

# Data Breach Findings and Mitigation Actions for the Payment System

21 October 2015

Glen Jones  
Lester Chan



**VISA**

# 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.

# Agenda

- Introduction
- Global Payment Compromises
- Cyber Attack Kill Chain
- Profile of Large & Small Breaches
- Wishful Thinking Security
- Breach Findings & Security Controls Deep Dive
- Secure Technology to Devalue Data
- Key Takeaways
- Questions and Answers

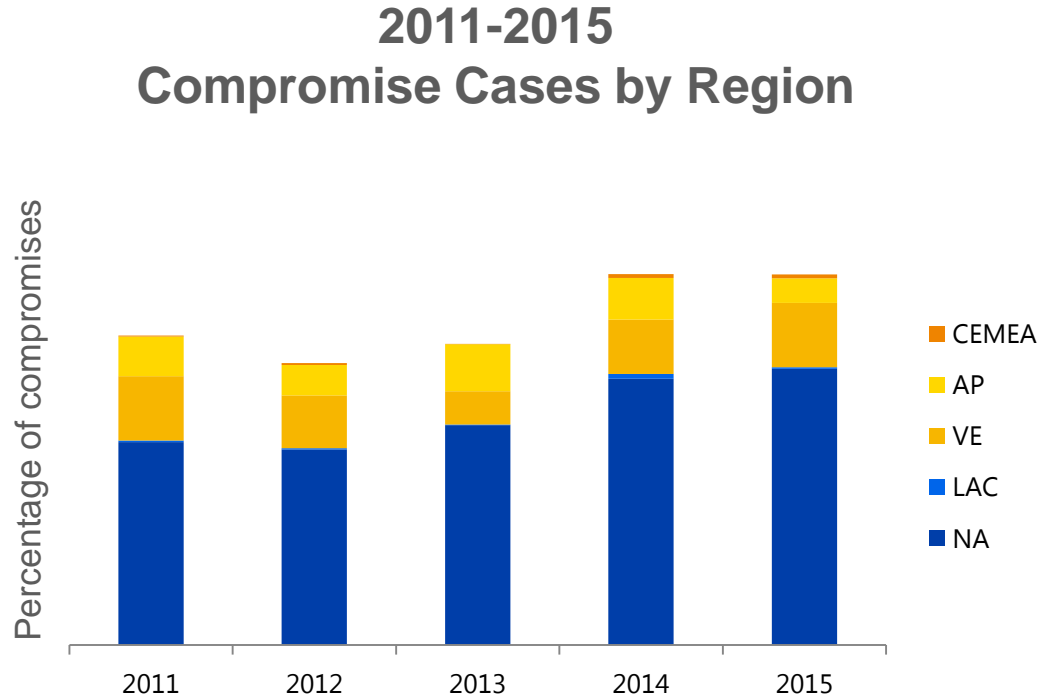
# Payment Card Compromises and Lessons Learned

Glen Jones, Sr. Director Cyber Intelligence



# Global Data Compromises

## US payment continues to be most at-risk



- Global data compromise events are slightly higher in 2015 over those managed in 2014
- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- VE and AP represent the next largest contributors to known breach events, together comprising a quarter of the total
- Breaches in VE and AP are primarily CNP

