G12 - Visa’s Strategy to Secure the Payment System

Tia Ilori

September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Visa's Strategy to Secure the Payment System

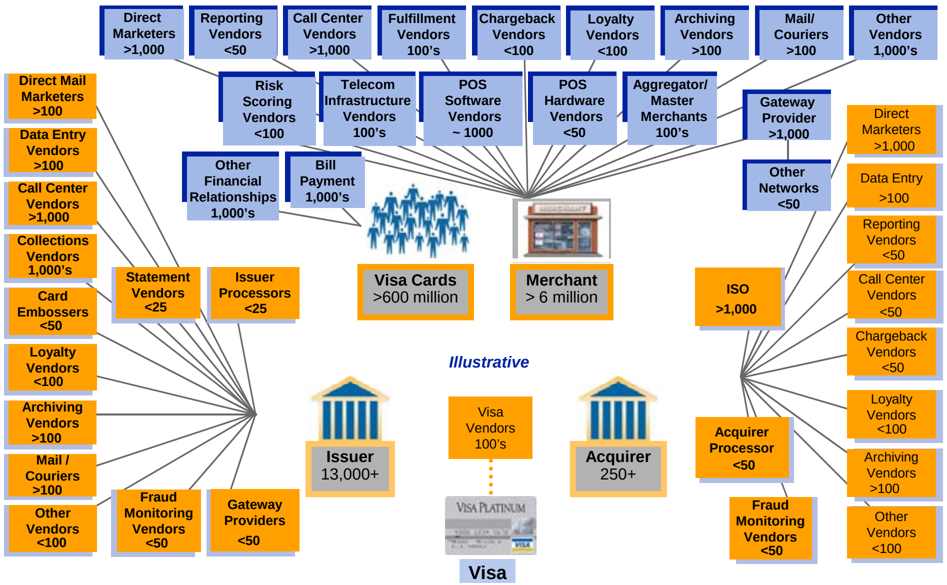
Tia D. Ilori
Payment System Security Compliance
Visa Inc.

September 22, 2009

Agenda

- Security Landscape
- Mission and Strategy
- Payment System Security Compliance
- Cyber Security and Investigation
- Q & A

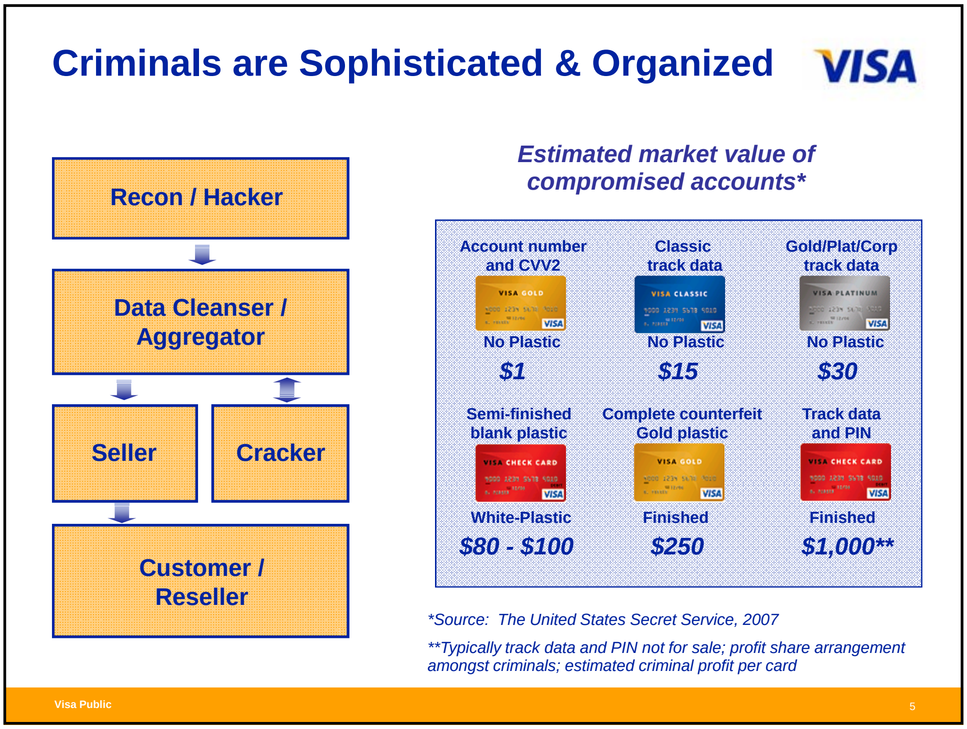
Complex Payment Landscape – U.S. Illustrative



Security Environment

As PCI DSS compliance rates rise, new compromise trends emerge

Compliance Milestone	Compromise Trend
PCI DSS compliance is adopted by acquiring participants in the U.S.	Issuers and processors increasingly targeted; non-U.S. compromises increasing rapidly
Merchants and service providers reduce historical storage of cardholder data	Data criminals seek capture of cardholder data in transit through sniffer attacks
PCI DSS compliance improves among large merchants	Compromises of small and medium size merchants increase
E-commerce and payment channel websites better secured	SQL injection attacks on non-payment sites to gain access to payment environment



