# IT Audit and Risk Trends
*for Credit Union Internal Auditors*

Blair Bautista, Director
Bob Grill, Manager
David Dyk, Manager

MOSS-ADAMS LLP
Certified Public Accountants | Business Consultants
*Acumen. Agility. Answers.*

# AGENDA

- Internet Banking Authentication
- ATM Security and PIN Compliance
- Social Media Trends
- PCI Compliance and Cardholder Security
- Questions and Answers

AGENDA TOPIC:

# INTERNET BANKING AUTHENTICATION CHANGES

# THE PROBLEM

- Dramatic rise in Internet Banking fraud in 2009-2011, due to improvements in malware
- Cross-channel fraud
- Commercial channel focus, with ACH and Wires being highest risk
- Some risk with consumer accounts and small business accounts with bill payment and account transfers to money mules

# UPDATED FFIEC GUIDANCE

- Regulators and examiners have been considering this issue in recent years, and provided updated guidance in June 2011
- Regulatory scrutiny in the area has increased, and institutions should carefully examine their Internet banking to determine if they are going to need to increase the security of high risk transactions such as ACH batches and wire transfers
- Recent June 2011 guidance is being used by examiners beginning in 2012

# OVERVIEW OF THE GUIDANCE - 1

- Differentiation between retail and business transaction risk
  - "Agencies recommend that institutions offer multifactor authentication to their business customers."
- Continued focus on Risk Assessment
- Continued, increased emphasis on Layered Security Programs

# OVERVIEW OF THE GUIDANCE - 2

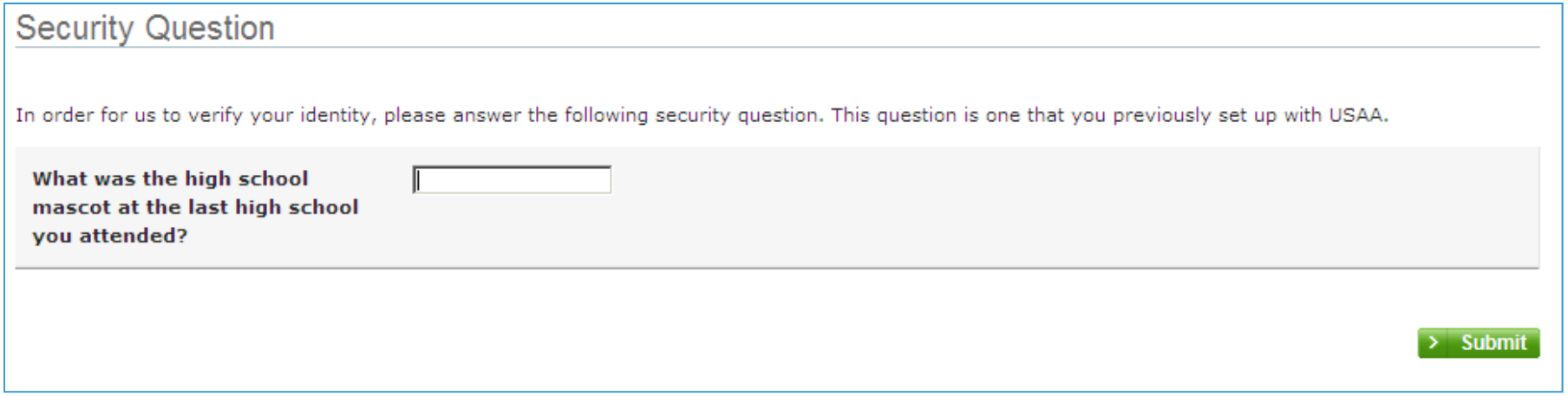
- Controls in Layered Security
  - Fraud detection and monitoring systems
  - Include consideration of customer history and behavior and enable a timely, effective institution response
  - Dual customer authorization through different access devices
  - Out-of-band verification for transactions
  - Use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account
  - Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times)

# OVERVIEW OF THE GUIDANCE - 3

- Controls in Layered Security (continued)
  - Internet protocol (IP) reputation-based tools
  - Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud
  - Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels
  - Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk

# OVERVIEW OF THE GUIDANCE - 4

- Guidance downplays two common controls
  - Device authentication
  - Challenge questions:  Encourages remaining challenges to focus on “out of wallet” questions



AGENDA TOPIC:

# ATM SECURITY AND PIN COMPLIANCE

# AGENDA

- Background
- PIN Compliance
  - STAR
  - Pulse
  - NYCE
  - Other Networks
- Common Findings
- How to Add Value
- ATM Logical Security Trends

# PIN SECURITY AND KEY MANAGEMENT BACKGROUND (1)

Requirements have been in place by the ATM networks that have created a large cross-section of the financial institution segment that must have regular audits of the PIN security and encryption key management function for their ATMs. These requirements also extend beyond financial institutions to organizations that are involved in the PIN security and encryption key management processes.

