



AIS Webinar

Payment Application Security

Hap Huynh
Business Leader
Visa Inc.

1 April 2009

Agenda



- Security Environment
- Payment Application Security Overview
- Questions and Comments

Security Environment



Data Security is a Hot Media Topic



Companies Say Security Breach Could Destroy Their Business

April 24, 2007

One-third of companies said in a recent poll security breach could put their company out of business, according to a report from McAfee.

The security company unveiled a study Tuesday of respondents said they believe a major data-incident involving accidental or malicious distribution of data could put them out of business. The study, called based on a survey of more than 1,400 IT profes-

60 MINUTES

Hi-Tech Heist

How Hi-Tech Thieves Stole Millions Of Customer Financial Records

Nov. 25, 2007

Comments 57 | Page 1 of 1

VIDEOS PHOTOS



Hi-Tech Heist

Consumers often feel safer using their credit cards in stores than online, where hackers are notorious for stealing personal information. But is it really safer? Lesley Stahl reports. | Share

Answer Tips™ enabled ([what's this?](#))
(CBS) Do you think twice when typing in your credit card number online, but have no problem handing over your plastic card at a store? Well actually, you may have it backward. Your personal information may be more secure in cyberspace than at the mall down the road.

That's because it's easier for dot-coms to protect the data. And most stores in America underestimate how vulnerable they are.

As correspondent **Lesley Stahl** reports, it's becoming a big problem. The retail industry got a wake-up call earlier this year, when TJX, the parent company of T.J. Maxx and Marshalls, disclosed it had suffered the worst high history. Hackers raided system, taking off with And what we have learned prevented it.



Security Breach Costs Jump 30%

The price tag for recovering from a single security incident is now \$6.3 million.

By Deborah Gage
November 28, 2007

Cost of recovering from a single data breach now averages \$6.3 million—that's up 31 percent since 2006 and 60 percent since 2005, according to the Ponemon Institute's annual report.

THE WALL STREET JOURNAL

BREAKING THE CODE

How Credit-Card Data Went Out Wireless Door Biggest Known Theft Came from Retailer With Old, Weak Security

By JOSEPH PEREIRA

The biggest known theft of credit-card numbers in history began two summers ago outside a Marshalls discount clothing store near St. Paul, Minn. There, investigators now believe, hackers pointed a telescope-shaped antenna toward the store and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers. That helped them hack into the

what was going on. The hackers, who have not been found, downloaded at least 45.7 million credit- and debit-card numbers from about a year's worth of records, the company says. A person familiar with the firm's internal investigation says they may have grabbed as many as 200 million card numbers all told from four years' records. The previous record for card numbers exposed to thieves was 40 million. The TJX hackers also got personal information such as driver's license numbers, military identification and Social Security numbers of 451,000 customers -- data that could be used for identity theft. The company has apologized for its security lapse and has fixed it.



TJX data breach may involve 94 million credit card Estimate in court filings much higher than retailer

By Jon Swartz
October 25, 2007

SAN FRANCISCO — The massive computer data breach at may be worse than expected. At least 94 million Visa and MasterCard accounts — nearly double the previous estimate the retailer — could have been exposed, new court files say. The filings, which cite security officials at Visa and MasterCard are part of a lawsuit filed by several banks and banking associations against TJX and Fifth handled its card transactions, in related losses. The depositions say fraud-related \$68 million to \$83 million and \$1.2 billion in data from compromised cards.

The latest estimate is significant. It says the retailer may have exposed



NEWS BLOGS WINDOWS SECURITY MOBILITY INTERNET SOFTWARE IAS
News Center • Blog • Columns • Product Reviews • Current Print Issue • Read All Stories • All

Online Retailer Settles Charges That It Left Consumer Data Open To Hackers

The FTC said a company called "Life is good" lacked "reasonable and appropriate security for the sensitive consumer information stored on its computer network."