Criminals are Sophisticated & Organized

Recon / Hacker

Data Cleanser / Aggregator

Seller

Cracker

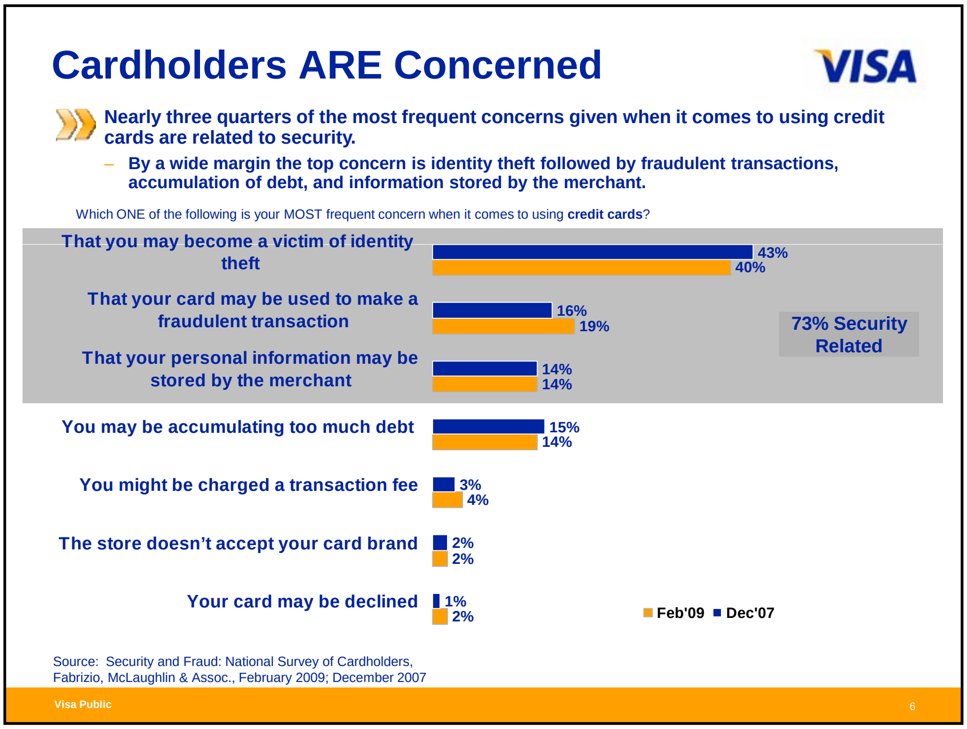
Customer / Reseller

*Estimated market value of compromised accounts**

Account number and CVV2	Classic track data	Gold/Plat/Corp track data
No Plastic	No Plastic	No Plastic
$1	***$15***	***$30***
Semi-finished blank plastic	**Complete counterfeit Gold plastic**	**Track data and PIN**
White-Plastic	Finished	Finished
$80 - $100	***$250***	***$1,000*****

**Source: The United States Secret Service, 2007*

***Typically track data and PIN not for sale; profit share arrangement amongst criminals; estimated criminal profit per card*



Cardholders ARE Concerned

- **Nearly three quarters of the most frequent concerns given when it comes to using credit cards are related to security.**
  - **By a wide margin the top concern is identity theft followed by fraudulent transactions, accumulation of debt, and information stored by the merchant.**

Which ONE of the following is your MOST frequent concern when it comes to using **credit cards**?

	Dec'07	Feb'09
That you may become a victim of identity theft	43%	40%
That your card may be used to make a fraudulent transaction	16%	19%
That your personal information may be stored by the merchant	14%	14%
You may be accumulating too much debt	15%	14%
You might be charged a transaction fee	3%	4%
The store doesn't accept your card brand	2%	2%
Your card may be declined	1%	2%

73% Security Related

Feb'09 Dec'07

Source: Security and Fraud: National Survey of Cardholders, Fabrizio, McLaughlin & Assoc., February 2009; December 2007

Compromises in the Media - Myths and Facts

Myths		Facts
PCI DSS compliant entities have been breached	»»	As of today, no compromised entity has been found to be compliant at the time of the breach
PCI DSS does not address sniffer* attacks	»»	PCI DSS should prevent and detect unauthorized network access and installation of sniffers
Visa does not support encryption	»»	Visa does support encryption for both online and batch files
Encryption of data transmission can prevent recent compromises	»»	Encryption does not eliminate the risk of data being "sniffed" if data is decrypted at any point

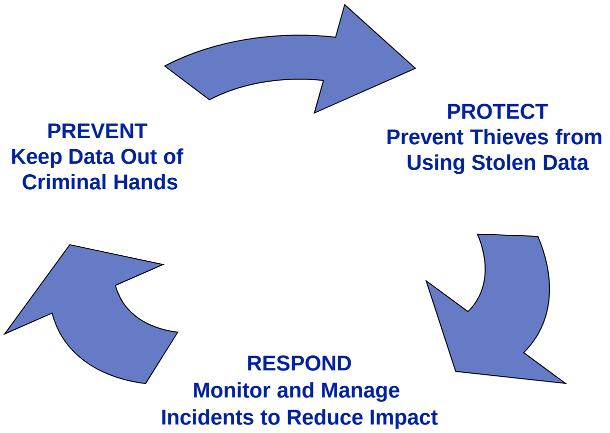
PCI DSS continues to serve as a robust foundation to protect cardholder data in a static data environment

*Sniffers are used by hackers to monitor and capture data in transit over an internal network

What is Payment System Risk strategy?