# PIN SECURITY AND KEY MANAGEMENT BACKGROUND (2)

Technical Guideline #3 (recently renamed Technical Report #39 or TR39) is an audit program guideline for PIN security and key management based on two ANSI Standards: X9.24 on key management and X9.8 for PIN security.

# WHO IS REQUIRED TO COMPLY – STAR (1)

- Any financial institution or merchant who is a processing member of the STAR network, directly or indirectly, is required to have a TG3/TR39 audit on a bi-annual basis and submit their report, ***done by a CTGA auditor***, to STAR.
- The TG3/TR39 due date for STAR members is December 31 of every *even numbered year*, unless the network grants an extension to that member.

# WHO IS REQUIRED TO COMPLY – PULSE (1)

Any financial institution or merchant who is a processing member of PULSE, directly or indirectly, is required to have this audit on a bi-annual basis and submit their report electronically by a CTGA auditor to PULSE network through their Website. ***For processing entities, the auditor must be a CTGA auditor***.

# WHO IS REQUIRED TO COMPLY – NYCE

NYCE: Any member of NYCE who is processing transactions and is *directly connected* to NYCE is mandated to have this audit. If a financial institution is processing transactions, but is *indirectly connected* to NYCE, it is not mandated to have this audit. The TR39/TG3 due date for NYCE members is every two years from its first TG3 audit, by December 31 of that year.

# WHO IS REQUIRED TO COMPLY – OTHER NETWORKS

In addition, other ATM network service providers require customers to comply with their own customized version of the PIN security and encryption key management requirements. For example, CO-OP clients are required to complete a self-assessment and submit the results via the CO-OP online reporting tool. The due date for CO-OP self assessments is December 31 of every even numbered year.

# COMMON FINDING (1)

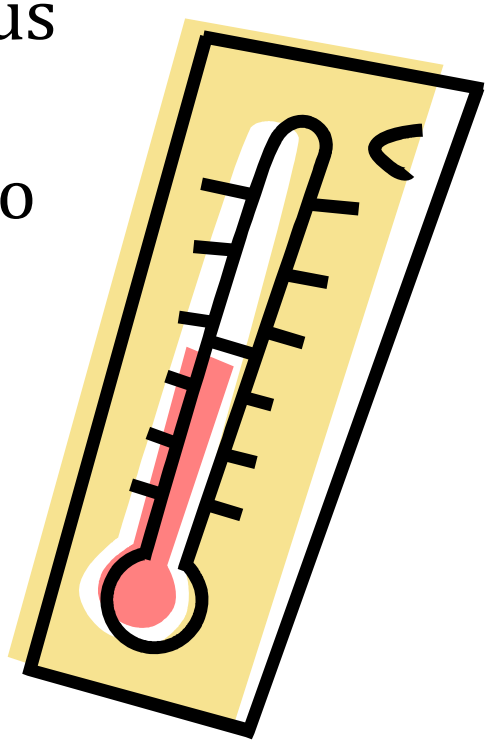
- Almost every control in the PIN audits includes the statement "documented procedures exist and are followed."
- The most common finding is a lack of written procedures relating to the controls and procedures surrounding PIN and encryption key management.
- Most findings can be avoided by ensuring that the processes in place are documented.

# COMMON FINDING (2)

- The PIN standards require that PIN numbers be entered and encrypted within the PIN Encryption Device (PED).
- Many ATM PIN pads do not meet this standard.
- A list of approved PEDs is available online. Procedures should ensure that all new ATMs contain approved PEDs as part of the purchasing and installation process.

# HOW CAN THE AUDIT ADD VALUE? (1)

The TR39 reviews cover numerous technical and operational areas. While the questions are specific to the scope of the encryption management process, the areas involved can be used as a “temperature check” for many other critical functions in the organization.



