Breach Findings for Large Merchants

28 January 2015

Glen Jones – Cyber Intelligence and Investigation
Lester Chan – Payment System Security

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

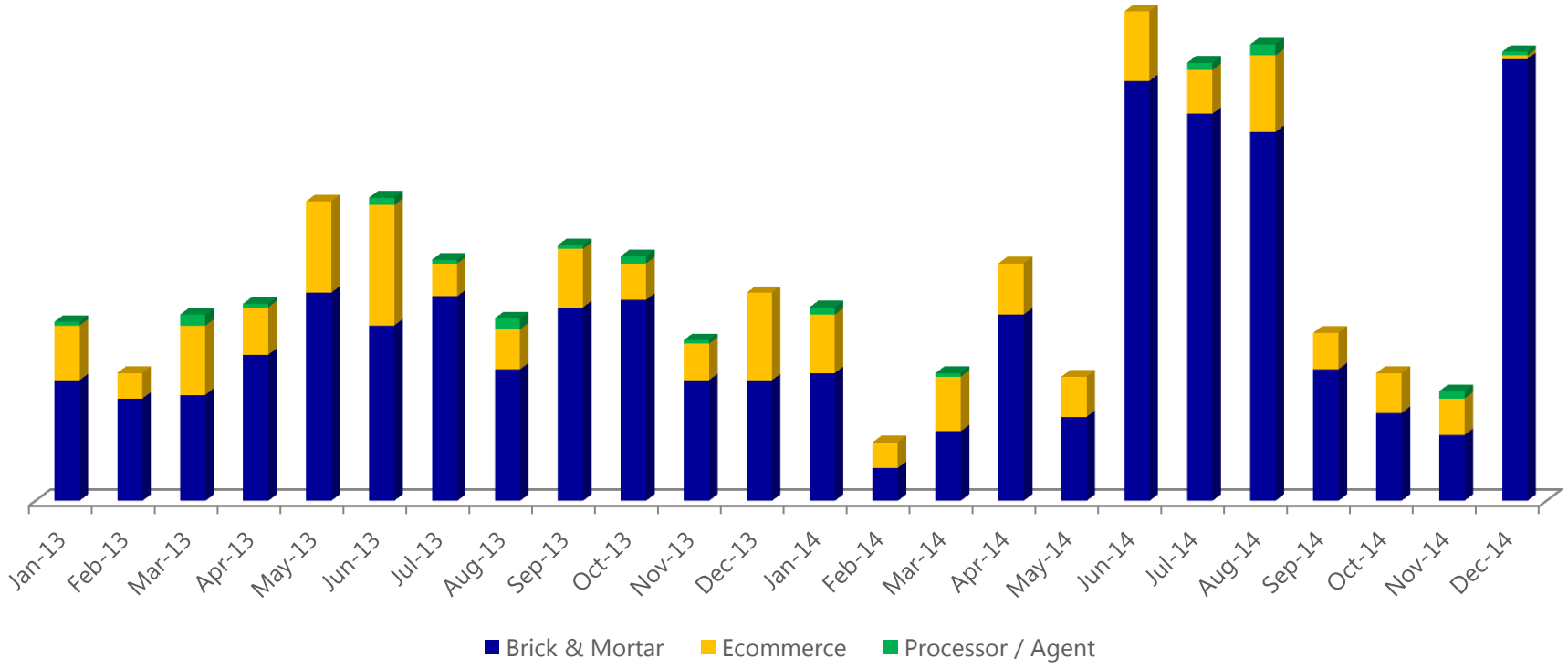
- Introduction
- Payment Card Compromises
- Analyzing Large Merchant Breaches
- Breach Findings & Vulnerabilities
- Security Controls for Large Merchants
- Questions and Answers