Easy to say, but difficult to do . . .

Maintain Trust in Visa Payments



PREVENT
Keep Data Out of Criminal Hands

PROTECT
Prevent Thieves from Using Stolen Data

RESPOND
Monitor and Manage Incidents to Reduce Impact

Partner with Clients & Stakeholders

Payment System Security Compliance

Major Programs:

- **PCI DSS Compliance –**
  Drive PCI DSS compliance to ensure entities protect cardholder data from compromise
- **PIN Security Compliance -**
  Advance compliance with the PCI PIN Security Requirements to prevent PIN compromises
- **Payment Application Security -**
  Promote development and use of secure payment applications and eliminate vulnerable applications
- **PCI Security Standards Council -**
  Ensure successful advancement of industry security standards in support of Visa programs

YOU'RE PROTECTED. Visa's multiple layers of security are designed to prevent fraud. But even if fraud does occur with your Visa® credit or check card, you're not liable. For peace of mind online and off, Visa security is key.

Common Compromise Vulnerabilities

PCI DSS compliance should mitigate common vulnerabilities found to contribute to data breaches

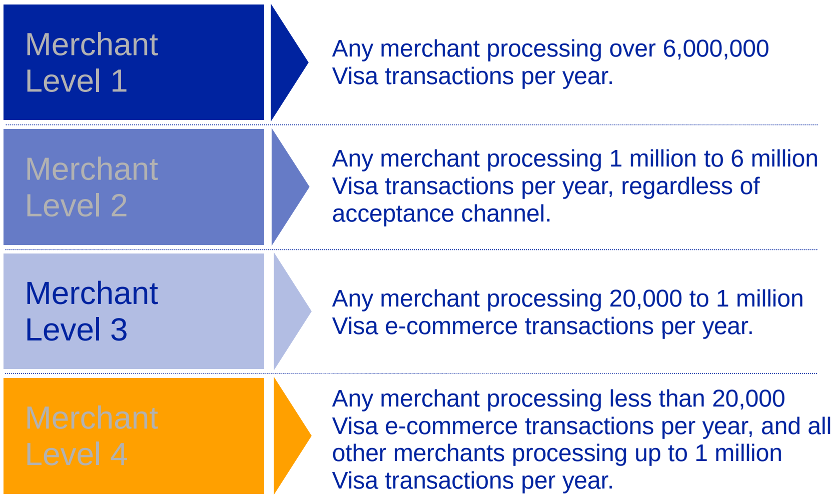
PCI Data Security Standard	Common Compromise Vulnerabilities	
Build and Maintain a Secure Network	▪ Failure to secure and monitor connected non-payment environment ▪ Improperly segmented networks ▪ Insufficient egress and ingress filtering and firewall monitoring ▪ Insecure database configuration ▪ Failure to update or change default passwords	PREVENTION ↓ DETECTION
Protect Cardholder Data		
Maintain a Vulnerability Management Program	▪ Unprotected systems vulnerable to SQL injection attacks ▪ Corporate websites targeted to gain access to network – Malware installed to capture passwords and cardholder data	
Implement Strong Access Control Measures	▪ Failure to limit user access to critical system	
Regularly Monitor and Test Networks	▪ No monitoring of privileged user access ▪ No implementation or monitoring of intrusion detection or anti-virus	
Maintain an Information Security Policy		

Compliance and Compromise Trends

Too much emphasis on PCI DSS validation as a finish line rather than ongoing security and compliance leaves exposure

- PCI DSS controls, when implemented properly, would prevent network intrusions
  - If the network is compromised, impact should be mitigated via timely detection
- In all compromise cases, forensic investigations have found significant gaps in the compromised entity’s PCI DSS controls to be major contributors to the breach
- Validating compliance is a snapshot, point-in-time review of a business’ systems, and is limited in scope to a sample of systems
  - Entities must not rely solely on a Qualified Security Assessors to determine their compliance
  - PCI DSS can no more account for every eventuality than a financial audit can review all the financial transactions of a company
- Maintaining good security requires an ongoing commitment
  - PCI DSS compliance is a 24 hour a day, 7 day a week, 365 day a year job
  - Businesses must build ongoing compliance monitoring into their internal auditing processes

Visa Merchant Levels



Merchant Level 1

Any merchant processing over 6,000,000 Visa transactions per year.