# HOW CAN THE AUDIT ADD VALUE? (2)

Areas that are addressed (either directly or indirectly) during the audit:

- Policies and Procedures
- Vendor Management
- GLBA
- Information Security
- Segregation of Duties
- System Access Rights
- Physical Security

# HOW CAN THE AUDIT ADD VALUE? (3)

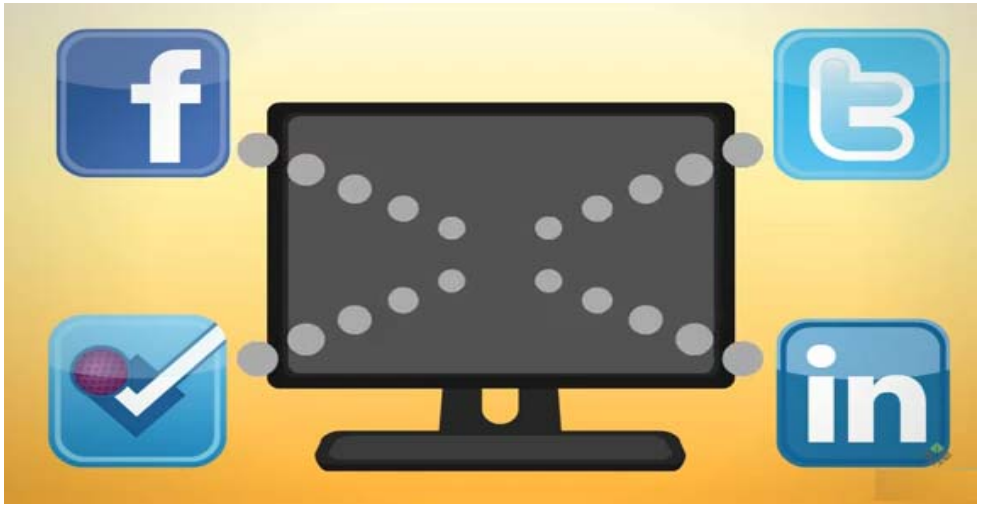
By approaching the audit as an opportunity to provide valuable feedback regarding best practice and improvement opportunities, you can turn the audit into something more than just a compliance checklist. You can turn this mandatory audit into an opportunity to further enhance the controls in place in the IT environment.

# ATM LOGICAL SECURITY TRENDS

- Increasing number of data breaches involving ATM devices
- Regulator expectation that ATMs will be segmented from the financial institution network
- Concern regarding antivirus, security monitoring, and patch management for ATM operating systems (partly driven by PCI)

AGENDA TOPIC:

# SOCIAL MEDIA TRENDS IN CREDIT UNIONS



# THE LANDSCAPE

- Social networking sites are increasing
  - Facebook – 500 million active users that spend 700 billion minutes per month and share 30 billion pieces of content. 550,000 active applications within more than 1million websites.
- More institutions have their own presence on Facebook, LinkedIn and Twitter
- Business units within companies are using social media for public relations, marketing, and sales programs
- Social networking is heading down the same path as online banking

# THE PROBLEM

- Lack of visibility and control
  - Identifying and controlling user access
- Widening attack surface
  - Lack of effective way to inspect streaming content for malicious code
- Data loss potential
  - Little control since policies do not cover what users contribute

# CASE STUDY: FACEBOOK DATA USE POLICY – IMPACT ON CREDIT UNIONS

- The Facebook privacy policy is 6 pages long and is very ambiguous.
- The policy indicates that they can find out (enumerate in hacker terms) the following information that are often be used as authenticators when consumer calls the credit union: TS1
  - Home address – taken from cell phone 911 settings
  - Date of birth
- Facebook can read any information sent in messages, used in conversation, or by searching your friends' information to find your identifiers commonly used in Credit Union interactions with customers; such as mother's maiden name or other identifiers used TS2
- All this data is shared with "advertising partners," facebook says they do not include "name" but with other information, such as address, you can determine the name easily – or just match with Facebook information you choose to make "public" or cross reference with the phone book. The Privacy policy does not say it hides your friends' names. TS3 TS4

