FIFTH THIRD
PROCESSING SOLUTIONS

Complying with PCI (DSS)
&
All the Moving Parts

Presented By:

Robert L. Day, Vice President, Merchant Processing

The information presented 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 Bank, or under the Operating Regulations of any credit card or debit card association.

Types of Risk

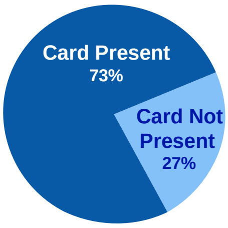
FIFTH THIRD
PROCESSING SOLUTIONS

- Operational Risk
  - Normal fraud risk associated with individual transactions
  - Can often be prevented by operational best practices
- Systemic Risk
  - Primarily Risk associated with large scale data breaches
  - Increasingly sensitive due to PR impact and potential for civil litigation
  - Often associated with organized crime and sophisticated IT “break ins”
  - PCI (Payment Card Industry Data Security Standards) meant to address major challenges

FIFTH THIRD
PROCESSING SOLUTIONS

Card Not Present vs. Card Present

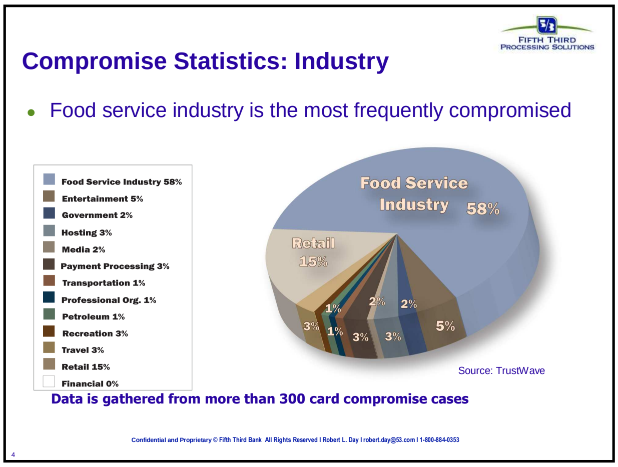
Compromise Statistics



Three out of four cases occur in a traditional brick and mortar environment.

Card-present merchants are not aware of these risks!

Source: TrustWave



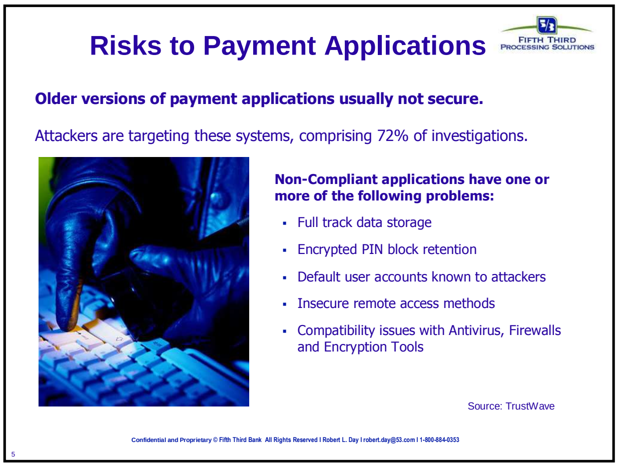
Compromise Statistics: Industry

- Food service industry is the most frequently compromised

- ▨ Food Service Industry 58%
- ▨ Entertainment 5%
- ▨ Government 2%
- ▨ Hosting 3%
- ▨ Media 2%
- ▨ Payment Processing 3%
- ▨ Transportation 1%
- ▨ Professional Org. 1%
- ▨ Petroleum 1%
- ▨ Recreation 3%
- ▨ Travel 3%
- ▨ Retail 15%
- □ Financial 0%