Payment Card Compromises

Glen Jones

Visa Public

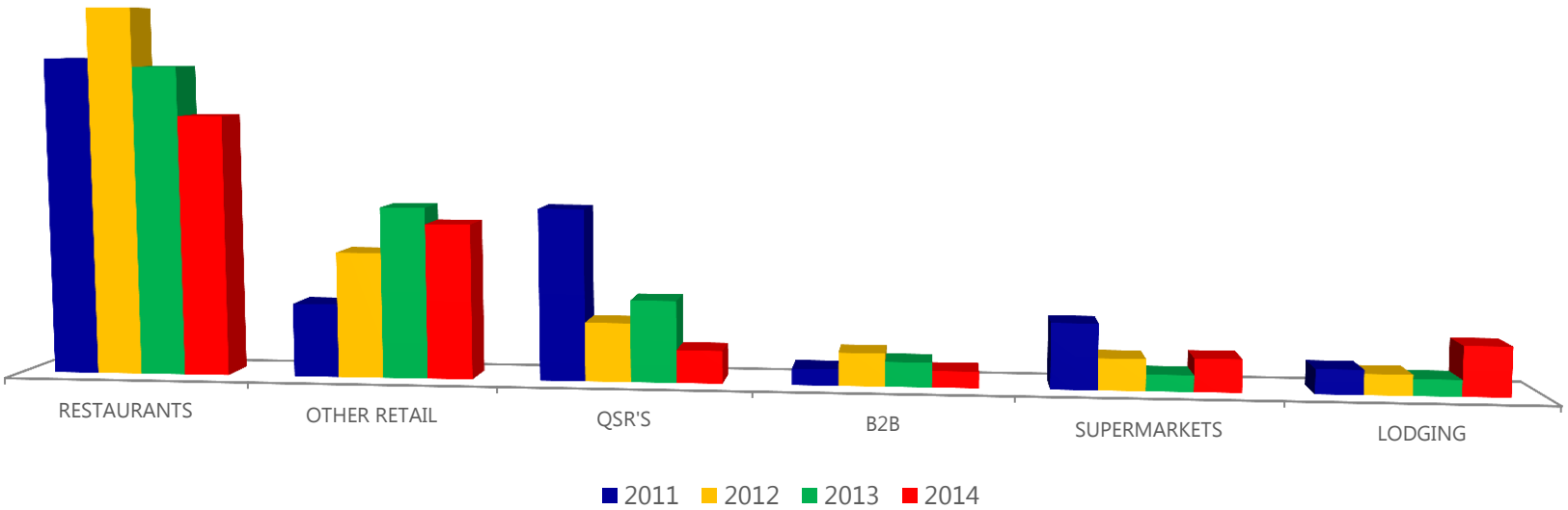
Visa Inc. CAMS Compromise Events
Entity Type by Month



Source: Compromised Account Management System (CAMS) – Original "IC" and "PA" Alerts

Visa Inc. CAMS Compromise Events
Top Market Segment* (MCC)

- Restaurants and retailers are leading market segments in 2014
- Insecure remote access and poor credential management continue to be attack vectors



* Market Segment based on Acceptance Solutions MCC "Market Segment" category

Source: Compromised Account Management System (CAMS) – Original "IC" and "PA" Alerts

Analyzing Large Breaches

Lester Chan

Visa Public

What we looked for…

- Large breaches over the past 2 years
- Common themes, sources
- Attack patterns, characteristics
- Malware used
- Determine vulnerabilities
- Large versus small breaches
- Lessons learned

Conclusion: Intruders are exploiting basic vulnerabilities

Breach Findings & Vulnerabilities

Visa Public

Profile of Large U.S. Merchant Breaches

Aggregate findings over the past 2 years

9	8	6	5	2
				
• Privileged accounts compromised • Sysadmin accounts exploited	• Weak AppSec testing • Inadequate monitoring	• Malware infected POS systems • Weak segmentation between CDE and core	• Completed PCI DSS validation before incident	• Weak audit function

Visa Public

Establish Security Controls for Remote Access

- Point of entry for attackers
- Harvest credentials using malware
- Social engineering to acquire

- Many remote servers not hardened
- Auditing not configured properly
- Lack of multi-factor authentication
- Lack of account management

REMOTE ACCESS

- Enable multi-factor authentication
- Only enable when needed
- Business need only restrict by IP
- Regularly audit

- 3rd party vendor remote access
- Malware on laptop harvested
- Remote access servers support end of life

Ensure Merchant Core Network is Properly Segmented from Cardholder Data Environment (CDE)

- Some had flat networks
- Weak using ACLs, VLANs
- Allows attacker to pivot and traverse

- Network reconnaissance
- Lack of auditing and monitoring
- Lack of IPS/IDS on systems

NETWORK SEGMENTATION

- ACLs and VLANs not sufficient
- Physical firewalls
- Separate CDE domain

- Some allowed Windows shares
- Patch servers access all
- Review alerts

Review Elevated Account Privileges, Reviews, and Justifications

- Attackers use multiple accounts
- Install malware on POS systems
- Login with one, switch to elevated