## Slide 27

**TS1** This doesn't make sense. There are words missing - needs to be rewritten.
Terri Scheumann, 2/7/2012

**TS2** Again, needs to be rewritten - why say mother's maiden name twice?
Terri Scheumann, 2/7/2012

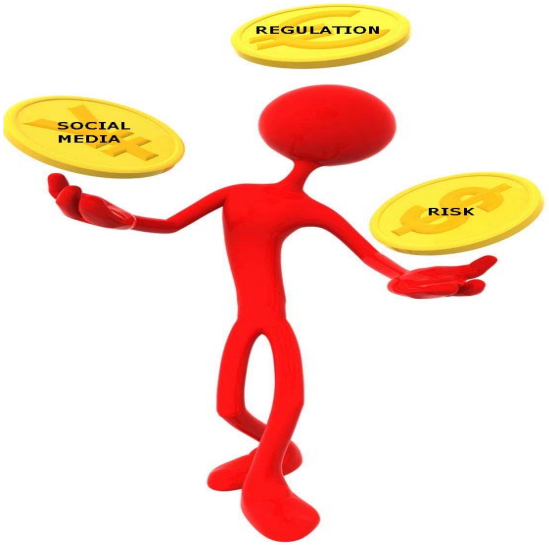
**TS3** who says?
Terri Scheumann, 2/7/2012

**TS4** who?
Terri Scheumann, 2/7/2012

# FACEBOOK MONITORING


# CONCLUSION – IMPACT ON CREDIT UNIONS

- Use Facebook and they can figure out your password reset identifiers
- Facebook advertisers can also determine the information from the information given to them by Facebook



