Payment Processing Threats Impacting Grocery Store Merchants

April 2013

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Visa's Multi-Layered Strategy

Mitigating fraud through continuous leadership, coordination and investment

Maintaining and enhancing stakeholder trust in Visa as the most secure way to pay and be paid

Agenda

- Common Security Deficiencies
- Intruder Footprints
- Attack Prevention
- PED Tampering Cases
- Preventive Measures for PED Tampering
- Authentication Roadmap
- What To Do If Compromised
- Questions

PCI DSS Requirements

Commonly Identified Security Deficiencies

	Vulnerability	Applicable Requirement
Network Security	Default or no firewall / router rules	Requirement 1
	No DMZ	Requirement 1
	Insecure remote access, no 2-factor authentication	Requirement 8
Host-based Security	Insecure operating systems and databases	Requirement 6
	No patching	Requirement 6
	No or outdated anti-virus signatures	Requirement 5
	No password management or access control lists (ACL)	Requirement 7
	Use of default or shared usernames and passwords	Requirement 2
	No system logging	Requirement 10
	No file integrity monitoring	Requirement 10
Application Security	SQL injection / other web-based exploits	Requirement 6
	No secure coding, independent code review, or penetration testing process in place	Requirement 6
Incident Response	No incident response plan	Requirement 12
General	No monitoring of systems, logs, access control, etc.	Requirement 10

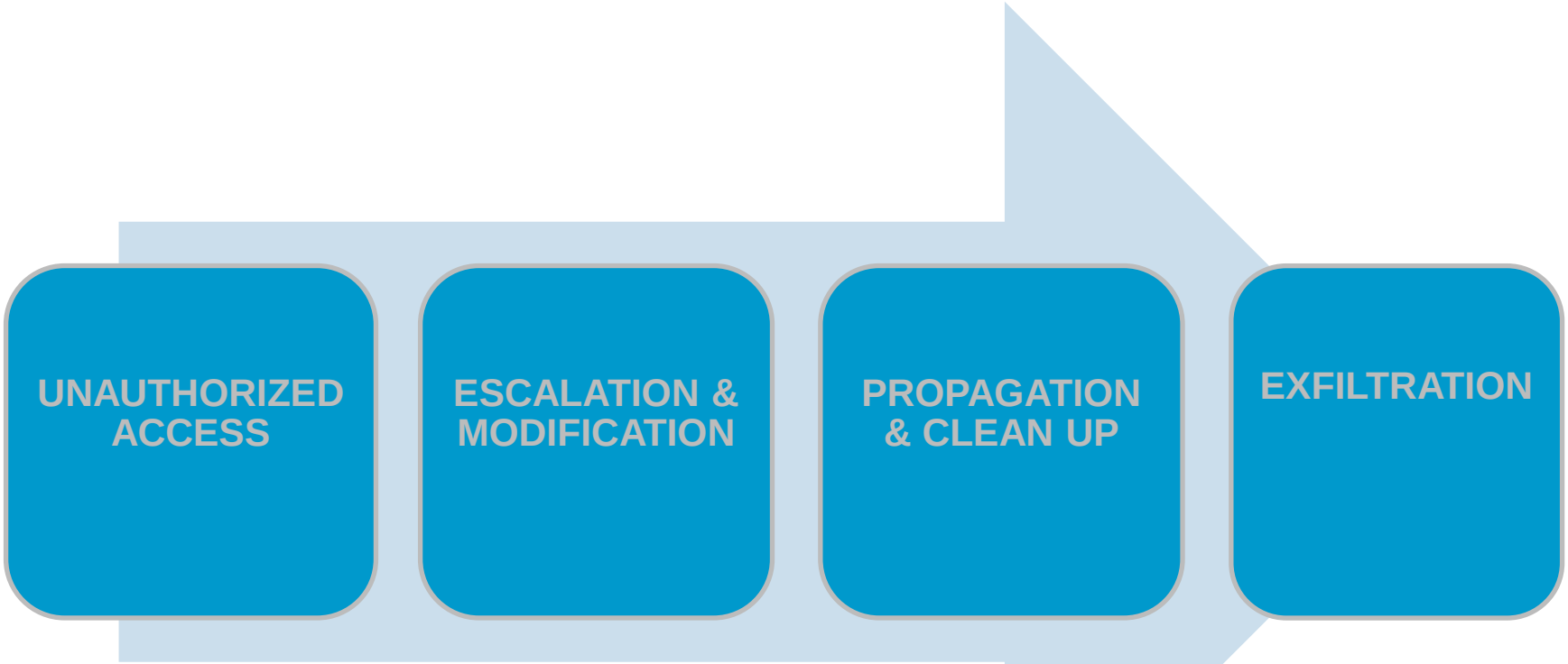
- **Lack of network segmentation has contributed to multiple location breaches**