Merchant Level 2

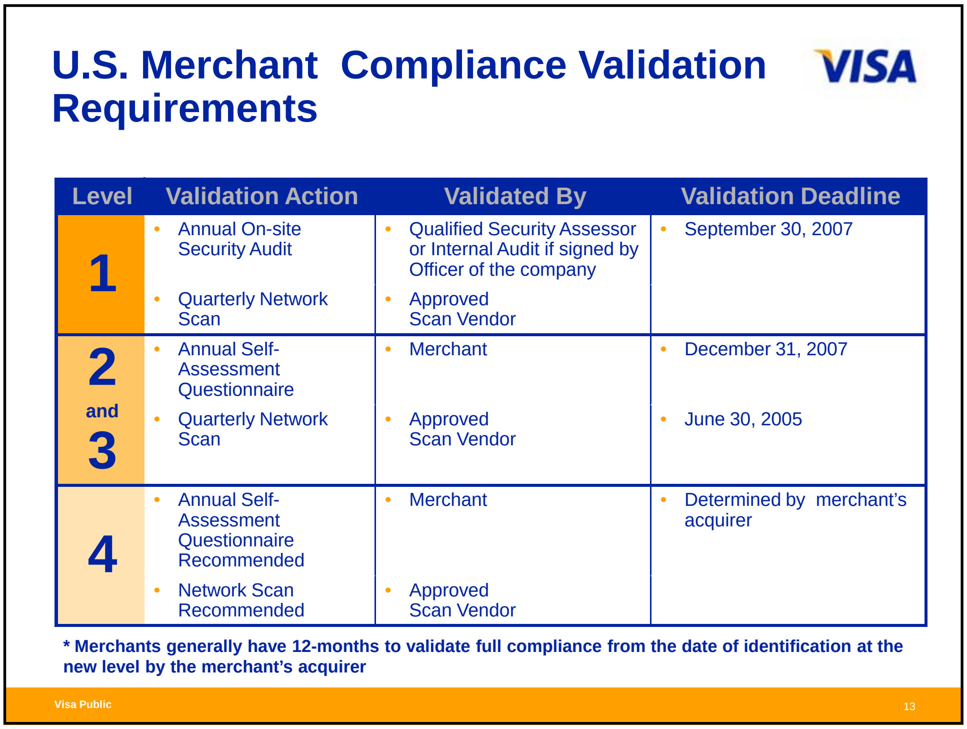
Any merchant processing 1 million to 6 million Visa transactions per year, regardless of acceptance channel.

Merchant Level 3

Any merchant processing 20,000 to 1 million Visa e-commerce transactions per year.

Merchant Level 4

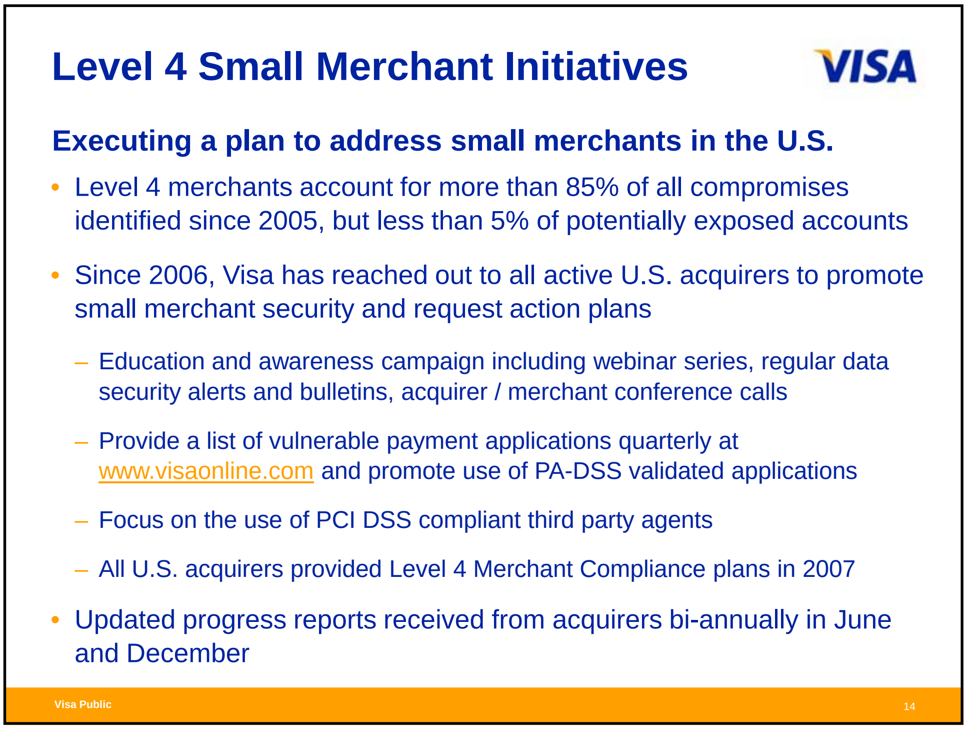
Any merchant processing less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1 million Visa transactions per year.



U.S. Merchant Compliance Validation Requirements

Level	Validation Action	Validated By	Validation Deadline
1	• Annual On-site Security Audit • Quarterly Network Scan	• Qualified Security Assessor or Internal Audit if signed by Officer of the company • Approved Scan Vendor	• September 30, 2007
2 and 3	• Annual Self-Assessment Questionnaire • Quarterly Network Scan	• Merchant • Approved Scan Vendor	• December 31, 2007 • June 30, 2005
4	• Annual Self-Assessment Questionnaire Recommended • Network Scan Recommended	• Merchant • Approved Scan Vendor	• Determined by merchant's acquirer