- Owns the network, systems
- Allows attackers to execute commands
- Hides audit trails, actions, logs

ELEVATED PRIVILEGES

- Ensure business justification
- Regularly review access
- No shared accounts

- Vendor account had Admin privileges
- Shared accounts used
- No account reviews

Review Audit Controls To Capture Relevant Data with Actionable Information

- Misconfigured logs
- Not capturing correct or enough
- Threshold for alerts

- Requires tuning (noise)
- Assists investigators
- Ensure integrity on logs

WEAK AUDITING

- Requires human interaction
- Use of automated tools
- Ensure capture of relevant info

- Some did not capture enough data
- Attacker deleted or modified logs
- Did not act on alerts

Review Internet Ingress/Egress for Controls, Insecure Protocols and Alerts

- Lack of monitoring
- Large data transfers
- Outside work hours

- Suspicious network activity
- Insecure protocols
- Infiltration of malware
- Exfiltration of cardholder data

INTERNET INGRESS/EGRESS

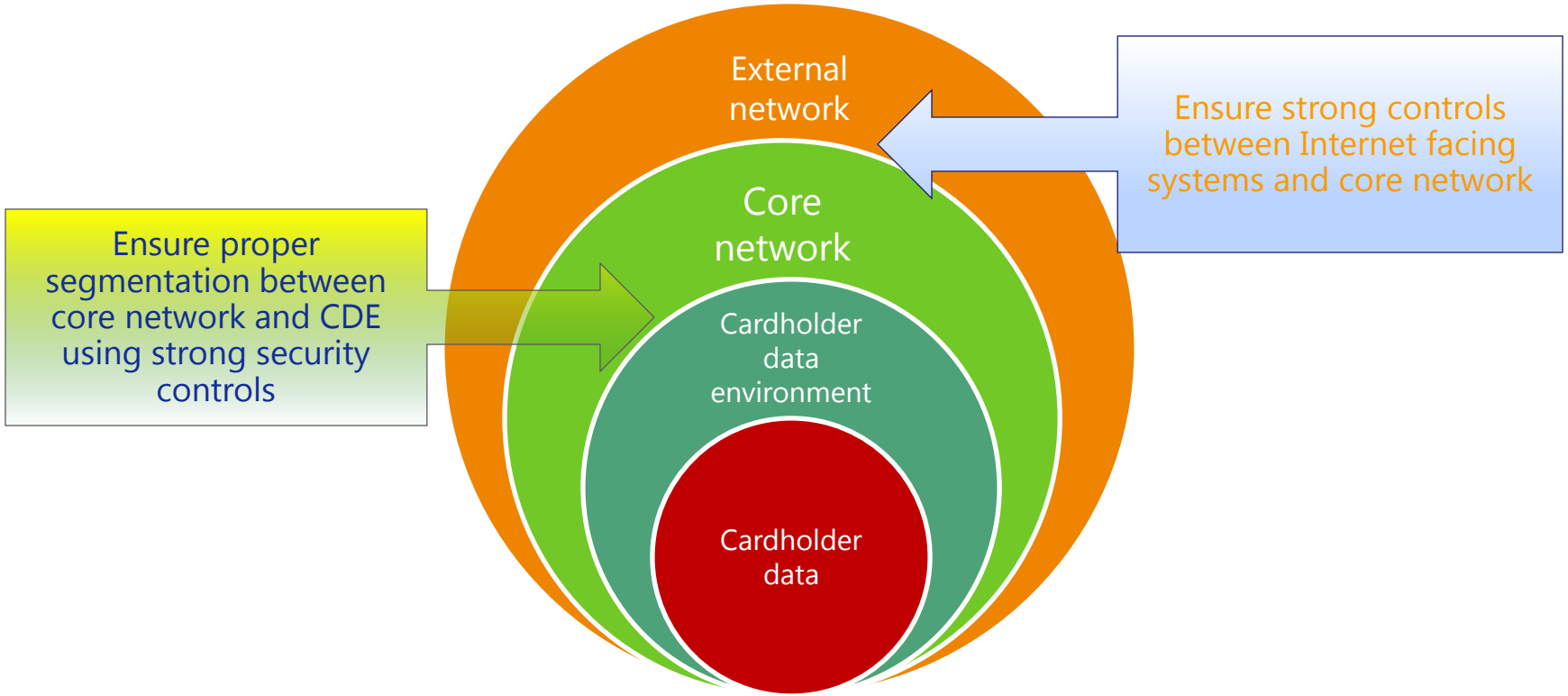
- Employ the use of IDS/IPS
- Assess protocols
- Threshold for alerts, actionable info
- No Internet egress from CDE