Source: Data breach forensic reports

Intruder Footprints

- **Malicious software**
  - Memory parser malware that hooks on POS binaries
- **FIM with no password**
  - Intruder whitelisted malware executable to prevent detection
- **Malware propagation**
  - Used existing script to deploy malware at individual locations
- **Auto-login enabled**
  - Credentials stored in the clear-text on Windows registry
- **Anti-forensic employed**
  - Logs deleted
  - Encrypted output file using strong encryption

The Attack Flow



Target of convenience. VPN credentials targeted (company users or third-party)

Root level access on corporate network. Map out internal networks, target DCs, POS system and scripts. Modification to FIM.

Using existing scripts and hard-coded password on POS, propagate malware to other store locations. Install other tools to delete hacker activities.

Malware created files are encrypted and exfiltrated out of network. Method of exfiltration using existing ports (e.g., 443 with no filtering).

Vulnerabilities

- **No two-factor authentication on user access**
  - VPN
  - Remote access
- **Lack of segmentation from corporate to store locations**
- **Outbound firewall configuration allow connection to any IP on the Internet**
- **Domain controllers targeted**
- **Excessive permissions**
- **Insecure POS systems (FIM with no password, auto-login)**
- **No incident response in place to detect malicious activity sooner**

Indicators of a Compromise (IOC)

File Name	Purpose	File Size (bytes)	MD5 Hash
rtcli.dll	Information stealer / downloader	118272	4bd819d9e75e4e8ecf1a9599f44af12a
mstdc.exe	Backdoor	64512	57703973ff74503376a650224aa43dfa
mstdc.bak	Backdoor	106496	67ed156e118b9aa65ed414a79633a3d4
msaudit.dll	Memory parser malware	97792	27bfffa7d034a94b79d3e6ffdda50084
mn32.exe	Prefetch file indicating execution of the malicious code	179200	89a8844c1214e7fc977f026be675a92a
si.vbs	Visual basic script used by hacker to deploy malware onto POS systems	2772	40efe7632b01116eefaba438c9bcee34
sd32.exe	Anti-forensic utility to remove malware from POS systems	134000	9c3a1d3829c7a46d42d5a19fe05197f3
TcpAdaptorService.exe	Memory parser malware	73728	cfee737692e65e0b2a358748a39e3bee
		118784	85f94d85cfeff32fa18d55491e355d2b
Osql.exe, svchosts.exe	Tool used in conjunction with TcpAdaptorService.exe to send track data to bad IP	122880	4b9b36800db395d8a95f331c4608e947
oposwin.exe	Memory parser malware	245760	3446cd1f4bee2890afc2e8b9e9eb76a2
svcmon.exe	Memory parser malware	253952	0fff972080248406103f2093b6892134

Indicators of a Compromise (IOC)

File Name	Purpose	File Size (bytes)	MD5 Hash
nYmTxGSJhLLFfagQ.bat	Batch file used to whitelist malware executables on FIM	74	eae4718ea5a860cc372b5728e96af656
tbcsvc.exe	Performs cryptographic operations	293583	1aa662d329cc7c51d2e9176024fedee8
mssec.exe	Attempts outbound communication via port 443	135242	d7e5e85ccb6c71a39b99a9228313cc33
msproc.exe	Malicious unknown purpose	184128	2e567707730ed2c76b162a97dcf28c05
mpw.exe	Custom password dumping utility based on pwdump6	151552	03462BD6A6008205264995BDEFEB027C
msrclr42.dll	Part of mpw.exe package	77824	4373855E29C40458552AB0463C3D4C4B
mstdc.exe	Apocalipto backdoor	64,512	57703973FF74503376A650224AA43DFA
N/A	Binary payload for apocalipto backdoor	49,664	9A460FA6F9F56415E3BA23667718039D
MSTDC.BAK	Apocalipto backdoor	106,496	67ED156E118B9AA65ED414A79633A3D4
N/A	Binary payload for apocalipto backdoor	49,152	751363A08365925B7C7A4ED8755B090D
rtcli.dll	Downloader and Internet Explorer information stealer	118,272	4BD819D9E75E4E8ECF1A9599F44AF12A
mstsk.exe	DNS-based backdoor	45,568	43D77242910BABE51CB12C25371CC5AC

