Effectively Managing Account Data Compromises

Stoddard Lambertson, Director, Fraud and Breach Investigations
Craig Johnson, Director, Fraud and Breach Investigations

28 September 2016

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

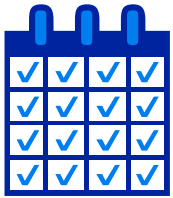
- Account Data Compromise Trends
- NEW: Visa What To Do If Compromised Version 5.0
- Investigations Overview / Mitigation and Detection Strategies
- Agent Programs: Integrators and Resellers & Franchisee Servicers
- Upcoming Events and Resources

Account Data Compromise Trends

Craig Johnson
Fraud and Breach Investigations

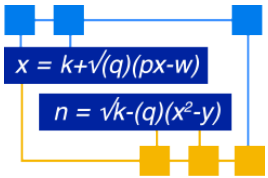
Trends in Data Compromises

- Criminals are launching more sophisticated attacks targeting merchants and agents with a focus on Integrator Resellers (IR's)

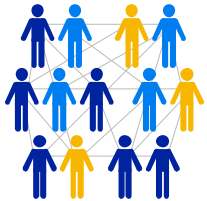


FREQUENCY

MAGNITUDE

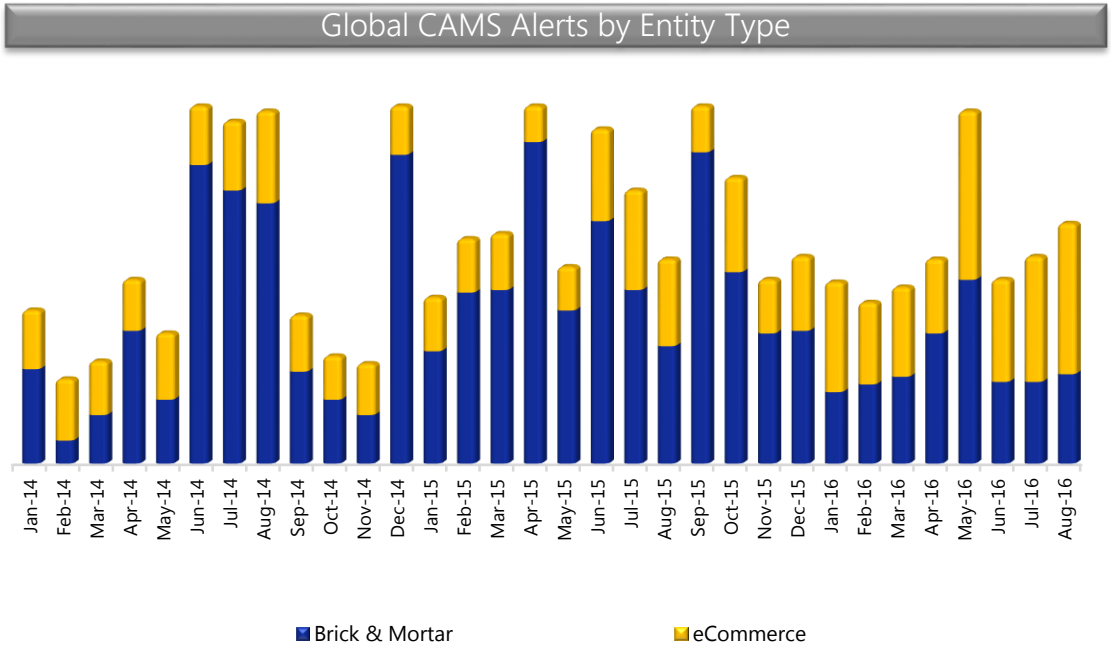


SOPHISTICATION



ORGANIZATION

Recent Increase in Ecommerce Breaches



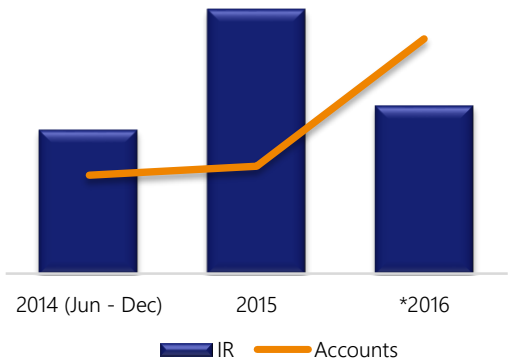
Source: Compromised Account Management System (CAMS) – Original 'IC' and 'PA' Alerts, Visa Account Bulletin (EU)
*YTD through August

Small Merchants Targeted Through Integrators / Resellers

Breach Events by Merchant Level

Entity Type		2014	2015	2016*
		%	%	%
Visa Inc.	Level 1	1%	<1%	0%
	Level 2	1%	<1%	1%
	Level 3	4%	5%	13%
	Level 4	93%	91%	84%
	Agent	1%	3%	2%
	Total	**100%**	**100%**	**100%**