Source: TrustWave

Data is gathered from more than 300 card compromise cases



Risks to Payment Applications

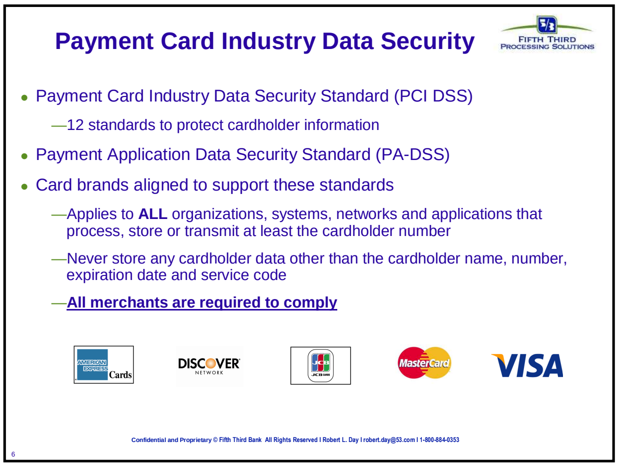
Older versions of payment applications usually not secure.

Attackers are targeting these systems, comprising 72% of investigations.

Non-Compliant applications have one or more of the following problems:

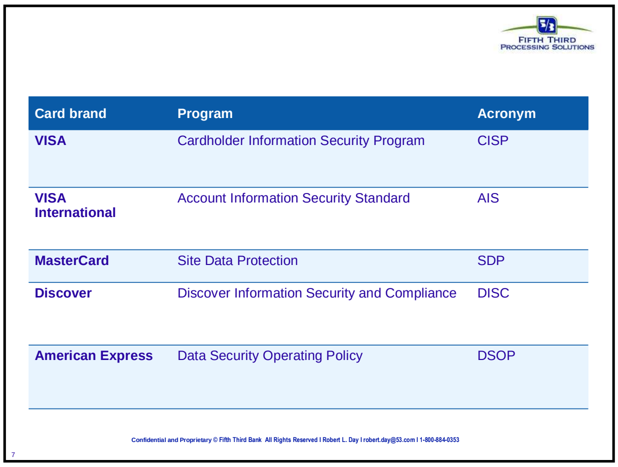
- Full track data storage
- Encrypted PIN block retention
- Default user accounts known to attackers
- Insecure remote access methods
- Compatibility issues with Antivirus, Firewalls and Encryption Tools

Source: TrustWave



Payment Card Industry Data Security

- Payment Card Industry Data Security Standard (PCI DSS)
  - —12 standards to protect cardholder information
- Payment Application Data Security Standard (PA-DSS)
- Card brands 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**

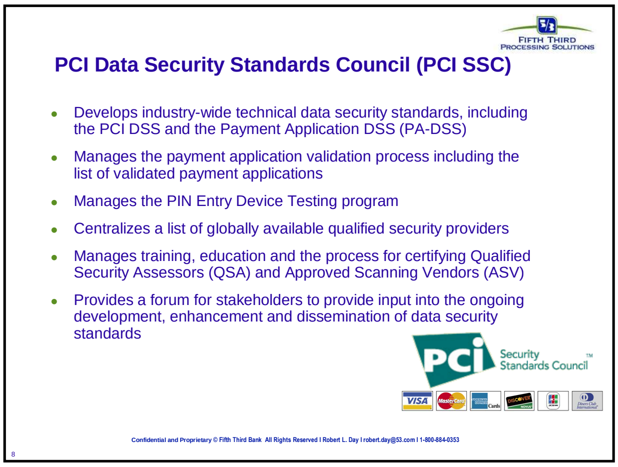


FIFTH THIRD PROCESSING SOLUTIONS

Card brand	Program	Acronym
VISA	Cardholder Information Security Program	CISP
VISA International	Account Information Security Standard	AIS
MasterCard	Site Data Protection	SDP
Discover	Discover Information Security and Compliance	DISC
American Express	Data Security Operating Policy	DSOP

Confidential and Proprietary © Fifth Third Bank All Rights Reserved l Robert L. Day l robert.day@53.com l 1-800-884-0353