By K.C. Jones
InformationWeek
January 11, 2008 01:35 PM

An online retailer has settled with the Federal Trade Commission on charges it didn't protect consumer information and that its security failures allowed hackers to steal credit card information.

An FTC complaint states that the company, "Life is good," claimed in its privacy policy that it was committed to protecting consumer information and stored the information in a secure file used to tailor communications with consumers. The FTC said that "Life is good" lacked "reasonable and appropriate security for the sensitive consumer information stored on its computer network."

The FTC said the company stored the information, including credit card numbers, in a file that was not

- E-Mail
- Print
- Discuss
- Vote To
- Flag
- Subscribe
- News Site

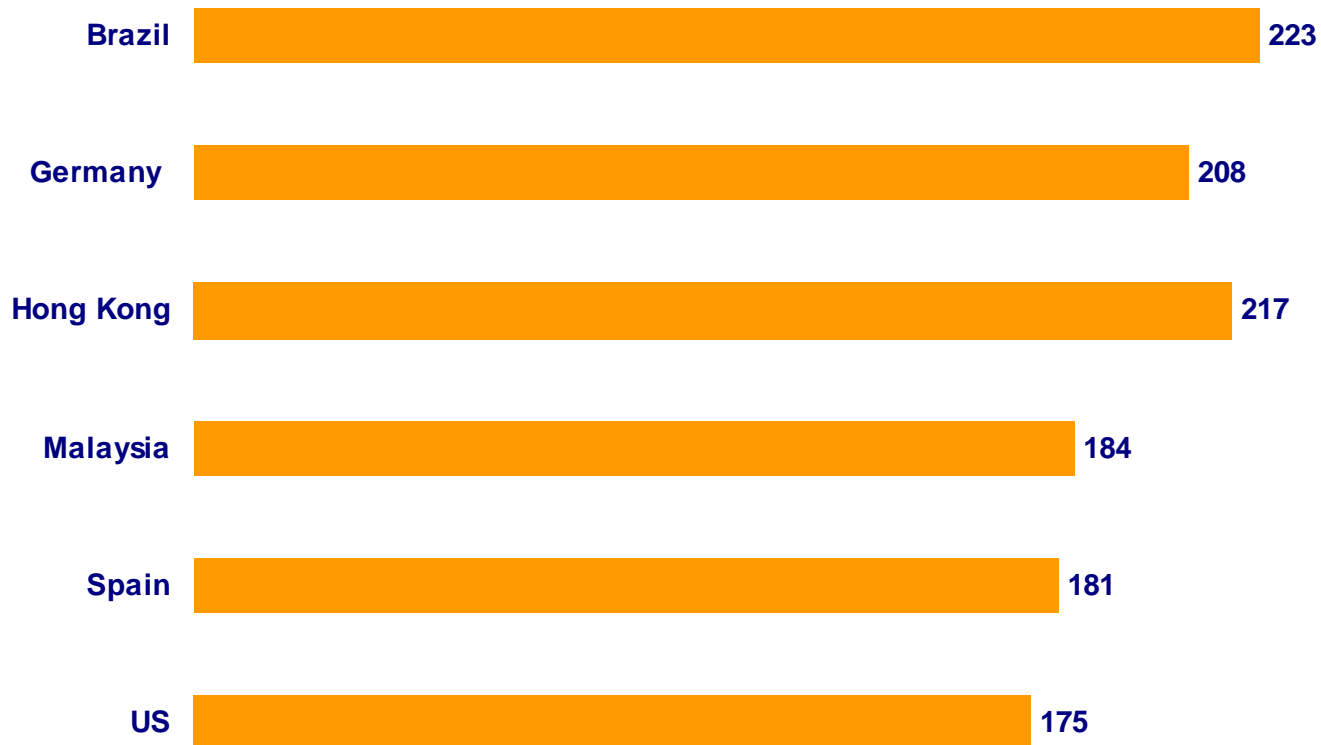
Security Environment



Fears about identity theft and financial fraud are top global concerns for consumers, according to the latest results of the Unisys Security Index.