- Insecure egress protocol
- Disguised as legitimate data
- Alerts but didn't take action

Security Controls for Large Merchants

Visa Public

Protecting Cardholder Data



Visa Public

Highlighted Changes to PCI DSS version 3.0

V 2.0	V 3.0	Changes to PCI DSS 3.0 related to breach findings
1.1.2	1.1.2, 1.1.3	Understand all data flows in your environment especially cardholder data ingress/egress and provide an updated network diagram
2.1	2.1	Clarifies requirement to change all default passwords and remove all unnecessary default accounts
2.2.2	2.2.2, 2.2.3	Enable only necessary services and ensure secure protocols are properly configured
	5.3	New requirement to ensure active anti-malware cannot be disabled or altered without authorization
7.1.1	7.1.2	Restrict privilege IDs to those necessary to carry out job functions
8.5.6	8.1.5	Remote vendor access disabled when not in use
8.3	8.3	Two-factor authentication for remote access applies to users, admins, and vendors
	8.5.1	Requires unique user authentication credentials for all remote access
10.1	10.1	Requires audit trails to be associated with a user not just a process
11.2.1	11.2.1	Quarterly vulnerability scans with “high” vulnerabilities are addressed by qualified staff, and re-scanned until remediated
	11.3.4	New requirement for pentesting the CDE if segmented from the core network to ensure controls are in place

Maturing Information Security

Validate to Version 3.0

After January 1, 2015, all merchants must validate to PCI DSS version 3.0.

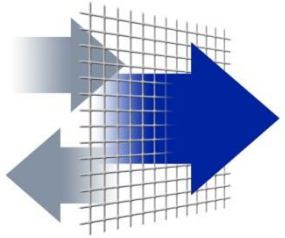
Version 3.0 continues to evolve the PCI DSS standard controls to address current threats and vulnerabilities.

Implement P2PE, EMV Chip, and Tokenization

EMV Chip - Creates a unique cryptogram for each transaction

Tokenization - Token replaces account number with unique digital token

P2PE -Encrypt from the point of sale to the point where the third-party payment processor or acquirer decrypts the data for processing



Proactive Security Controls

- Use two-factor authentication especially for remote access
- File integrity monitoring to protect against malware
- Application whitelisting to allow only those allowed applications
- Improve segmentation between CDE and core network
- Web application firewalls (WAF)

Additional Security Controls…

SIEM

- Security intelligence and correlation
- Alerts and notification
- Tuning

Vulnerability Management

- Frequency of scans
- Zero day vulnerabilities
- Remediation and tracking

Antivirus

- Keep signatures updated
- Ensure settings cannot be altered

Patch Management

- Keep all software, hardware, appliances up to date
- End of life systems
- Vulnerability window

Key Takeaways

- Large merchant breaches continue to occur
- Continue focus on security “basics”, ongoing maturity and going “beyond PCI”
  - Review security controls for remote access
  - Review elevated account privileges, reviews, and justifications
  - Ensure proper network segmentation
  - Review auditing and logging to capture relevant data
  - Review Internet ingress/egress for controls, insecure protocols, alerts
  - Fully understand all cardholder data flows
- Changes in 2015 due to EMV liability shift
- Consider secure technologies to de-value data, reduce scope and fortify payment processing environments

Upcoming Events and Resources

Upcoming Webinars – Training tab on www.visa.com/cisp

- Cyberlocker Merchant Overview & Enhanced Due Diligence
  - 24 February 2015, 7 pm PST (Asia Pacific / Central Europe, Middle East, Africa audience)
- Cyberlocker Merchant Overview & Enhanced Due Diligence
  - 25 February 2015, 10 am PST (North America, Latin America audience)
- Visa Third Party Risk Management Basics
  - 26 February 2015, 10 am PST

Visa Data Security Website – www.visa.com/cisp

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

PCI Security Standards Council Website – 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?