7



FIFTH THIRD PROCESSING SOLUTIONS

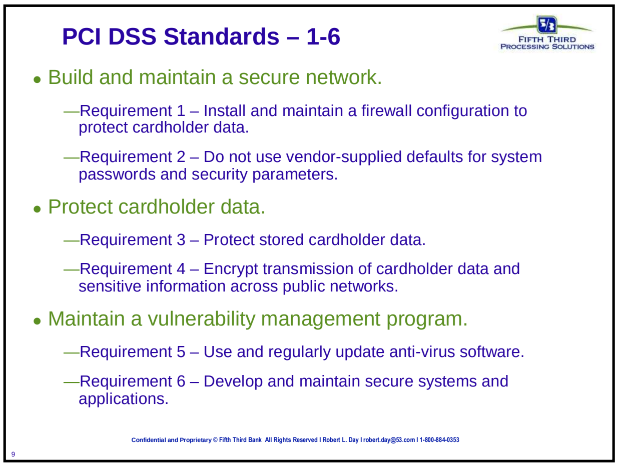
PCI Data Security Standards Council (PCI SSC)

- Develops industry-wide technical data security standards, including the PCI DSS and the Payment Application DSS (PA-DSS)
- Manages the payment application validation process including the list of validated payment applications
- Manages the PIN Entry Device Testing program
- Centralizes a list of globally available qualified security providers
- Manages training, education and the process for certifying Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV)
- Provides a forum for stakeholders to provide input into the ongoing development, enhancement and dissemination of data security standards

PCI Security Standards Council™

Confidential and Proprietary © Fifth Third Bank All Rights Reserved l Robert L. Day l robert.day@53.com l 1-800-884-0353

8



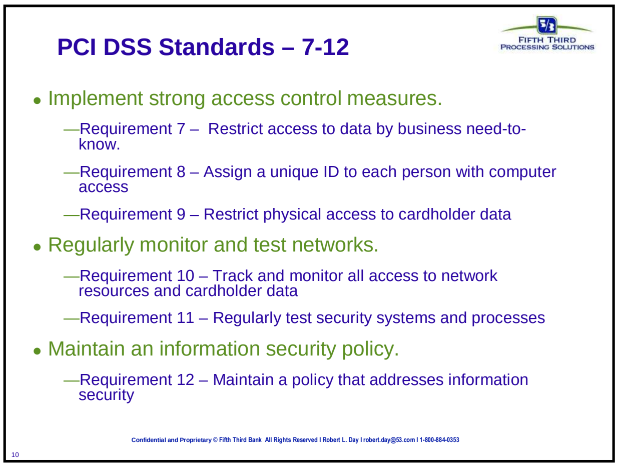
FIFTH THIRD PROCESSING SOLUTIONS

PCI DSS Standards – 1-6

- 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.

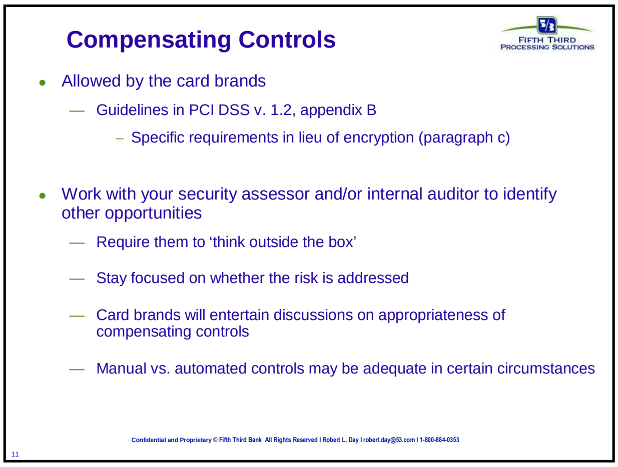
Confidential and Proprietary © Fifth Third Bank All Rights Reserved l Robert L. Day l robert.day@53.com l 1-800-884-0353

9



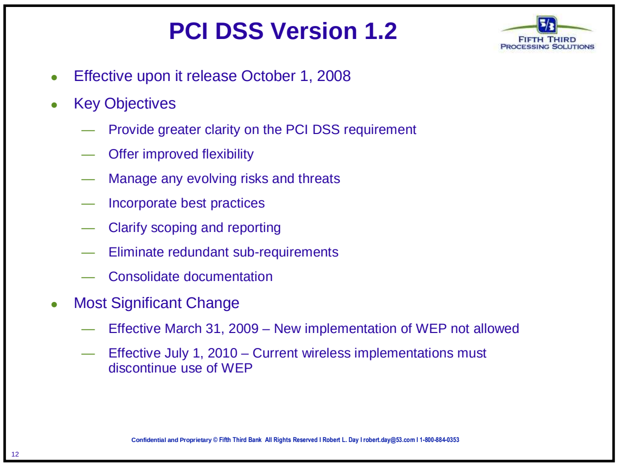
PCI DSS Standards – 7-12

- Implement strong access control measures.
  - —Requirement 7 – Restrict access to 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



