted to Acquirer Annually)</small>	Not Applicable	Required Quarterly
Level 2 <small>(see note below)</small>	Report on Compliance (ROC) <small>(Submitted to Acquirer Annually)</small>	Submitted to Acquirer Annually	Required Quarterly
Level 3	Not Applicable	Submitted to Acquirer Annually	Required Quarterly
Level 4	Not Applicable	Best Practice Annually <small>(submission at acquirer's discretion)</small>	Required Quarterly <small>(submission at acquirer's discretion)</small>

Note: By December 31, 2010 and annually thereafter, MasterCard is requiring that both level 1 and 2 merchants undergo an on-site assessment completed by a Qualified Security Assessor (QSA) and submit a ROC from the QSA to their acquirer.

Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

Key PCI DSS Considerations



- Do not store magnetic-stripe data after transaction authorization
- Do not store PIN blocks after transaction authorization
- Do not store the card's validation / security code (CVV2 / CVC2)
- Guard against SQL injection attacks caused by insecure shopping carts (primarily an E-Commerce phenomenon)
- Protect against remote access vulnerabilities
- Never use vendor-supplied defaults

Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

Protection in a Compromise Situation



Breach Assistance Program

- Hackers continue to find ways into the most vital data of companies large and small.
 - In fact, hackers are concentrating more on smaller merchants because that is where they see the greatest vulnerability.
- Our **Breach Assistance Program** helps protect your business from financial losses in **four critical areas** in the case of a suspected or actual data breach at your merchant location(s)*.
- Specifically, our Breach Assistance Program provides indemnification of up to \$50,000 per merchant location and up to \$500,000 per incident**.

* Assistance requires written notification or acknowledgement from the card associations of a suspected or actual data breach.
** Indemnification of costs is provided by Great American E&S Insurance Company, Cincinnati, Ohio and is limited to the terms and conditions set forth in the insurance policy issued to the named insured Fifth Third Processing Solutions

Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

10

Breach Assistance Program – 4 Critical Areas



Forensic Audit Expense

- Cost associated with the mandatory 3rd party forensic investigation required by the card associations for suspected or confirmed breaches.
- General cost range: \$8,000 - \$20,000 for Level 4 merchants (single location).

Card Replacement and Monitoring Costs

- Issuer cost associated with compromised card replacement or account monitoring to watch for potential fraud.
- General cost range: \$3 - \$5 per card replacement.

Association Fines

- Association non-compliance fines that may be assessed depending on the size of the business and circumstances that led to the breach.
- General fine range: \$5,000 to upwards of \$500,000.

Compliance Cases & Account Data Compromise Recovery Costs

- Issuer fraud loss recovery from fraudulent transactions attributable to the breach.
- General cost range: Will vary depending on the size and scale of the breach.

Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved

11

Breach Assistance Program



- Maintaining an ongoing assistance program is critical.
- The Breach Assistance Program provides an enrolled merchant assistance with an eligible breach that is discovered while the merchant is enrolled in the program, regardless of when the breach occurred.


What does this mean??

- If the merchant is enrolled in the program and processing with Fifth Third Processing Solutions, the merchant is covered for eligible expenses even if the breach occurred while they were accepting payments with another merchant processor!

Confidential and Proprietary | For Internal Use Only
Fifth Third Processing Solutions | All Rights Reserved


12

Ongoing Education is Critical!




- This presentation is based upon information available to Fifth Third Processing Solutions as of the date of this communication.
- Its important that you continue to stay current with new PCI DSS requirements by leveraging the following website links:
 - www.ftpsllc.com
 - <http://www.pcisecuritystandards.org>
 - <http://usa.visa.com/cisp>
 - <https://sdp.mastercardintl.com/sdp>
 - www.americanexpress.com/datasecurity
 - www.discovernetwork.com/fraudsecurity/disc.html
- Our dedicated PCI Compliance Team offers a series of monthly webinars on topics related to the PCI DSS.
 - To see a schedule or register for one of the upcoming sessions, visit www.trustwave.com/53webinars.php.

Confidential and Proprietary | For Internal Use Only
© Fifth Third Processing Solutions | All Rights Reserved



Questions?

Confidential and Proprietary | For Internal Use Only
© Fifth Third Processing Solutions | All Rights Reserved



Your Fifth Third Representatives

Vivian Van Keuren
 Covering NACM Midwest – Chicago and Nebraska
 219-902-4911 (phone)
 866-844-3877 (fax)
 Vivian.vankeuren@53.com

&

Matt Fluegge
 Covering NACM Midwest – Wisconsin and Upstate New York
 608-834-2539 (phone)
 608-834-2563 (fax)
 Matt.fluegge@53.com

Confidential and Proprietary | For Internal Use Only
© Fifth Third Processing Solutions | All Rights Reserved