Attack Prevention - Overview

- Network Security
- POS Security
- Administrator Accounts
- Incident Response

Network Security

- Apply a defense-in-depth approach to protect the most critical resources on your network, including POS systems
- Limit access to only network ports and services that are necessary to perform desired business functions
- Segregate the payment processing network from other non-payment processing networks
- Users with administrative access should use two-factor authentication when accessing the payment processing networks
- Apply access controls on the router configuration to limit unauthorized traffic to the payment processing networks
- Implement strict inbound and outbound filtering on the firewall rule sets

POS Security

- Implement P2P PEDs
  - EMV capability
  - Secure Reading and Exchange of Data (SRED)
  - Hardware-based encryption
- Install PA-DSS compliant payment applications
- Deploy the latest version of operating system and ensure it is up-to-date with security patches, anti-virus, FIM, HIDS
- Perform a binary or checksum comparison
- Disable unnecessary ports and services, null sessions, default users and guests
- Enable logging of events and make sure there is a process to monitor logs on a daily basis

POS Security - Continued

- Implement least privileges and access controls lists (ACLs) on users and applications on the system
- Implement a security policy that includes operating system security configuration. The policy should include the following:
  - Security installation guide
  - Password management guide to manage users on the system
  - Mechanism to ensure consistent security baseline on critical systems

Administrative Accounts

- Use two-factor authentication when accessing the payment processing networks
- Limit administrative privileges on applications
- Periodically review systems (local and domain controllers) for unknown and dormant users.
- Apply same security on database users

Incident Response

- Deploy Security Information and Event Management (SIEM)
- Review logs and offload to a dedicated server (e.g., syslog and in a secure location where hackers can’t tamper with logs)
- Invest in an incident response team
  - Knowledge
  - Training
  - Certification
- Test your incident response plan
- Implement IOC signatures on your solution

PIN Entry Device (PED) Tampering Cases

- **Number of PED tampering cases increasing**
  - Criminals target merchants with certain PED models
    - Attacks on older vulnerable PEDs and newer PED models
    - Wireless models becoming a target
  - Small and large merchants, often multiple stores, targeted
    - Swap out PEDs with altered PEDs
- **Attacks are more sophisticated & technically advanced**
  - Recent attacks involved *VeriFone Everest and Ingenico i3070 PED* models
  - However new PED models are being targeted
- **Evidence of technology being exported globally**

PED Tampering usually involves:

- A second mag stripe reader or connection to existing reader
- Additional circuit board(s)
- Keypad membrane
- Bluetooth device
- Flash memory chip or drive

Preventive Measures for PED Tampering

- Replace vulnerable PEDs as quickly as possible
- Train staff to regularly inspect PEDs visually to identify anything abnormal such as
  - Missing or altered seals or screws
  - Extraneous wiring, holes in the device, or the addition of labels
  - Overlay material used to mask damage from tampering
- Ensure PEDs are physically secured / locked down to counters

Review Visa's Terminal Usage Best Practices:

"Point-of-Sale Terminal Tampering Is a Crime …and You Can Stop It"

www.visa.com/cisp

VISA

Point-of-Sale Terminal Tampering Is a Crime . . . and You Can Stop It

Increasingly, criminals with sophisticated tools are actively targeting vulnerable merchant point-of-sale (POS) terminals to steal payment card data and PINs for counterfeit fraud purposes. That's the bad news! The good news is that all acquirers, merchants, and processors can take appropriate steps to eliminate POS terminal weaknesses and the possibility of POS tampering.

Criminal gangs worldwide are illegally accessing active POS terminals and modifying them by inserting an undetectable

Compromised PIN-Entry Device List

- Review PEDs in use to identify any known vulnerable devices
- *Visa Bulletin* available on www.visa.com/cisp
- Take precautions to secure all PEDs in use…or in storage

VISA

Visa Security Alert

16 November 2012

Help Protect Cardholder Data From Attacks on PIN Entry Devices

U.S. | Acquirers, Processors, Merchants, Agents

To promote the security and integrity of the payment system, Visa is reminding clients, merchants and payment system participants of their responsibility to protect cardholder account and PIN data.

Criminals trying to obtain cardholder account and PIN data at the point of sale (POS) frequently target PIN Entry Devices (PEDs) that are known to be vulnerable. Last year, Visa alerted clients that the VeriFone Everest Plus PED was used in tampering and skimming attacks.

Evidence indicates that these devices were removed from the point of sale and replaced with modified devices designed to capture magnetic stripe card and PIN data, which was then transmitted to criminals wirelessly. Surveillance footage shows that the suspects were able to remove a PED and install a modified device in less than one minute.