Compensating Controls

- Allowed by the card brands
  - — Guidelines in PCI DSS v. 1.2, appendix B
    - – Specific requirements in lieu of encryption (paragraph c)
- Work with your security assessor and/or internal auditor to identify other opportunities
  - — Require them to 'think outside the box'
  - — Stay focused on whether the risk is addressed
  - — Card brands will entertain discussions on appropriateness of compensating controls
  - — Manual vs. automated controls may be adequate in certain circumstances



PCI DSS Version 1.2

- Effective upon it release October 1, 2008
- Key Objectives
  - — 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
  - — Consolidate documentation
- Most Significant Change
  - — Effective March 31, 2009 – New implementation of WEP not allowed
  - — Effective July 1, 2010 – Current wireless implementations must discontinue use of WEP

Merchant Levels	Validation Actions		
Merchant Level Criteria	***On Site Security Audit***	***Self – Assessment Questionnaire***	***Network Vulnerability Scans***
Level 1 · **At least 6 million transactions annually from any acceptance channel with one card brand** · **Any merchant who has experienced a card data compromise** · **Any merchant that a card brand, at its sole discretion, determines should meet the level 1 merchant validation requirement**	**Report on Compliance (ROC) (Submitted to Acquirer Annually)**	**Not Applicable**	**Required Quarterly**
Level 2 · **1 million to 6 million transactions annually from any acceptance channel with one card brand**	**Not Applicable**	**Submitted to Acquirer Annually**	**Required Quarterly**
Level 3 · **20k to 1 million ecommerce transactions annually with one card brand**	**Not Applicable**	**Submitted to Acquirer Annually**	**Required Quarterly**
Level 4 · **Less than 20k ecommerce annually with one card brand; or** · **Less than 1 million transactions from any acceptance channel annually with one card brand**	**Not Applicable**	**Best Practice Annually (submission to acquirer not mandatory)**	**Required Quarterly (submission to acquirer not mandatory)**

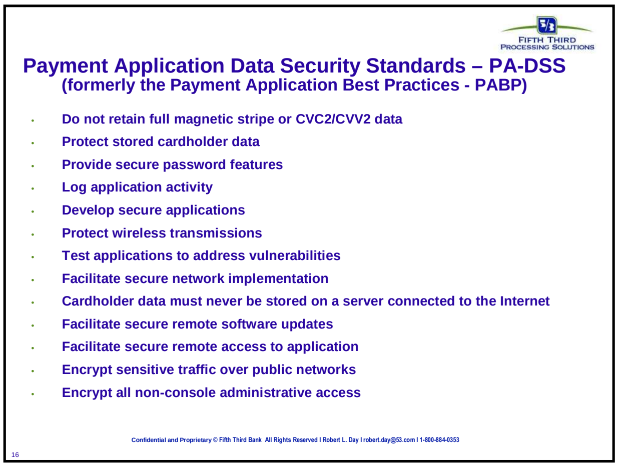
Self-Assessment Questionnaire (SAQ)

- Four different versions to tailor to different types of merchants
  - **SAQ A:** Applies to card-not-present merchants who have outsourced all cardholder data storage, processing and transmission.
  - **SAQ B:** Created to address requirements pertinent to merchants who process cardholder data via imprint machines or standalone dial-up terminals only.
  - **SAQ C:** Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet, but are not storing cardholder data electronically.
  - **SAQ D:** Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by A, B or C.
- **IMPORTANT** – Although Fifth Third Processing Solutions can provide guidance, the merchant is in the best position to determine which SAQ applies to their processing environment.