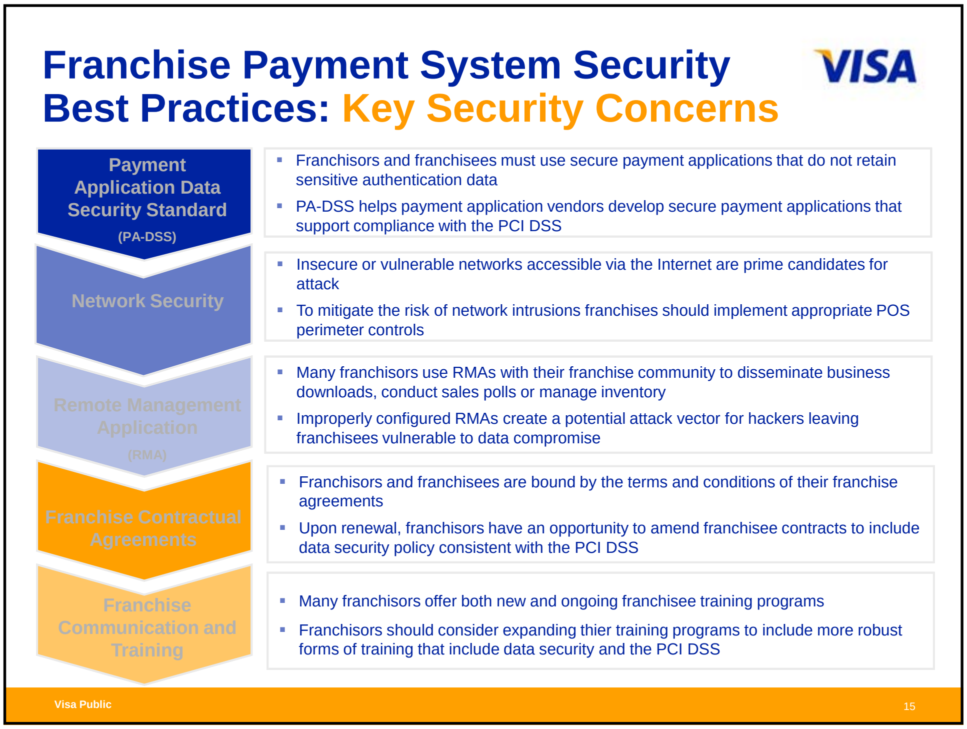
*** Merchants generally have 12-months to validate full compliance from the date of identification at the new level by the merchant's acquirer**



Level 4 Small Merchant Initiatives

Executing a plan to address small merchants in the U.S.

- Level 4 merchants account for more than 85% of all compromises identified since 2005, but less than 5% of potentially exposed accounts
- Since 2006, Visa has reached out to all active U.S. acquirers to promote small merchant security and request action plans
  - Education and awareness campaign including webinar series, regular data security alerts and bulletins, acquirer / merchant conference calls
  - Provide a list of vulnerable payment applications quarterly at www.visaonline.com and promote use of PA-DSS validated applications
  - Focus on the use of PCI DSS compliant third party agents
  - All U.S. acquirers provided Level 4 Merchant Compliance plans in 2007
- Updated progress reports received from acquirers bi-annually in June and December



Franchise Payment System Security Best Practices: Key Security Concerns

VISA

Payment Application Data Security Standard (PA-DSS)

- Franchisors and franchisees must use secure payment applications that do not retain sensitive authentication data
- PA-DSS helps payment application vendors develop secure payment applications that support compliance with the PCI DSS

Network Security

- Insecure or vulnerable networks accessible via the Internet are prime candidates for attack
- To mitigate the risk of network intrusions franchises should implement appropriate POS perimeter controls

Remote Management Application (RMA)

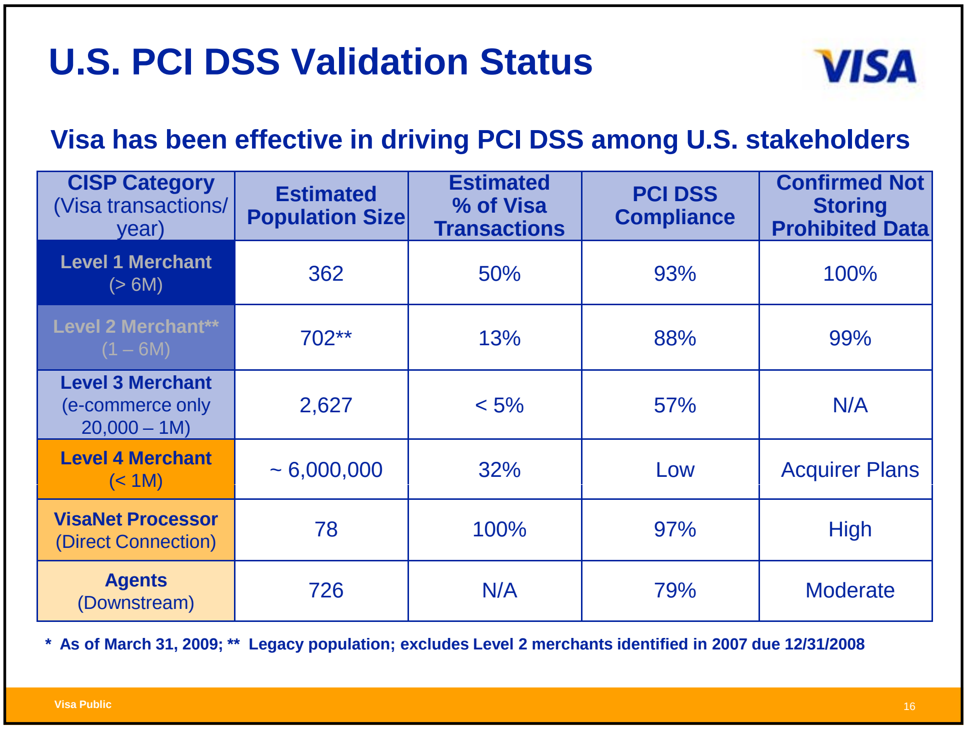
- Many franchisors use RMAs with their franchise community to disseminate business downloads, conduct sales polls or manage inventory
- Improperly configured RMAs create a potential attack vector for hackers leaving franchisees vulnerable to data compromise

