ICCCFO Conference, Fall 2011

Payment Fraud Mitigation:
Securing Your Future

Presented by:
Brian Irwin, CTP
Vice President Fifth Third Bank
Commercial Treasury Management
And
Claire Dittrich
Executive Consultant- Middle Market
Fifth Third Processing Solutions
Agenda

Check Fraud

ACH Fraud

Your role in preventing fraud

PCI Compliance

Questions
Payment fraud is on the rise:

- According to the FBI, fraud costs consumers, banks, and businesses $18 to $20 billion per year.

- American Bankers Association (ABA) reported a spike in reports of fraudulent checks – federal regulators blamed easier access on the counterfeiting technology.

- AFP Payments Risk Survey, March 2010 Report: 71% of organizations were targets of attempted or actual payments fraud in 2005; up from 68% in 2005 and 55% in 2004!
Type and frequency of payment fraud during 2006:

- 2/3 of organizations were targets of attempted or actual fraud
- Checks were most often the vehicle for fraud; ACH was second
- 75% of the cases of attempted check fraud did not result in a financial loss
- Organizations that were victim of attempted ACH fraud were more likely to suffer a loss
Types of Check Fraud:

- Alterations
- Forged signatures
- Counterfeit
- Third-party bill payment services
- Closed account fraud
- Forged and improper endorsements
Minimize Risks:

• *Positive pay and payee verification* greatly reduce your risk of loss by identifying fraudulent items quickly.

• The risk of loss from check fraud is substantial, therefore the bank and its client must work together in preventing check and payment fraud.
Understanding ACH Fraud:

• Automated Clearing House (ACH) debit fraud risk is the risk that a transaction will be initiated or altered in an attempt to misdirect or misappropriate funds.

• Although ACH fraud risk does occur, the frequency is relatively low when compared to other payment systems, particularly check frauds.

• ACH fraud is relatively simple to perpetrate:
  • ACH is easy to process by banks
  • ACH is a widely accepted transaction
  • ACH offers flexibility for a variety of payment applications
Understanding ACH Fraud:

- Any ACH debit may post to your account if no proactive fraud prevention measures are in place.

- Critical elements of ACH fraud – accounting and routing numbers can be obtained from any given check.

- The number of days after which a client may recover a fraudulent or unauthorized ACH transaction is:
  - 60 days for Internet and telephone initiated transactions (e.g. WEB, TEL)
  - 60 days for converted or truncated check items (e.g. POP, ARC, BOC, RCK)
  - Two days for business-to-business transactions (e.g. CCD, CTX)
Reduce Your Risks of Fraud:

- Convert as many payments as possible to electronic delivery (such as ACH, EDI, wire and card)
- Implement positive pay/payee line positive pay
- Reconcile accounts frequently and regularly
  - Use online reporting and reconcilement services for faster reconcilement
- Place physical controls on check stock
  - Secure storage and access to check stock and signature plates
  - Dual control and usage restrictions
  - Policies on how check stock is ordered and received
- High Security Checks- contain at least 10 safety features
- http://www.safechecks.com/
Clients are responsible for safeguarding their checks.

In some cases, clients may be found negligent if they fail to:

• Maintain sufficient controls for check storage, issuance and reconciliation

• Notify the bank in a timely manner when fraud occurs

• Review bank statements and reconcile accounts in a timely fashion

• For more information, see the Uniform Commercial Code, §3-406 and §4-406
Reduce Your Risks of Fraud:

- **Separate accounts**
  - Collection and disbursement activity
  - Check and electronic payments
  - Payroll and accounts payable disbursements
  - High-volume accounts vs. low-volume (e.g. petty cash)

- **Implement ACH debit blocks or filters**

- **Segregate duties – making payments and reconciling accounts**

- **Limit number of official signors on checks**

- **Update bank records immediately after staffing changes**
Reduce Your Risks of Fraud:

- Form an internal “anti-fraud” committee
- Use prior fraud occurrences to level set
- Match industry “best practices”
- Establish and maintain general controls
  - Document and enforce procedures
- Awareness and training
- Screen new employees and temporary help
- Know who you do business with
  - Vendors (including maintenance staff)
  - Clients
Check Fraud - A National Epidemic

“Punishment for fraud and recovery of stolen funds are so rare, prevention is the only viable course of action.”

- Frank Abagnale

www.Abagnale.com

- 40% of organizations polled by AFP experienced payment fraud loss, majority from check fraud

- Average check fraud loss over $15,000

- In 2009, 71% of organizations polled affirmed victim of payment fraud, up from 55% in 2005
ICCCFO Conference

Payment Card Industry (PCI) Compliance
Learning Objectives

- What is the PCI DSS?
- Who does it apply to?
- Why is it important?
- How does a merchant validate compliance?
- Where do I find more information on PCI?
• The card associations aligned to support these security 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**
Payment data breaches represented 98% of all data breaches in 2009. ¹

More than 280 million payment card records were breached in 2008 alone. ²

The average cost of a data breach is $202 per record and rising, with the average cost of a large scale breach reaching $6.6 million.³

Credit card data remains an extremely valuable commodity.