Service Provider Validation Levels and Requirements

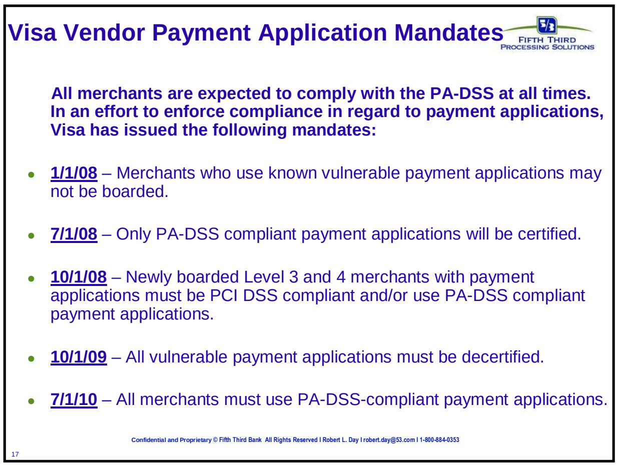
Service Provider Levels	Validation Actions		
Service Provider Level Criteria	***On Site Security Audit***	***Self – Assessment Questionnaire***	***Network Vulnerability Scans***
Level 1 · **Any processor directly connected to a Visa or MasterCard or any service provider that stores, processes and/or transmits over 300,000 transactions per year**	**Report on Compliance (ROC) (Required Annually)**	**Not Applicable**	**Required Quarterly**
Level 2** · **Any service provider that stores, processes and/or transmits less than 300,000 transactions per year**	**Not Applicable**	**Required Annually**	**Required Quarterly**

**Effective February 1, 2009, Level 2 service providers will no longer be 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 Application Data Security Standards – PA-DSS
(formerly the Payment Application Best Practices - PABP)

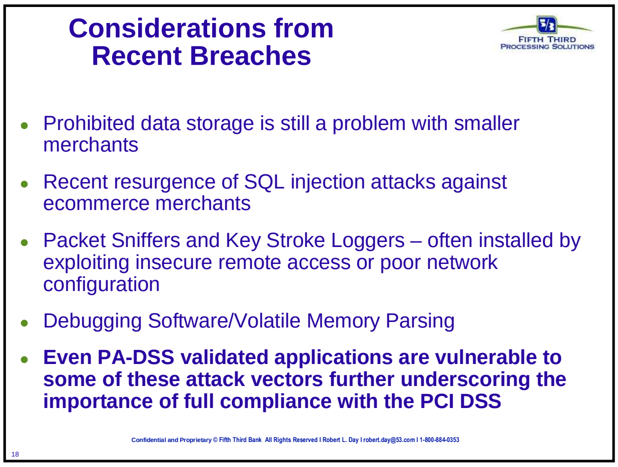
- **Do not retain full magnetic stripe or CVC2/CVV2 data**
- **Protect stored cardholder data**
- **Provide secure password features**
- **Log application activity**
- **Develop secure applications**
- **Protect wireless transmissions**
- **Test applications to address vulnerabilities**
- **Facilitate 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**



Visa Vendor Payment Application Mandates

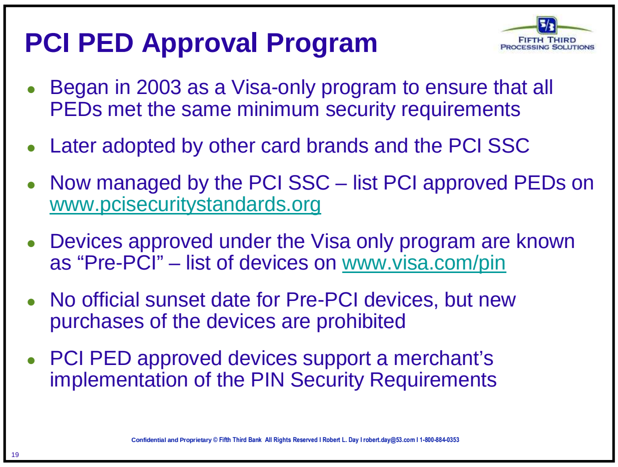
All merchants are expected to comply with the PA-DSS at all times. In an effort to enforce compliance in regard to payment applications, Visa has issued the following mandates:

- **1/1/08** – Merchants who use known vulnerable payment applications may not be boarded.
- **7/1/08** – Only PA-DSS compliant payment applications will be certified.
- **10/1/08** – Newly boarded Level 3 and 4 merchants with payment applications must be PCI DSS compliant and/or use PA-DSS compliant payment applications.
- **10/1/09** – All vulnerable payment applications must be decertified.
- **7/1/10** – All merchants must use PA-DSS-compliant payment applications.