- Identity theft is the primary security concern cited among respondents in nine out of 14 countries, while misuse of credit or debit card information ranks as the first or second greatest fear in 12 out of the 14 countries.

Countries that identified card fraud as a serious concern:



Source: Unisys Security Index, Unisys Inc., December 2008

Today's Targets



- **Hackers are attacking:**

- Brick-and-mortar merchants
- Issuers
- E-commerce merchants
- Processors and Agents



- **Hackers are looking for:**

- Software that stores sensitive cardholder data
- Personal information to perpetrate identity theft
- Track data and payment account numbers
- PINs



What are Criminals Doing?



- Stealing payment card information from retailers, agents, clients, ATMs and other sources with security vulnerabilities
- Organizing and selling stolen account information in online markets known as “Carder” sites:

“I sell the freshest DUMPS, they are mostly USA, some EU and Asia.”

“You can choose your favorite BINs from over 300...”

- Committing fraud attacks

Estimated market value of compromised accounts*

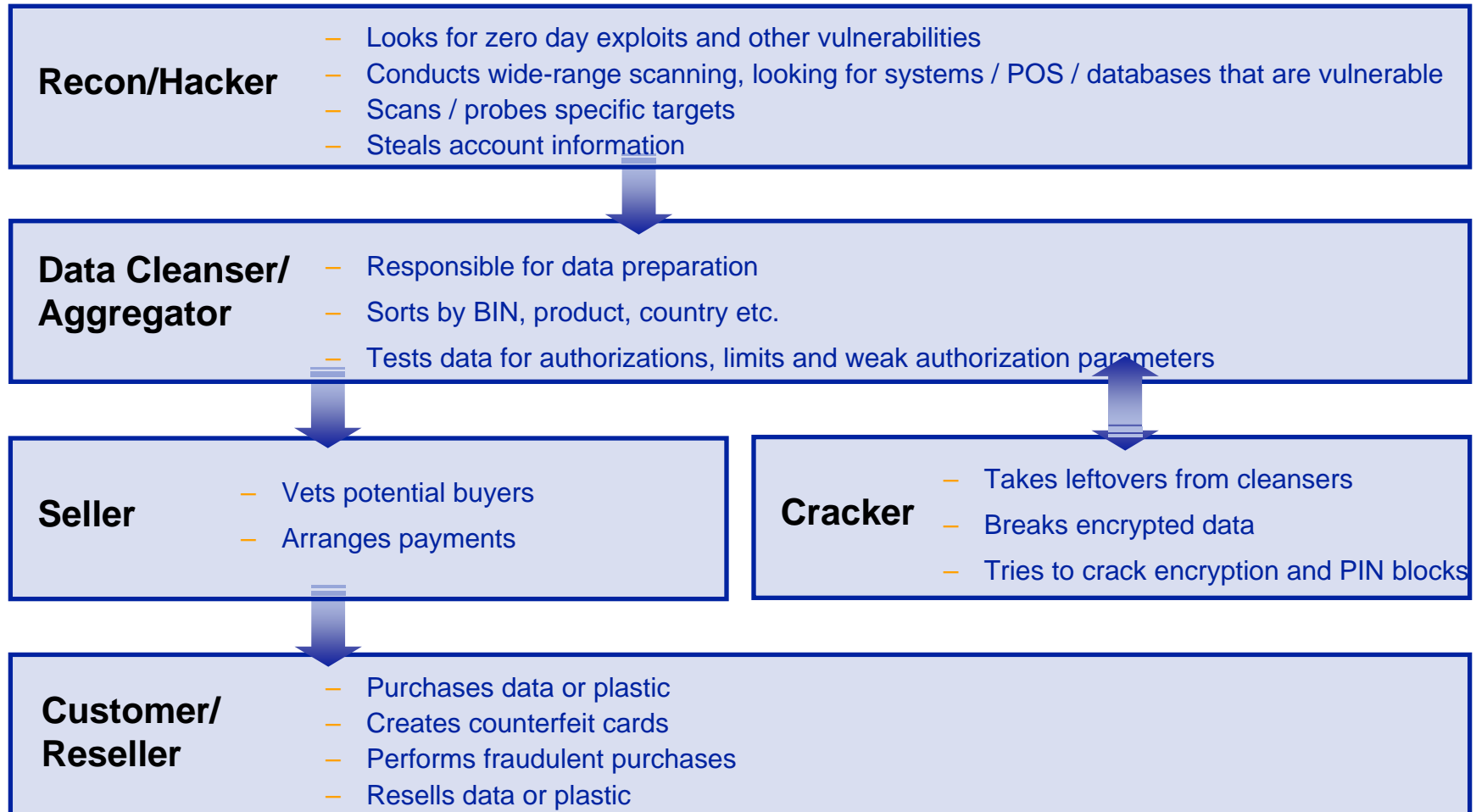
Account number and CVV2	Classic track data	Gold/Plat/Corp track data	Semi-finished blank plastic	Complete counterfeit Gold plastic	Track data and PIN
					