A significant data breach at one PCI Level 1 retailer has cost over $250 million so far....

1 Trustwave Global Security Report 2010
2 Verizon 2009 Data Breach Investigations Report
3 Ponemon Institute, 2008 Annual Study: Cost of a Data Breach
Compromise Statistics by Industry

- Food & Beverage: 57%
- Retail: 18%
- Hospitality: 10%
- Government: 6%
- Financial: 6%
- Education: 1%
- Construction: 1%

Source: Trustwave 2011 Global Security Report
Data gathered from more than 220 Trustwave breach investigations in 2010
Card present merchants are targeted most!

Source: Trustwave 2011 Global Security Report
Data gathered from more than 220 Trustwave breach investigations in 2010
PCI DSS
Requirements
PCI DSS Requirements 1 through 6

**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 security parameters

**Protect cardholder data**

**Requirement 3**
Protect stored cardholder data

**Requirement 4**
Encrypt transmission of cardholder data and sensitive information across public networks

**Maintain a vulnerability management program**

**Requirement 5**
Use and regularly update anti-virus software

**Requirement 6**
Develop and maintain secure systems and applications
Implement strong access control measures (Requirement 7)
Restrict access to data by business need-to-know

Regularly monitor and test networks (Requirement 10)
Track and monitor all access to network resources and cardholder data

Maintain an information security policy (Requirement 12)
Maintain a policy that addresses information security

Assign a unique ID to each person with computer access (Requirement 8)

Restrict physical access to cardholder data (Requirement 9)

Track and monitor all access to network resources and cardholder data (Requirement 11)

Regularly test security systems and processes

Maintain an information security policy

PCI DSS Requirements 7 through 12
PCI Security Standards Council
PCI Security Standards Council

- Develops industry-wide technical data security standards, including the PCI DSS, Payment Application DSS (PA-DSS), and the PIN Transaction Security (PTS) program
- Manages training, education and the process for certifying Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV)
- Manages the payment application validation process, including the List of Validated Payment Applications
- Provides a forum for stakeholders to provide input into the ongoing development, enhancement and dissemination of data security standards
- Manages the List of PTS Approved Devices
PCI DSS Version 2.0

- Released October 2010, Effective January 1, 2011
- No significant changes to requirements
- Key Objectives for Revisions
  - Provide greater clarity on the PCI DSS requirement
  - Offer improved flexibility
  - Manage any evolving risks and threats
  - Incorporate best practices
  - Clarify scoping and reporting
  - Eliminate redundant sub-requirements
- Merchants can use either version 1.2 or 2.0 for 2011 assessments
- FTPS strongly recommends using the latest version, 2.0.
- Now on a 3 year revision cycle, next new version due out in 2013
Compliance Validation Steps
**Validation:** A snapshot of your compliance status

- Entails completion of the Self-Assessment Questionnaire (SAQ) or an On-Site Audit (depending on your merchant level) in order to “validate” that your organization is compliant according to PCI DSS requirements
- Also requires the quarterly submission of External Network Vulnerability Scans

**Compliance:** Ongoing security controls and procedures that help to protect your business on a 24/7 basis

- Entails continual adherence to the PCI DSS requirements

**Validation** does not necessarily mean **Compliance**

Validation documentation must be available to the card associations upon their request and for audit purposes
# PCI DSS Compliance by Merchant Levels:

<table>
<thead>
<tr>
<th>Merchant Level 1</th>
<th>Level 1 merchants have rigorous validation requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any merchant, regardless of acceptance channel, processing 6M Visa® or MasterCard® transactions/yr or any merchant that the card brands determine should be considered a Level 1 merchant.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Merchant Level 2</th>
<th>Any merchant, regardless of acceptance channel, processing 1 million to 6 million Visa® or MasterCard® transactions per year.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Level 3</td>
<td>Any merchant processing 20,000 to 1 million e-commerce Visa® or MasterCard® transactions per year.</td>
</tr>
<tr>
<td>Merchant Level 4</td>
<td>All other merchants regardless of acceptance channel.</td>
</tr>
</tbody>
</table>

Level 4 merchants are impacted, as well!
Due to MasterCard® Site Data Protection (SDP) program rules, all level 1 and 2 merchants that elect to perform their own validation assessments must ensure that the primary internal auditor staff engaged in validating PCI DSS compliance attend merchant training programs offered by the PCI Security Standards Council (PCI SSC) and pass any PCI SSC associated accreditation program annually in order to continue validation in this manner. The training deadline is June 30, 2012.