# Global Data Compromises

## Breach trends by merchant level

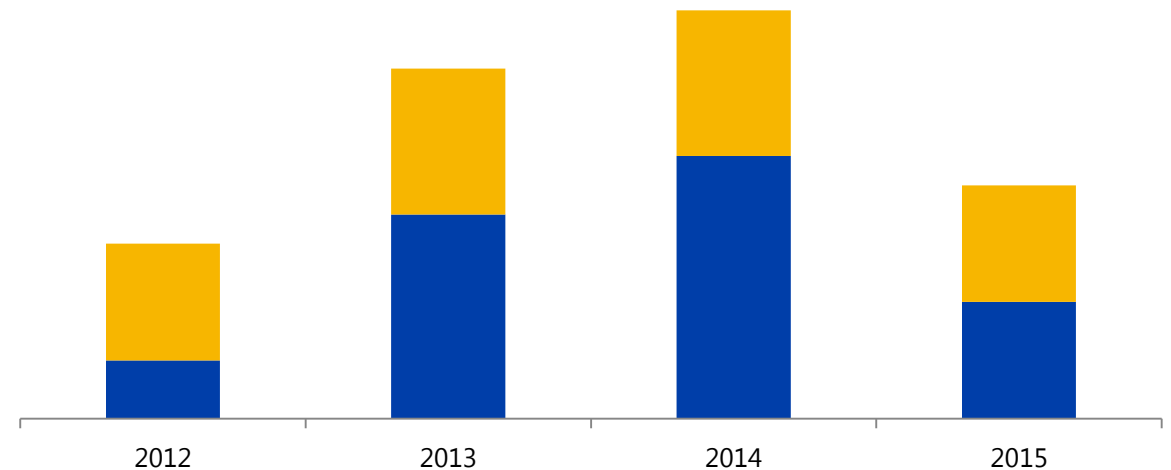
Breach events by merchant level

Entity Type		2012	2013	2014	2015*
		%	%	%	%
Merchant / Entity size	Level 1	<1%	1%	1%	<1%
	Level 2	<1%	1%	1%	<1%
	Level 3	1%	4%	4%	4%
	<b>Level 4</b>	<b>95%</b>	<b>92%</b>	<b>93%</b>	<b>93%</b>
	Agent	<1%	1%	1%	2%
	Other	2%	<1%	0%	0%
	<b>Total</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>

- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- At-risk accounts in 2015 were largely attributed to L4 merchants
- Level 4 merchants outnumber L1s in the US

\*2015 year-to-date

Large breach events (levels 1 & 2)



- Fewer level 1 and 2 breaches in 2015
- Threat actors are targeting smaller interconnected merchants in large numbers
- Restaurants and “other retail” make up the biggest portion of total known breaches
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs

# Cyber Attack Kill Chain

## Elements of the attack / opportunities for prevention and detection



\* Based on Lockheed Martin Cyber Kill Chain

# Profile of Large U.S. Merchant Breaches

## Large merchant breach root causes



- Had privileged accounts compromised
- Had sysadmin accounts exploited



- Had weak application security testing
- Had inadequate security event monitoring



- Had weak anti-malware detection on POS systems
- Had weak segmentation between CDE and core



- Most had completed PCI DSS validation before incident, but environment did not reflect what was assessed



- Had a weak audit function

\* Based on US forensic investigation reports



# Profile of Small (Level 4) U.S. Merchant Breaches

## What do breached small merchants have in common?



- Third-party remote access for POS management (LogMeIn, for example)
- Always-on remote access
- Single-factor authentication



- Few host, user, network security controls
- No security monitoring



- Did not have application white-listing
- Did not use anti-malware software



- None had completed PCI DSS validation before incident



- Common / shared username & password
- Intrusion began with spear phishing attack against POS integrator

\* source: US forensic investigation reports

# Wishful Thinking vs. Effective Security Controls

## Perceived Security

- A plan to implement security
- A firewall (ANY/ANY ALLOW)
- Separate networks with two-way trusts
- Intrusion detection technology without process
- SIEM without a plan
- File integrity: change monitoring only
- External account access with shared credentials

## Security Controls

- Implemented security
- A firewall that blocks traffic
- Truly segmented cardholder data environment
- Risk-prioritized intrusion detection as part of a well-managed, tested process
- SIEM with relevant, risk-prioritized data and retention
- Monitoring for the instruction of new, unexplained files
- External account access with unique credentials

# Breach Findings & Security Controls

Lester Chan, Director, Merchant Security



# Breaches Continue to Occur

Hackers and fraudsters target specific industries and victims

## Small Businesses



- Continue to be targeted fraudsters
- Many have low/no security controls
- Work with a qualified Integrator/Reseller
- Perform security basics
- Implement secure technology – EMV chip, tokenization, P2PE

## Integrators & Resellers



- Targeted by hackers
- Improper implementation
- Always-on remote access
- Enroll into the Qualified Integrator/Reseller program
- Ensures that PCI DSS and PA DSS applications are installed properly






## Hospitality Industry



- Hotels and restaurants continue to be targeted
- Typically, back of house servers
- Social engineering or spear phishing attacks
- Malware on systems allows attackers to gain access
- Ensure anti-malware and file integrity monitoring are used