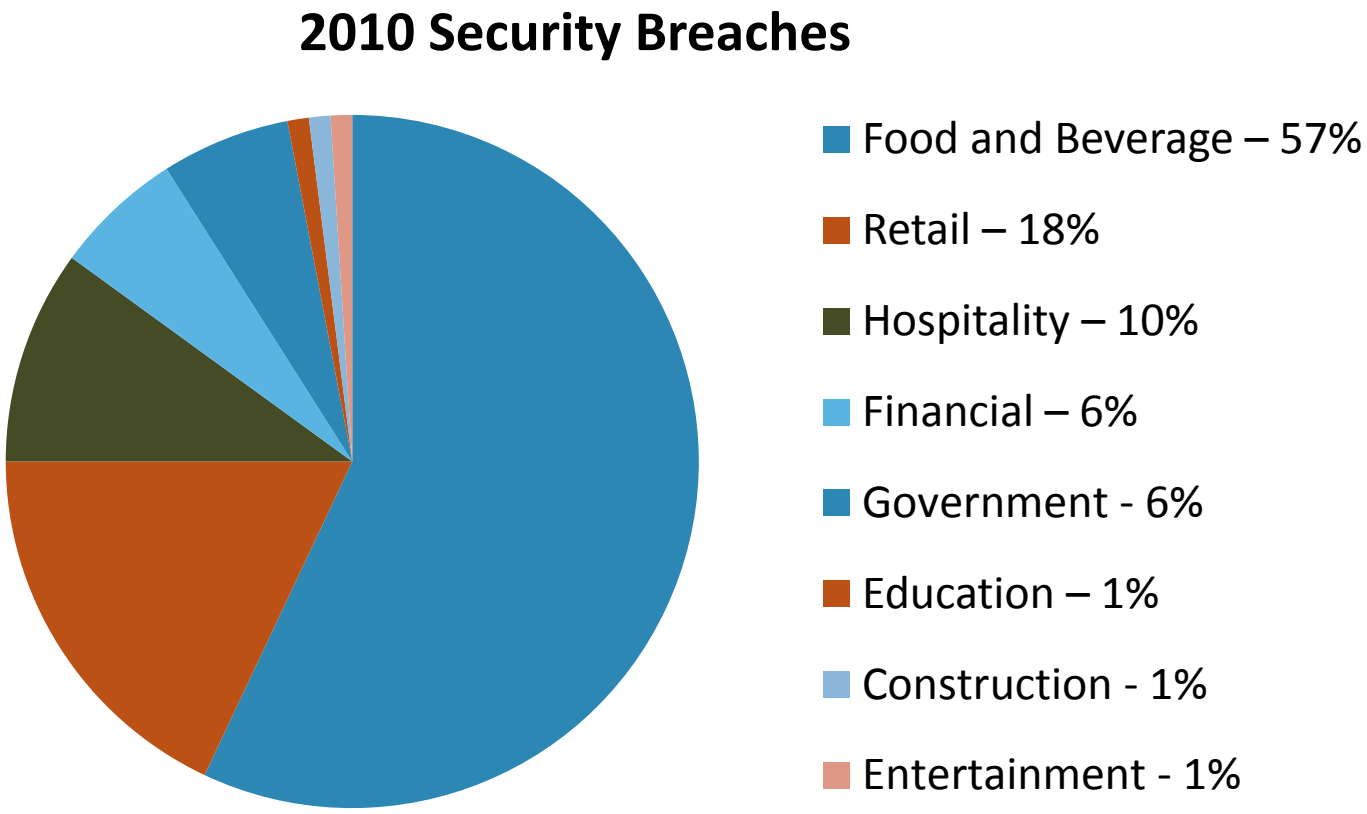
# CONCLUSION – IMPACT ON REGULATIONS

- Gramm Leach Bliley
- California Financial Privacy Act: Senate Bill 1
- Red Flag Rule

AGENDA TOPIC:

# PCI COMPLIANCE FOR CREDIT UNIONS

# CARD BREACHES ARE ON THE RISE




Source*: Trustwave's Global Security Report 2010*

# NOTABLE CARD BREACHES

- TJX Companies – 2007 – Hackers compromised wireless network to steal information on approximately 94 million card transactions.
- Heartland Payment Systems – 2008 – Hackers attacked system used to process card transactions. Inserted malware. Up to 100+ million transactions compromised.
- Lush Cosmetics – 2010 – Ecommerce website hacked. 5,000 card transactions accessed. Led to shutdown of their ecommerce operations.
- Sony PS Network – 2011 – Hackers accessed an old database containing consumer info and credit card info. Millions of customers' information stolen.