No Plastic	No Plastic	No Plastic	White-Plastic	Finished	Finished
\$1	\$15	\$30	\$80-\$100	\$250	Revenue Share

* Source: The United States Secret Service

Sophisticated and Well Organized



Organized crime uses business-like structure and separates duties...



Vulnerabilities Resulting in Security Breaches



Vulnerabilities



- Integrated Point of Sale (POS) systems connected directly to the Internet
- Insecure network configuration
- Insecure remote access configuration
- Use of default user ID and password
- Use of legacy operating system
- Lack of current patches
- No anti-virus protection
- Lack of logging and monitoring
- Malware

Impact of Data Compromises



- Notification/disclosure requirements
- Brand/reputation damage
- Loss of business/consumer confidence
- Financial liabilities
 - Compromised entity
 - Visa clients
- Litigation
- Government intervention/legislation

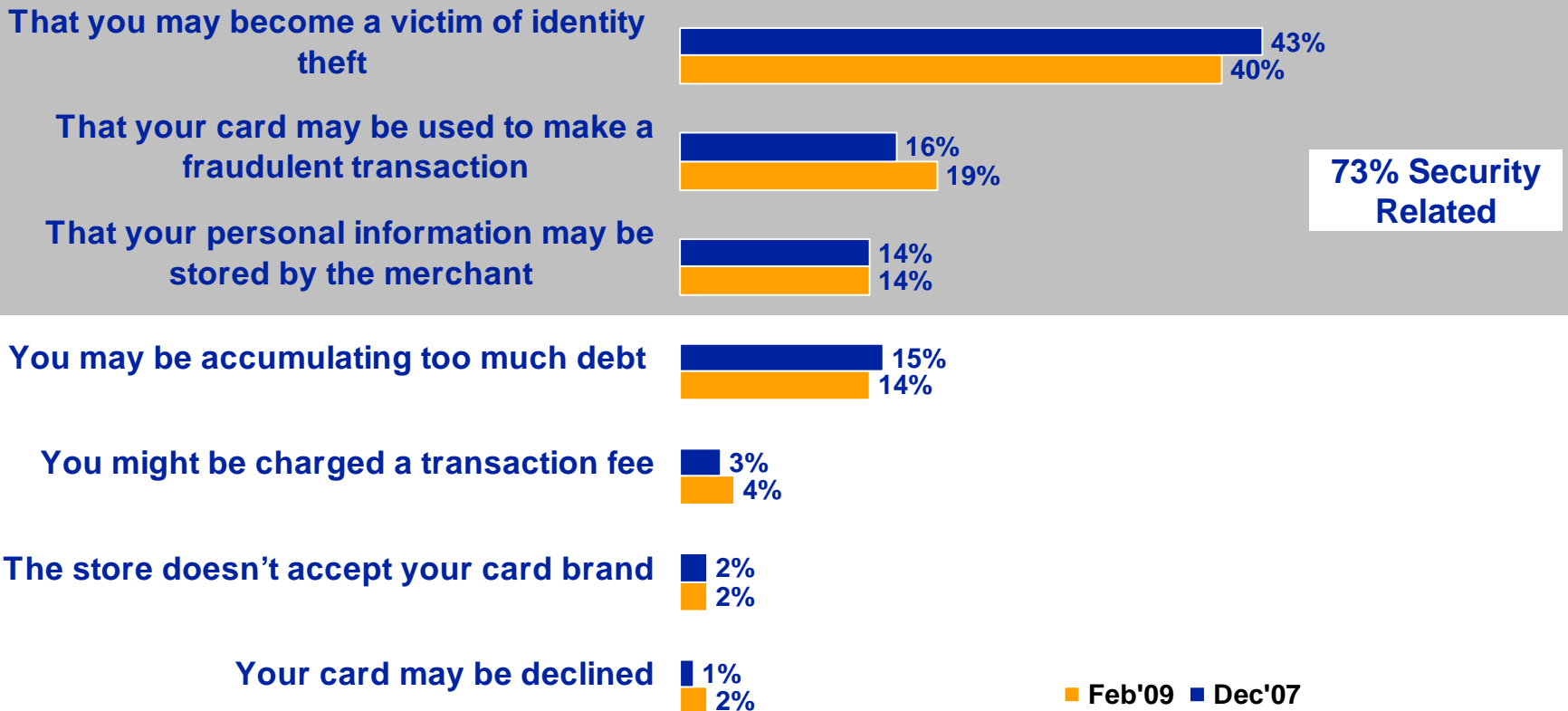
Cardholders ARE Concerned



» 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?



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

Incident Response Procedures

Immediate Action Steps



1. Isolate the compromised or suspected compromised systems
 - Take “offline” and store securely; Do not “rebuild” and continue to use
 - Ensure controls are in place to limit further damage
2. Determine the scope of the compromise or breach
 - Was cardholder data compromised?
 - Was sensitive authentication data or full track data included?
3. Contact your merchant bank or Visa within 24 hours
 - Visit AIS website and download the *What to Do If Compromised* document
4. Engage a Visa approved Qualified Incident Response Assessor
 - Assessor will assist in determining what type and how much data was compromised