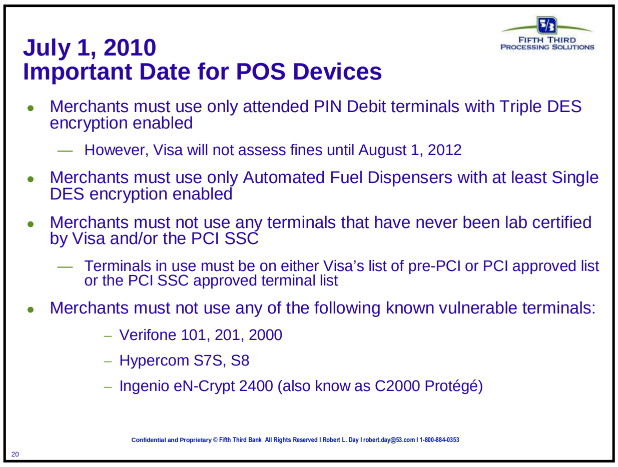
Considerations from Recent Breaches

- Prohibited data storage is still a problem with smaller merchants
- Recent resurgence of SQL injection attacks against ecommerce merchants
- Packet Sniffers and Key Stroke Loggers – often installed by exploiting insecure remote access or poor network configuration
- Debugging Software/Volatile Memory Parsing
- **Even PA-DSS validated applications are vulnerable to some of these attack vectors further underscoring the importance of full compliance with the PCI DSS**



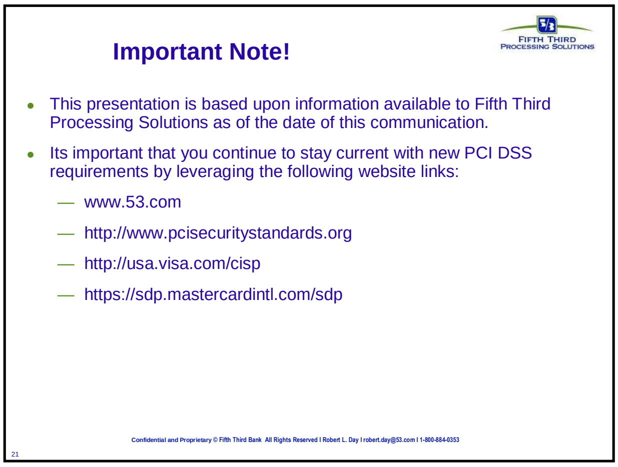
PCI PED Approval Program

- Began in 2003 as a Visa-only program to ensure that all PEDs met the same minimum security requirements
- Later adopted by other card brands and the PCI SSC
- Now managed by the PCI SSC – list PCI approved PEDs on www.pcisecuritystandards.org
- Devices approved under the Visa only program are known as “Pre-PCI” – list of devices on www.visa.com/pin
- No official sunset date for Pre-PCI devices, but new purchases of the devices are prohibited
- PCI PED approved devices support a merchant’s implementation of the PIN Security Requirements



July 1, 2010
Important Date for POS Devices

- Merchants must use only attended PIN Debit terminals with Triple DES encryption enabled
  - — However, Visa will not assess fines until August 1, 2012
- Merchants must use only Automated Fuel Dispensers with at least Single DES encryption enabled
- Merchants must not use any terminals that have never been lab certified by Visa and/or the PCI SSC
  - — Terminals in use must be on either Visa’s list of pre-PCI or PCI approved list or the PCI SSC approved terminal list
- Merchants must not use any of the following known vulnerable terminals:
  - – Verifone 101, 201, 2000
  - – Hypercom S7S, S8
  - – Ingenio eN-Crypt 2400 (also know as C2000 Protégé)



Important Note!

- 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.53.com
  - — http://www.pcisecuritystandards.org
  - — http://usa.visa.com/cisp
  - — https://sdp.mastercardintl.com/sdp

Fifth Third Processing Solutions

Questions?

The information presented 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 Bank, or under the Operating Regulations of any credit card or debit card association.