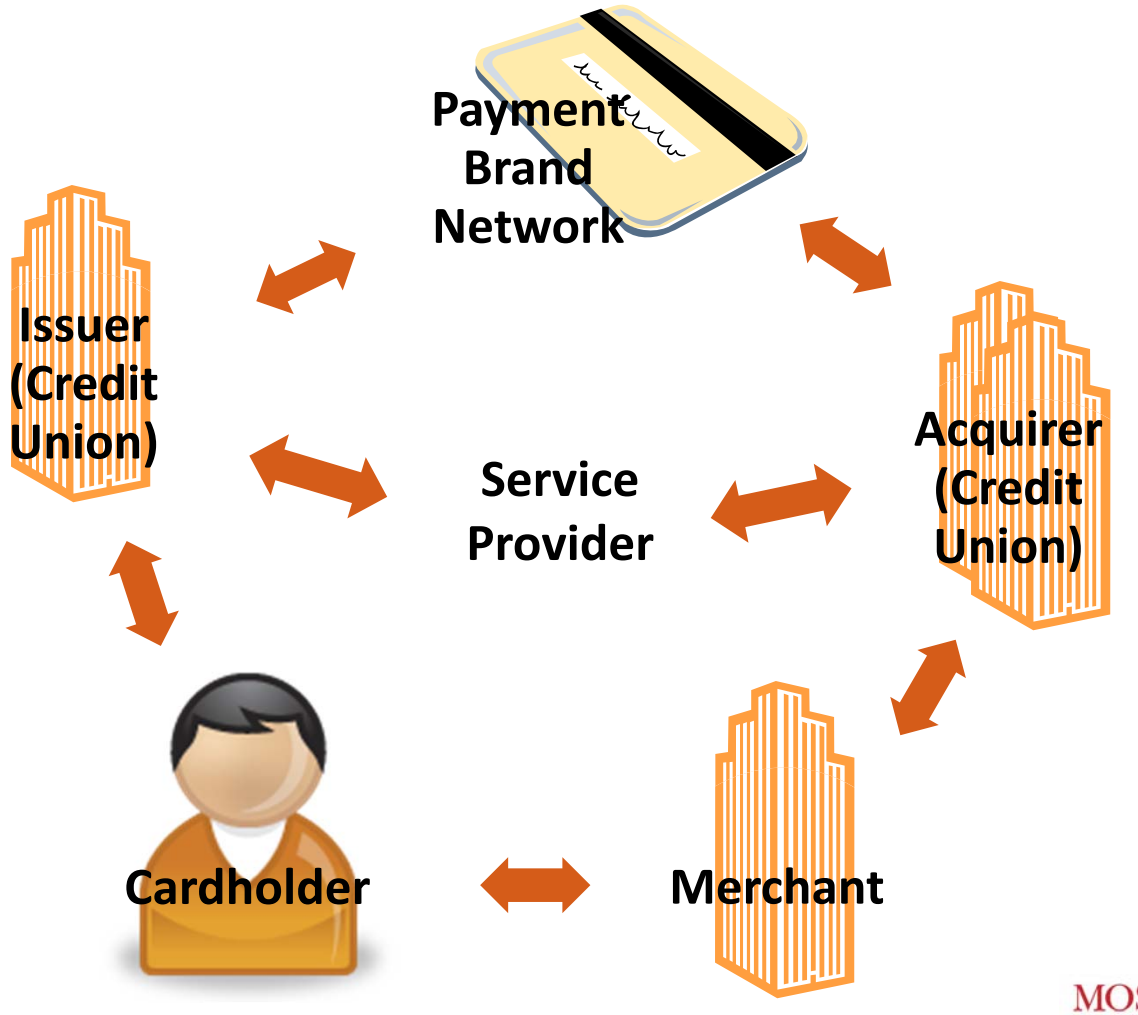
# PCI OVERVIEW

- **PCI Security Standards Council** (PCI SSC or the Council) founded in 2006 is responsible for the development, management, education, and awareness of the PCI Security Standards.
- **PCI Data Security Standard** (PCI DSS) is a comprehensive set of international security requirements for protecting cardholder data.
- **Payment Application Data Security Standard** (PA-DSS) is a set of requirements for software vendors to develop secure payment applications.
- **PCI PIN Transaction Security** (PCI PTS) is a set of requirements for device vendors and manufacturers for all personal identification number (PIN) terminals, including POS devices, encrypting PIN pads, and unattended payment terminals.

# PCI OVERVIEW

- Not a federal regulation, but an industry regulation.
- In some states, they are state laws.
- Purpose is to help prevent credit card fraud and maintain public confidence in payment cards.
- All entities that process, store, or transmit payment card information need to comply. (Primary Account Number (PAN) is the deciding factor.)
- Card transaction players: card brands, merchants, service providers, acquirers, and issuers.
- Effective compliance dates vary depending on merchant level or service provider level and card brand. All deadline enforcement will come from the acquiring credit union.
- Card brands have their own compliance programs and are responsible for compliance tracking, enforcement, penalties, and fees.

# THE PAYMENT CARD TRANSACTION



# ROLES OF THE QSA AND ASV

- QSA – Qualified Security Assessor
  - Certified to validate compliance with PCI-DSS
  - Qualified Security Assessor companies have been qualified to have their employees assess compliance to the PCI-DSS standard
  - Qualified Security Assessors are employees of these organizations who have been certified to validate an entity's adherence to the PCI-DSS
- ASV – Approved Scanning Vendor
  - Approved Scanning Vendors are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers.

# PCI DSS REQUIREMENTS

## PCI Data Security Standard – High-Level Overview

### 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 |

### Protect Cardholder Data

| | |
|---|---|
| Requirement 3: | Protect stored cardholder data |
| Requirement 4: | Encrypt transmission of cardholder data across open, 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 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 |

### 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 |

### Maintain an Information Security Policy

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

# SERVICE PROVIDERS

| Service Provider Level | Description | Posted on Visa's Global List of Validated Service Providers |
|---|---|---|
| 1 | VisaNet® processors or any service provider that stores, processes, and/or transmits over 300,000 Visa transactions annually. | Yes |
| 2* | Any service provider that stores, processes, and/or transmits less than 300,000 Visa transactions annually. | No* |

* Level 2 service providers may choose to validate as a Level 1 service provider in order to be listed on Visa's Global List of Validated Service Providers.

# QUESTIONS?


blair.bautista@mossadams.com

415-677-8322



bob.grill@mossadams.com

916-503-8127



david.dyk@mossadams.com

503-478-2145


# QUESTIONS?

francis.tam@mossadams.com
310-295-3852

bob.grill@mossadams.com
916-503-8127