### Merchant Levels

<table>
<thead>
<tr>
<th>Level 1*</th>
<th>Level 2*</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Site Assessment</td>
<td>Self – Assessment Questionnaire</td>
<td>Network Vulnerability Scan</td>
<td></td>
</tr>
<tr>
<td>Report on Compliance (ROC)*</td>
<td>Not Applicable</td>
<td>Required Quarterly</td>
<td></td>
</tr>
<tr>
<td>Not Applicable</td>
<td>Submitted to Acquirer Annually</td>
<td>Required Quarterly</td>
<td></td>
</tr>
<tr>
<td>Not Applicable</td>
<td>Submitted to Acquirer Annually</td>
<td>Required Quarterly</td>
<td></td>
</tr>
<tr>
<td>Not Applicable</td>
<td>Best Practice Annually</td>
<td>Required Quarterly</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Due to MasterCard® Site Data Protection (SDP) program rules, all level 1 and 2 merchants that elect to perform their own validation assessments must ensure that the primary internal auditor staff engaged in validating PCI DSS compliance attend merchant training programs offered by the PCI Security Standards Council (PCI SSC) and pass any PCI SSC associated accreditation program annually in order to continue validation in this manner. The training deadline is June 30, 2012.
Service Providers
• Requirement 12.8 – Addresses Third Party compliance within the PCI DSS requirements

• Merchant’s responsibility to monitor compliance status of Third Parties and ensure appropriate contractual language is in place

• Use of Gateway/Service Provider does not exempt merchant from compliance requirements

• Potential to use SAQ A
  – Only IF you fully outsource all storing, processing and transmitting of cardholder data to a third party AND you are exclusively a card-not-present merchant
## Service Provider Validation

<table>
<thead>
<tr>
<th>Service Provider Levels</th>
<th>Validation Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Provider Level Criteria</td>
<td>On Site Security Audit</td>
</tr>
<tr>
<td><strong>Level 1</strong></td>
<td>Report on Compliance (ROC)</td>
</tr>
<tr>
<td>Any processor directly connected to a Visa or MasterCard or any service provider that stores, processes and/or transmits over 300,000 transactions per year</td>
<td>Required Annually</td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Any service provider that stores, processes and/or transmits less than 300,000 transactions per year</td>
<td></td>
</tr>
</tbody>
</table>

**Effective February 1, 2009, Level 2 service providers were no longer listed on Visa’s List of PCI DSS Compliant Service Providers. Entities that wish to be on the List of PCI DSS Compliant Service Providers must validate as a Level 1 provider.**
Payment Applications
These standards consist of the security requirements applicable to 3rd party, commercially-available payment applications.

By July 2010, all merchants must use PA DSS compliant applications.

Lists of compliant applications can be found at...
- www.pcisecuritystandards.org
- www.visa.com/cisp

Important: The requirement to use a PA DSS compliant application is separate from the requirement to be PCI compliant at all times.
- Using a PA DSS compliant application does not inherently make a merchant PCI compliant!
• Do not retain full magnetic stripe or CVC2/CVV2 data
• Protect stored cardholder data
• Provide secure password features
• Log application activity
• Develop secure applications
• Protect wireless transmissions
• Test applications to address vulnerabilities

• Facilitate secure network implementation
• Cardholder data must never be stored on a server connected to the Internet
• Facilitate secure remote software updates
• Facilitate secure remote access to application
• Encrypt sensitive traffic over public networks
• Encrypt all non-console administrative access
Final Thoughts

& Resources
1. Exploitation of insecure remote access seems to be the most common method of entry.
2. Once inside, malware such as packet sniffers and key stroke loggers are installed to capture and exfiltrate card data.
3. Prohibited data storage is still a problem with smaller merchants.
4. Ecommerce merchants are still vulnerable to SQL injection attacks.
5. Even PA-DSS validated applications are vulnerable to some of these attack vectors further underscoring the importance of full compliance with the PCI DSS!
Helpful PCI Resources

• **PCI Security Standards Council** – www.pcisecuritystandards.org
  - PCI DSS, PA DSS and PTS Standards
  - Downloadable Self Assessment Questionnaires
  - List of Approved Scanning Vendors (ASV)
  - List of PA DSS Validated Payment Applications
  - Searchable FAQ Tool
  - PCI Supporting Documents

• **Visa’s CISP website** – www.visa.com/cisp
  - Merchant Levels Defined
  - List of PABP Validated Payment Applications
  - List of CISP Compliant Service Providers
  - Important Alerts, Bulletins and Webinar

• **MasterCard® SDP website** – www.mastercard.com/sdp
  - PCI Merchant Education Program
  - Program provides a variety of PCI-related webinar recordings

NOTE: This presentation is based upon information available to Fifth Third Processing Solutions as of the date of this communication. It’s important that you continue to stay current with changing industry requirements.
The information included in this presentation is for information purposes only, and is not intended as legal or financial advice. The information does not amend or alter your obligations under your agreement with Fifth Third Processing Solutions, or under the operating regulations of any credit card or debit card association.
Thank You!

Brian Irwin, CTP
VP, Treasury Management
Fifth Third Bank
Brian.Irwin@53.com
312.704-2986

Claire Dittrich
Executive Consultant
Middle Market
Claire.Dittrich@ftpsllc.com
312.475.1504