Payment Application Security Overview



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 PABP-validated applications published at www.visa-asia.com/padss
 - 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 Data Security Standard



PCI SSC adopts PABP as the PA-DSS in April 2008

- **PCI SSC is responsible for:**
 - Maintaining and updating the PA-DSS and related documentation
 - Qualifying and training Payment Application Qualified Security Assessors (PA-QSAs) to perform PA-DSS assessments
 - Being a single point of repository for PA-DSS Reports of Validation (ROVs)
 - Performing quality assurance reviews of PA-DSS ROVs to confirm report consistency and quality
 - Listing PA-DSS validated payment applications on the PCI SSC website
- **Visa will continue to:**
 - Work with PCI SSC for potential enhancements to address emerging risks
 - Maintain a list of vulnerable payment applications that are known to store prohibited data
 - Promote payment applications that support PCI DSS compliance

Payment Application Data Security Standard



Payment applications that support PCI DSS compliance

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data
2. Protect stored cardholder data
3. Provide secure authentication features
4. Log payment application activity
5. Develop secure payment applications
6. Protect wireless transmissions
7. Test payment applications to address vulnerabilities
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote software updates
11. Facilitate secure remote access to payment application
12. Encrypt sensitive traffic over public networks
13. Encrypt all non-console administrative access
14. Maintain instructional documentation and training programs for customers, resellers, and integrators