Recommended Mitigation Strategies

All VeriFone Everest Plus users are encouraged to upgrade to systems that feature the most up-to-date security

Merchant Best Practices to Prevent Skimming

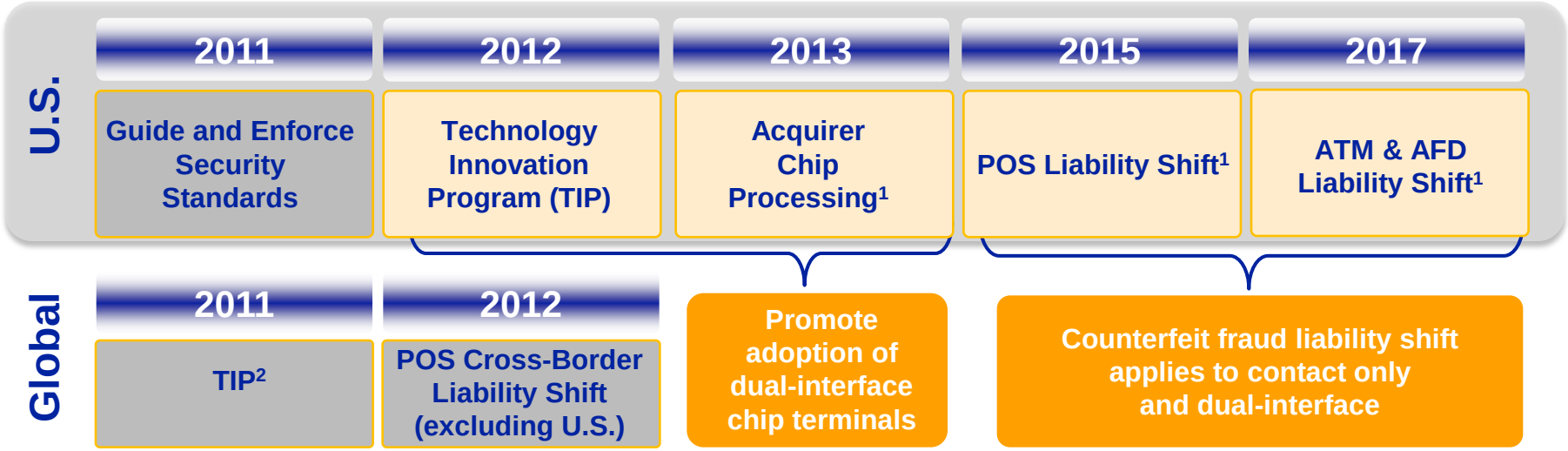
1. Implement a terminal authentication system to detect internal serial number or connectivity changes
2. Secure terminals / PEDs to counters to prevent removal and secure cable connections
3. Inspect and secure PEDs within unattended self checkout lanes
4. Use terminal asset tracking procedures for devices deployed, stored and shipped
5. Secure stored PEDs and validate inventory against asset records

- www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf

Authentication Roadmap

U.S. EMV chip roadmap supports three primary opportunities

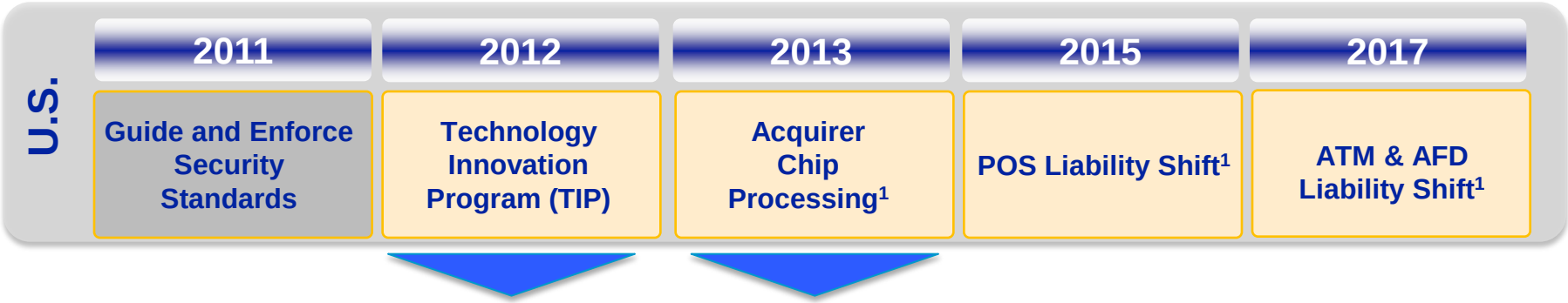
1. **Build framework** for mobile payments and future innovation leveraging EMV infrastructure for both contact and contactless payments
2. **Support interoperability and improve authorization decisions** as EMV adoption continues to grow worldwide
3. **Reduce reliance on static data** and incidence of counterfeit fraud