Franchise Contractual Agreements

- Franchisors and franchisees are bound by the terms and conditions of their franchise agreements
- Upon renewal, franchisors have an opportunity to amend franchisee contracts to include data security policy consistent with the PCI DSS

Franchise Communication and Training

- Many franchisors offer both new and ongoing franchisee training programs
- Franchisors should consider expanding thier training programs to include more robust forms of training that include data security and the PCI DSS



U.S. PCI DSS Validation Status

VISA

Visa has been effective in driving PCI DSS among U.S. stakeholders

CISP Category (Visa transactions/ year)	**Estimated Population Size**	**Estimated % of Visa Transactions**	**PCI DSS Compliance**	**Confirmed Not Storing Prohibited Data**
Level 1 Merchant (> 6M)	362	50%	93%	100%
Level 2 Merchant** (1 – 6M)	702**	13%	88%	99%
Level 3 Merchant (e-commerce only 20,000 – 1M)	2,627	< 5%	57%	N/A
Level 4 Merchant (< 1M)	~ 6,000,000	32%	Low	Acquirer Plans
VisaNet Processor (Direct Connection)	78	100%	97%	High
Agents (Downstream)	726	N/A	79%	Moderate

*** As of March 31, 2009; ** Legacy population; excludes Level 2 merchants identified in 2007 due 12/31/2008**

PCI PIN Security Program

Focus on prevention of PIN data storage and key encryption

- Support all participants in the acquiring transaction processing chain to maintain the highest level of PIN security
- Assist all participants to protect cardholder PIN confidentiality through educational key workshops
- Established end-to-end TDES usage mandates (VisaNet endpoints, ATM and POS)
- Mandated usage of lab-evaluated, Visa-approved PIN Entry Devices (PED)
- Establishes encryption key management policies and practices via enforcement of the PCI PIN & PED Security Requirements
- PIN related risk and compliance policies
- On-site PIN security reviews on risk prioritized basis

- Annual Attestations required from program participants
- Partner with PIN debit networks to eliminate track data storage. Visa Technical Letter pending
- Visa activities:
  - PIN related risk and compliance policies
  - On-site PIN security reviews on risk prioritized basis
  - Key Management workshops
  - www.visa.com/pin

Payment Application Security

Drive the adoption of secure payment applications that do not store prohibited data

- Visa's PABP published in 2005
  - Provide vendors guidance to develop products that facilitate Payment Card Industry Data Security Standard (PCI DSS) compliance
  - Minimize compromises caused by insecure payment applications with emphasis on track data storage
- List of validated payment applications published monthly since January 2006
  - 555 products across 254 vendors independently validated by a Qualified Security Assessor (QSA)
  - List of PA-DSS validated applications published at www.pcisecuritystandards.org and www.visa.com/cisp
- List of vulnerable payment applications published quarterly since February 2007
- PABP adopted by PCI SSC as an industry standard, PA-DSS in April 2008

Payment Application Mandates: U.S.

Visa plans to drive the use of secure payment applications in the marketplace

Phase	Compliance Mandate	Effective Date
I.	Newly boarded merchants must not use known vulnerable payment application and VisaNet Processors (VNPs) and agents must not certify known vulnerable payment applications	1/1/08
II.	VNP and agents must certify only PA-DSS compliant payment applications to their platforms	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or utilize PA-DSS compliant payment applications[1]	10/1/08
IV.	VNP and agents must decertify all known vulnerable payment applications[2]	10/1/09
V.	Acquirers must ensure their merchants, VNP and agents use PA-DSS compliant payment applications	7/1/10

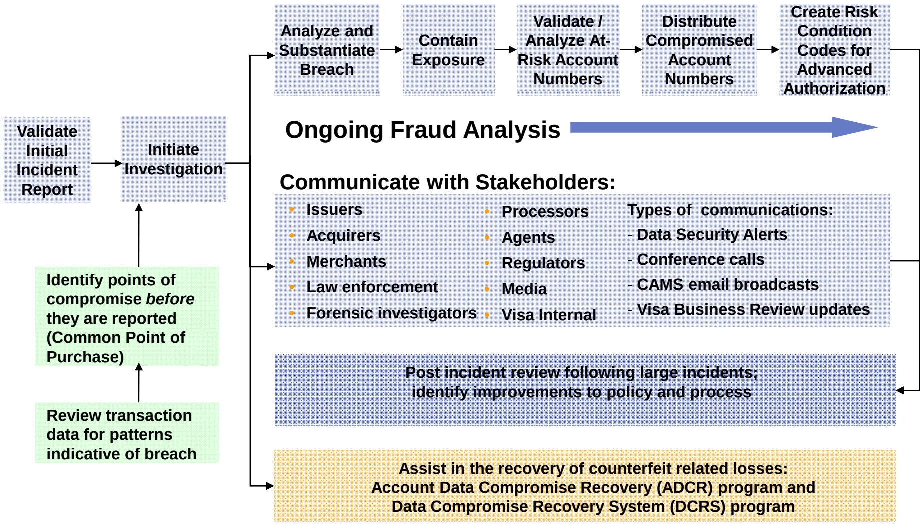
1. **In-house use only developed applications & stand-alone POS terminals are not applicable**
2. **VisaNet Processors and agents must decertify vulnerable payment applications within 12 months of identification**