Software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

Page 6, PA-DSS version 1.2

PA-DSS Applicability



Type of application	Does PA-DSS apply?
“Off-the-shelf” standard payment applications without much customization	YES
Software developed in modules	YES, applies to any module with payment functions
For hardware terminals	YES, unless terminal meets specific criteria
Software for only one, typically large customer, developed to customer’s specifications	NO, application is covered as part of customer’s Payment Card Industry Data Security Standard (PCI DSS) assessment
Software developed by merchant or service provider and used only in-house	NO, application is covered as part of merchant’s or service provider’s PCI DSS assessment
Supporting systems, for example, operating systems, databases, back-office systems, firewalls, routers, etc.	NO, these are NOT payment applications

Applicability for Hardware Terminals



- PA-DSS does not apply only if **all** of these items are true:
 - The terminal has no connections to any of the merchant's systems or networks
 - The terminal connects only to the acquirer or processor
 - The vendor provides secure remote:
 - Updates
 - Troubleshooting
 - Access
 - Maintenance
 - Sensitive authentication data is never stored after authorization

Cardholder Data: Important Concepts



	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number	YES	YES	YES
	Cardholder Name ¹	YES	YES ¹	NO
	Service Code ¹	YES	YES ¹	NO
	Expiration Date ¹	YES	YES ¹	NO
Sensitive Authentication Data ²	Full Magnetic Stripe Data ³	NO	N/A	N/A
	CAV2/CID/CVC2/CVV2	NO	N/A	N/A
	PIN/PIN Block	NO	N/A	N/A

1. *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*
2. *Do not store sensitive authentication data after authorization (even if encrypted).*
3. *Full track data from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.*

PA-DSS List of Validated Applications



- The PCI SSC has assumed the management of the list of validated payment applications at PCI SSC's website www.pcisecuritystandards.org
- PCI SSC has a process to transfer or “grandfather” payment applications validated against the PABP to the PA-DSS
 - Listed with an expiration indicating a mandatory date for revalidation under PA-DSS
 - PABP validation documents were to be provided to Visa by September 15, 2008 and transitioned to the PCI SSC list
 - If PABP validation was not accepted by November 30, 2008, the application would undergo the PCI SSC's PABP to PA-DSS Transition Procedures in order to be listed
- Visa is committed to working with the PCI SSC to ensure a successful transition of PABP to the PA-DSS

Cardholder data security is a shared responsibility and all participants must do their part to prevent fraud

- Create PA-DSS compliant applications that facilitate and do not prevent a customer's PCI DSS compliance
- Create a *PA-DSS Implementation Guide*, specific to each application and educate customers, resellers, and integrators on how to install and configure the payment application in a PCI DSS compliant manner
- Alert the PCI SSC and Visa if a vulnerability is identified for the payment application and of the recommended fix/patch to ensure the safety and soundness of the payment system

Integrator and Reseller's Role



- Must implement security requirements as instructed by the vendor's PA-DSS implementation guide and training
- When installing payment applications, protect customers by following strict security requirements, including but not limited to:
 - Remote management software should be disabled, removed and not used unless necessary and required (e.g., VNC, PCAnywhere, Remote Desktop, SSH, LogMeIn, WebEx, etc.)
 - If necessary, ensure appropriate security controls are implemented to prevent unauthorized access
 - Do not use system default settings and do not re-use the same usernames or passwords for payment applications or any system across multiple customers
 - Advise customers to implement a properly-configured firewall to protect the payment environment from unauthorized access
 - Instruct customers to maintain the latest security patches for the payment application, including the operating system and other necessary software

Reference Tools



PCI SSC

- PCI Data Security Standard
- PIN Entry Devices Program
- Payment Application Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaires
- Security Scanning Procedures
- Qualified Security Assessor List
- Approved Scan Vendor List
- Glossary of Terms

www.pcisecuritystandards.org

Visa AIS

- What To Do If Compromised guide
- List of PCI DSS-Compliant Service Providers (Registry of Service Providers)
- List of PABP-Validated Payment Applications

www.visa-asia.com/secured

www.visa-asia.com/padss

vpssais@visa.com