[1]Dates and/or timelines may change
[2]Visa Europe announced a corresponding program

Encouraging Terminal Adoption

Building processing infrastructure for chip and mobile acceptance



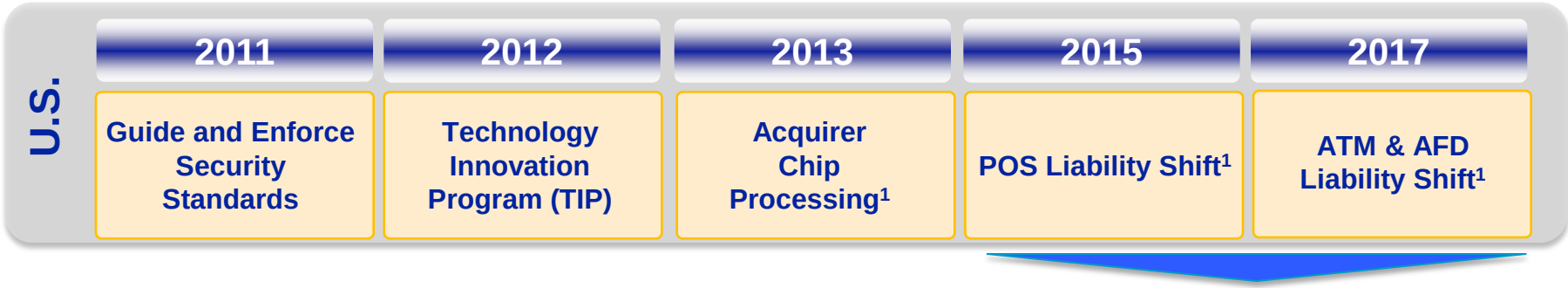
- TIP recognizes and incents merchant chip investments, while maintaining expectation for merchants to protect cardholder data
- Participation results in cost savings by waiving the annual PCI DSS validation exercise
- Eligible merchants must meet **all** of the minimum qualification criteria
  - PCI DSS compliance or remediation plan
  - No storage of prohibited data
  - At least 75 percent of merchants' transactions must originate from dual interface chip terminals and can process end-to-end chip transactions
  - No involvement in cardholder data breach[2]

- Mandate for U.S. acquirer processors and sub-processor service providers to support chip processing, effective April 1, 2013
- Acquirers must certify the ability to comply
- Visa will require support of Field 55 and additional related chip fields for VIP authorization messages between the acquirer and Visa
- Acquirers should also ensure downstream connections certify to their own platforms prior to the deadline

[1]Dates and/or timeline may change
[2]Merchants previously involved in a breach may qualify if they have completed subsequent PCI DSS validation

Managing Liability

Liability shift rewards the entity making the investment in EMV. It is not a mandate to issue or accept chip cards



- Visa intends to establish a U.S. liability shift for domestic and cross-border counterfeit POS transactions
- If a card is contact chip-capable and the merchant has not invested in chip, liability for counterfeit fraud will shift to the Acquirer
- The chip card's counterfeit fraud protection plus the liability shift encourage issuer chip adoption by providing dynamic authentication that helps better protect all parties
- The liability shift does not cover
  - Cards without a contact chip
  - Card-not-present transactions
  - Lost-and-stolen fraud

Liability Shift

Product Type	Merchant Terminal	Liable Party
Contact Chip or Dual Interface	Magstripe Only	Liability Shifts from Issuer to Acquirer

Note: When a chip-on-chip transaction occurs, in the unlikely event there is counterfeit fraud, liability follows current *Visa International Operating Regulations*

[1]Dates and/or timelines may change

What To Do If Compromised

- Take compromised system off the network
- If you must rebuild system, take a forensic image prior to rebuild
- Review firewall configuration and disable any unnecessary inbound and outbound traffic
- Pair down ACLs, ports and services between PCI and non-PCI environment
- Create strict ACLs segmenting public facing systems and backend database systems that house payment data (e.g., DMZ)
- Change all passwords on the network including applications and local accounts
- Review all access to the payment processing environment and terminate connectivity

What To Do If Compromised

- Notify your acquiring bank
- Engage a PCI Forensic Investigator (PFI) https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php
- For more information, please refer to Visa's *What To Do If Compromised,* available at www.visa.com/cisp under the "If Compromised" section
- You can also contact Visa Fraud Control and Investigations at usfraudcontrol@visa.com or (650) 432-2978, option 4

Questions?