Cyber-Security and Investigation

Major Programs:

- **Fraud Investigations –**
  Investigate data compromise and fraud incidents affecting Visa and its customers in order to reduce fraud
- **Compromised Account Management System (CAMS) –**
  Provides secure means of distributing compromised accounts to Visa customers
- **Incident Management, Systems, Policies and Reporting –**
  Manage internal systems, policies / procedures and reporting for fraud investigations
- **Forensic and Cyber Security –**
  Manage forensic program, provide forensic cause / trend analysis, gather and distribute cyber-intelligence to help secure the payment system

Security Strategy: Manage the Impact
. . . on behalf of 1,000’s of stakeholders

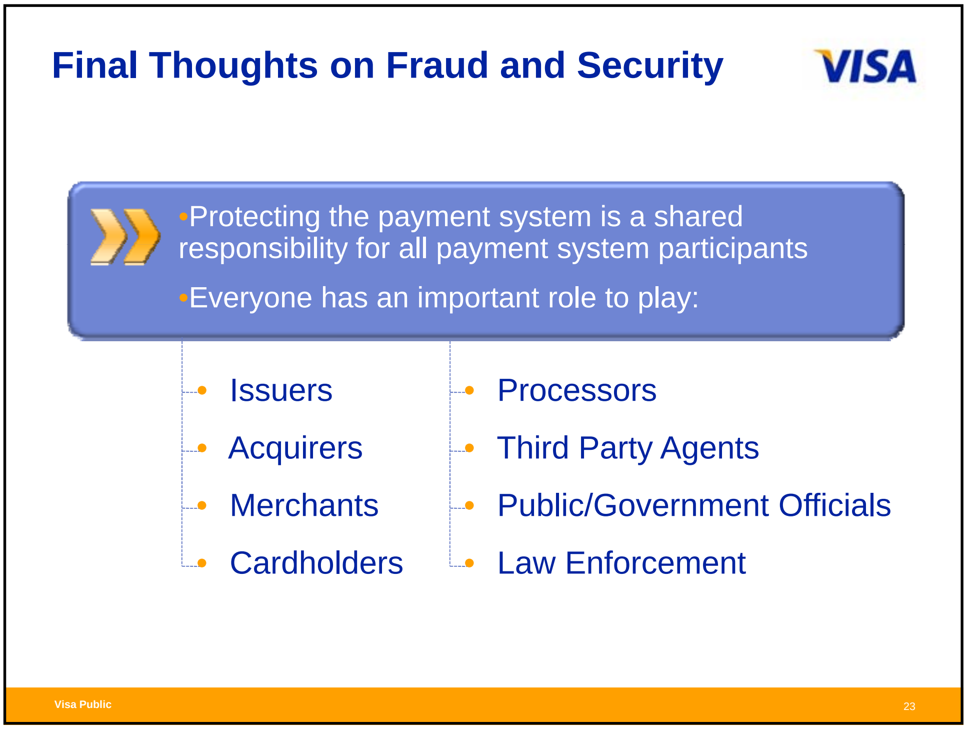


Validate Initial Incident Report
Initiate Investigation
Identify points of compromise *before* they are reported (Common Point of Purchase)
Review transaction data for patterns indicative of breach
Analyze and Substantiate Breach
Contain Exposure
Validate / Analyze At-Risk Account Numbers
Distribute Compromised Account Numbers
Create Risk Condition Codes for Advanced Authorization
Ongoing Fraud Analysis
Communicate with Stakeholders:
Issuers
Acquirers
Merchants
Law enforcement
Forensic investigators
Processors
Agents
Regulators
Media
Visa Internal
Types of communications:
- Data Security Alerts
- Conference calls
- CAMS email broadcasts
- Visa Business Review updates
Post incident review following large incidents; identify improvements to policy and process
Assist in the recovery of counterfeit related losses: Account Data Compromise Recovery (ADCR) program and Data Compromise Recovery System (DCRS) program