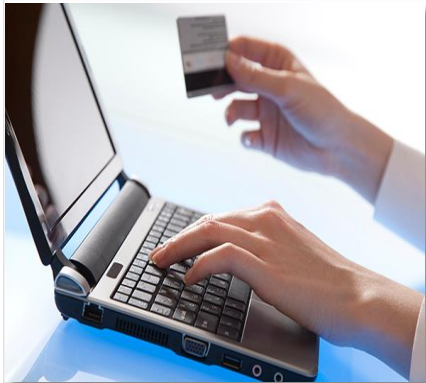
# Breach Findings to Security Controls

## Mapping vulnerabilities to PCI DSS requirements

Breach Findings	Remote Access 	Network Segmentation 	Elevated Privileges 	Weak IT Audit 	Internet Egress/Ingress 
PCI DSS Requirement	8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access	Strongly recommended to separate the CDE from core network and reduce PCI scope	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	10.1 Implement audit trails to link all access to system components to each individual user.	1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
Lack of Controls	<ul style="list-style-type: none"> <li>• Two-factor authentication</li> <li>• Always on remote access</li> <li>• No review of remote access accounts</li> </ul>	<ul style="list-style-type: none"> <li>• Flat networks</li> <li>• Little/no controls between CDE and core network</li> </ul>	<ul style="list-style-type: none"> <li>• Justification for elevated privileges</li> <li>• Includes service and admin accounts</li> <li>• Allows an attacker to install malware</li> </ul>	<ul style="list-style-type: none"> <li>• Log retention</li> <li>• Improper logs</li> <li>• Hinders investigations</li> </ul>	<ul style="list-style-type: none"> <li>• Outbound FTP, HTTP, HTTPS from CDE</li> <li>• Allows attacker to exfiltrate harvested cardholder data</li> </ul>

# Fraud Migration to Other Channels

## Fraud will migrate to e-commerce, automated fuel dispensers, and ATMs



- Fraud and attacks will continue in card not present/e-commerce channels
- Insecure websites and mis-configured security settings make it easy for attackers to exploit
- Internet facing websites make it easy for attackers to exploit weaknesses



- Scan for vulnerabilities
- Be aware of OWASP Top 10
- Properly scope all payment applications
- Work with a QIR on implementation best practices



- AFD liability shift to EMV chip in 2017
- Fraudsters will continue to target AFDs
- Stations in remote locations often targeted
- Skimmers and overlays are more sophisticated



- Regularly review pumps for devices
- Review POS for overlays
- Know who to contact if known or suspected attack



- ATM liability shift to EMV chip in 2017
- White label ATM higher risk for skimming and other overlay devices
- Remote locations or foreign countries are at higher risk for fraud and attacks



- Regularly review ATM devices for tampering
- Ensure software is kept up to date
- Know who to contact if known or suspected attack

# Implement Secure Technology

## Benefits of secure technology



### Implement EMV Chip Terminals

- EMV chip or “smart” cards are credit, debit or prepaid cards that have an embedded microchip
- Microchip generates a dynamic one-time use code (a cryptogram)
- Prevents the data being re-used to create counterfeit cards
- Reduces overall PCI scope



### Implement Tokenization

- Token replaces account number with unique digital token
- If payment token is used as the account number, it will be identified as stolen and rejected
- Devalues payment card data



### Implement Point to Point Encryption

- Secures the payment card transaction from swipe to processor
- Implement an approved PCI PTS terminal
- Reduces overall PCI scope

### Benefits of Implementing Secure Technology

- Reduce your liability from counterfeit fraud
- Reduce risk to the Payment System
- Partner with your Integrator/Reseller to simplify implementation
- Reduce your overall PCI scope
- Enroll in the Secure Acceptance Incentive Program that grants safe harbor from non-compliance fines

# Key Takeaways

- Breaches continue to occur with fraud and attacks to migrate
- Scrutiny between controls documented in ROC and PFI report
- Control effectiveness is as important as the control itself
- Additional analysis on security controls:
  - Remote access
  - Network segmentation
  - Elevated privileges
  - Weak IT audit
  - Internet ingress/egress
- Impacts to small businesses, integrators/resellers and hospitality merchants
- Many large merchant breaches over the last several years were preventable
- Fraud to migrate to CNP, AFD and ATMs



# Upcoming Events and Resources

Visa Data Security Website – [www.visa.com/cisp](http://www.visa.com/cisp)

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – [www.pcissc.org](http://www.pcissc.org)

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more...

Questions?

**VISA**