Call to Action

Ensure your data security program is comprehensive and continuously maintained

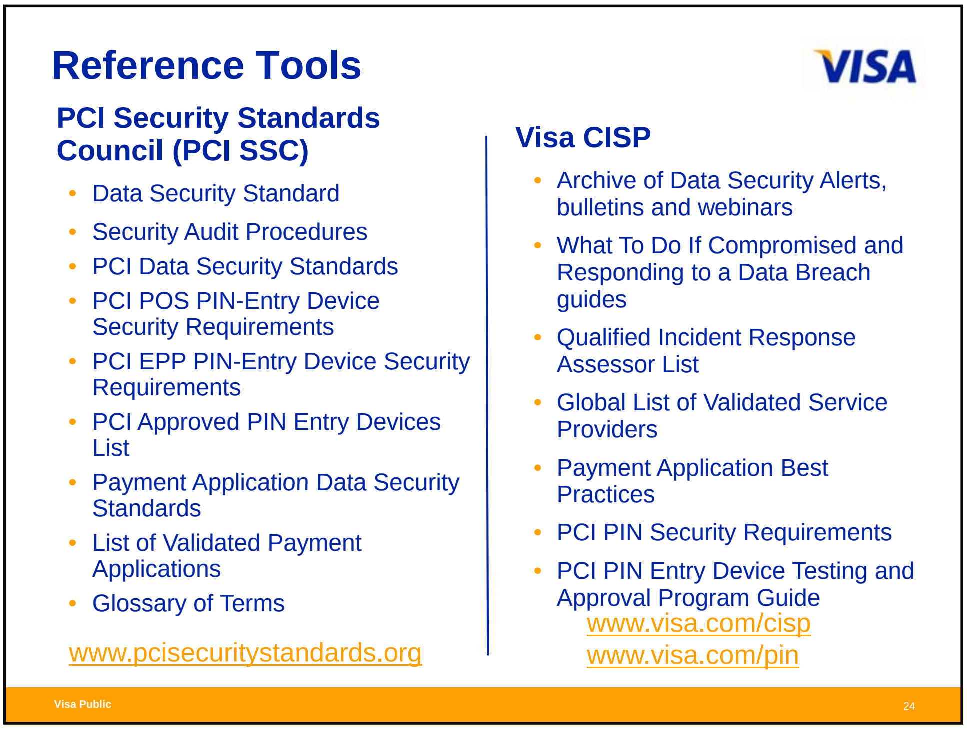
- Stay up-to-date on security alerts, bulletin and other important communications posted on www.visa.com/cisp
- Scan network for malware and IP addresses provided by Visa
- Do not lose focus on corporate network security
- Identify affiliated entities / business lines / products that store, process or transmit Visa account numbers or develop payment applications and their respective compliance status



Final Thoughts on Fraud and Security

- Protecting the payment system is a shared responsibility for all payment system participants
- Everyone has an important role to play:

- Issuers
- Acquirers
- Merchants
- Cardholders
- Processors
- Third Party Agents
- Public/Government Officials
- Law Enforcement



Reference Tools

PCI Security Standards Council (PCI SSC)

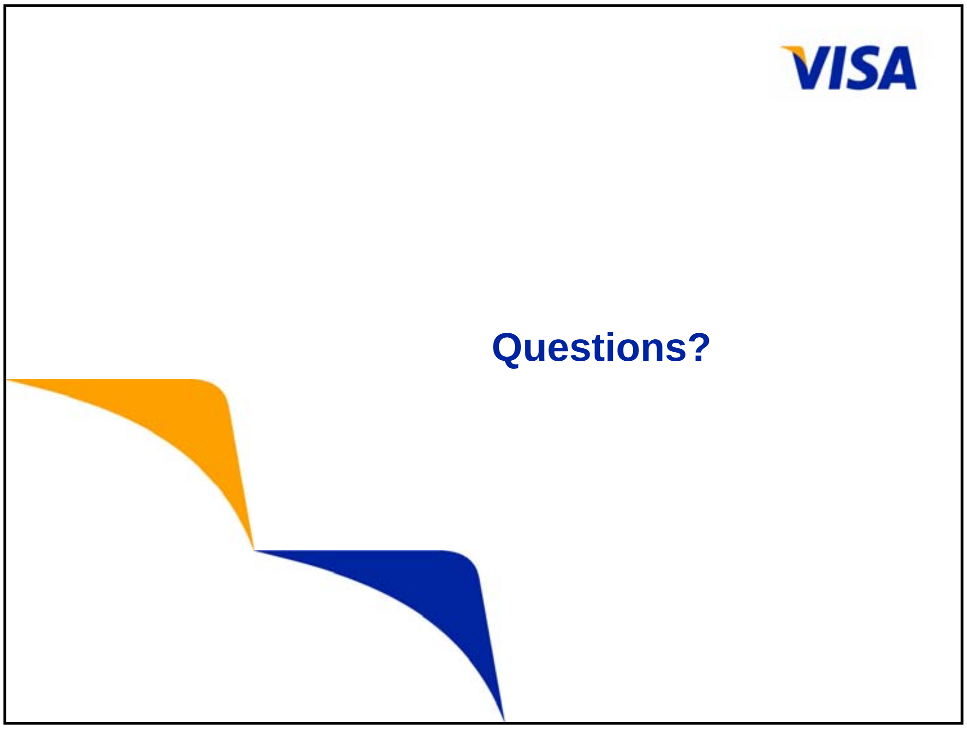
- Data Security Standard
- Security Audit Procedures
- PCI Data Security Standards
- PCI POS PIN-Entry Device Security Requirements
- PCI EPP PIN-Entry Device Security Requirements
- PCI Approved PIN Entry Devices List
- Payment Application Data Security Standards
- List of Validated Payment Applications
- Glossary of Terms

www.pcisecuritystandards.org

Visa CISP

- Archive of Data Security Alerts, bulletins and webinars
- What To Do If Compromised and Responding to a Data Breach guides
- Qualified Incident Response Assessor List
- Global List of Validated Service Providers
- Payment Application Best Practices
- PCI PIN Security Requirements
- PCI PIN Entry Device Testing and Approval Program Guide

www.visa.com/cisp
www.visa.com/pin



Questions?