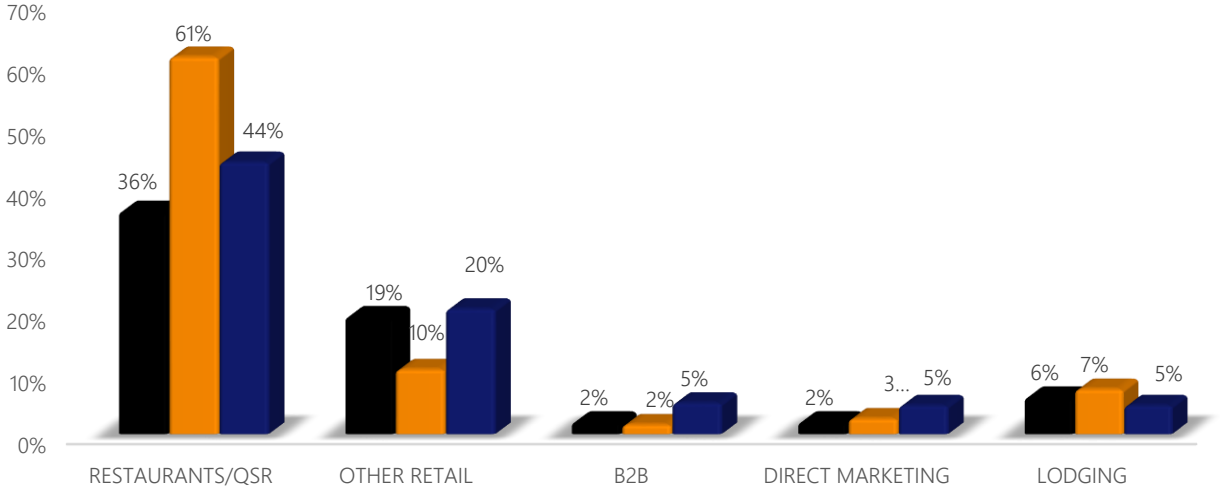
Breach Events by Integrator Resellers (I/R)



Source: Compromised Account Management System (CAMS); Fraud Incident Tracking (FIT), *YTD through August

Top Market Segments (MCC) Targeted

- Restaurants and retailers continue to be the two leading market segments through the first six months of 2016
- Integrators and resellers implementing insecure remote access and poor credential management are targeted by hackers



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

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

*YTD through August 2016

Rise in Skimming Attacks

Criminals are targeting mag stripe data

- Criminals are shifting their attacks to skimming
- Increase in report skimming attacks in the news
- Criminals are targeting:
  - Self-checkout terminals
  - Automated fuel dispensers
  - White-label ATMs
- Increasing in sophistication of attacks and technology

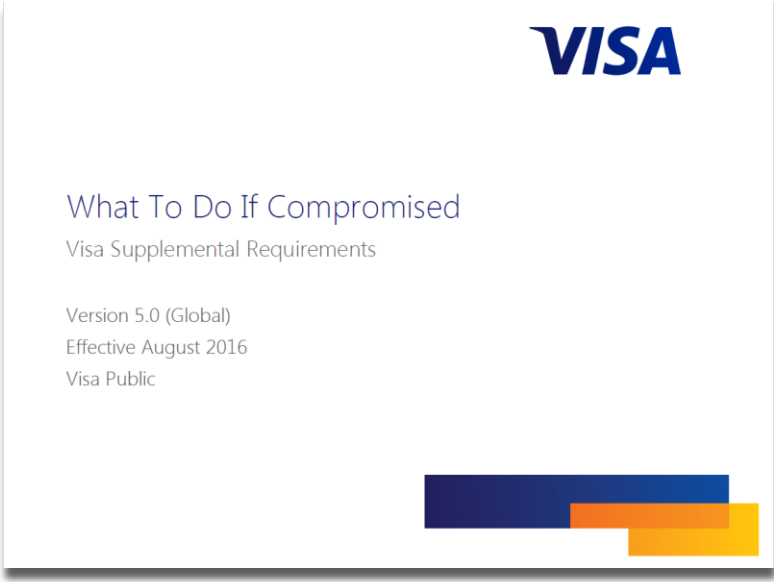
- All stores targeted – regardless if they are 100% EMV enabled
- Overlays
  - 3D printers leveraged by criminals
  - Placed in seconds not minutes as with physical swaps
  - Easier to deploy in large numbers

Guiding Principles for Managing an Account Data Compromise

Revised: What To Do If Compromised V5.0

What To Do If Compromised

- Indicators of a Data Breach
  - Visa notification of Common Point of Purchase (CPP) identification
  - Customer complaints of fraudulent activity on payment cards
  - Law enforcement notification
  - Bank reports of fraud after legitimate use
  - Abnormal activity/behavior of Point of Sale (POS)



Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located at: http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

Compromised Entity Responsibilities Overview

- Notification
  - Immediately report suspected or confirmed unauthorized access or data exposure to your acquiring bank and / or Visa Fraud & Breach Investigations

    usfraudcontrol@visa.com or **650-432-2978, option 4**
- Initial Containment
  - Immediately contain and limit the data exposure and minimize data loss
  - Document containment and remediation actions taken, including dates/times (preferably in UTC), individuals involved, and detailed actions performed

Visa Investigation Report	
Name of entity:	
Type of entity:	
Acquirer BIN(s): (List all that are applicable.)	
Does the entity send transactions to a payment processor?	☐ Yes ☐ No *(If yes, attach a list of processor(s) and provide name and contact information. If reporting entity is a Processor, please provide a list of all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City and State.)*
Entity PCI DSS Level *(e.g. Level 1-4):*	

- Evidence preservation
  - Preserve all evidence to identify root cause and facilitate the investigation
  - Do not access or alter compromised systems
  - Preserve all original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.
- Forensic engagement
  - Visa may require an onsite forensic investigation for any entity that has exposed cardholder data or caused a cardholder data compromise
  - Avoid Conflicts of Interest (COI) - QSA vs PFI

Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located at: http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

Compromised Entity Responsibilities Overview Continued

- Law Enforcement
  - Notify the appropriate law enforcement agency in the event of an account data compromise.
- Communications Plan
  - Merchants can consult with Visa Corporate Communications for assistance in preparing a public breach response
  - *Responding to a Data Breach: Communications Guidelines for Merchants*
- Validate PCI Data Security Standards (DSS) Compliance and PCI PIN Security as applicable

Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located at: http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

Member Responsibilities Overview

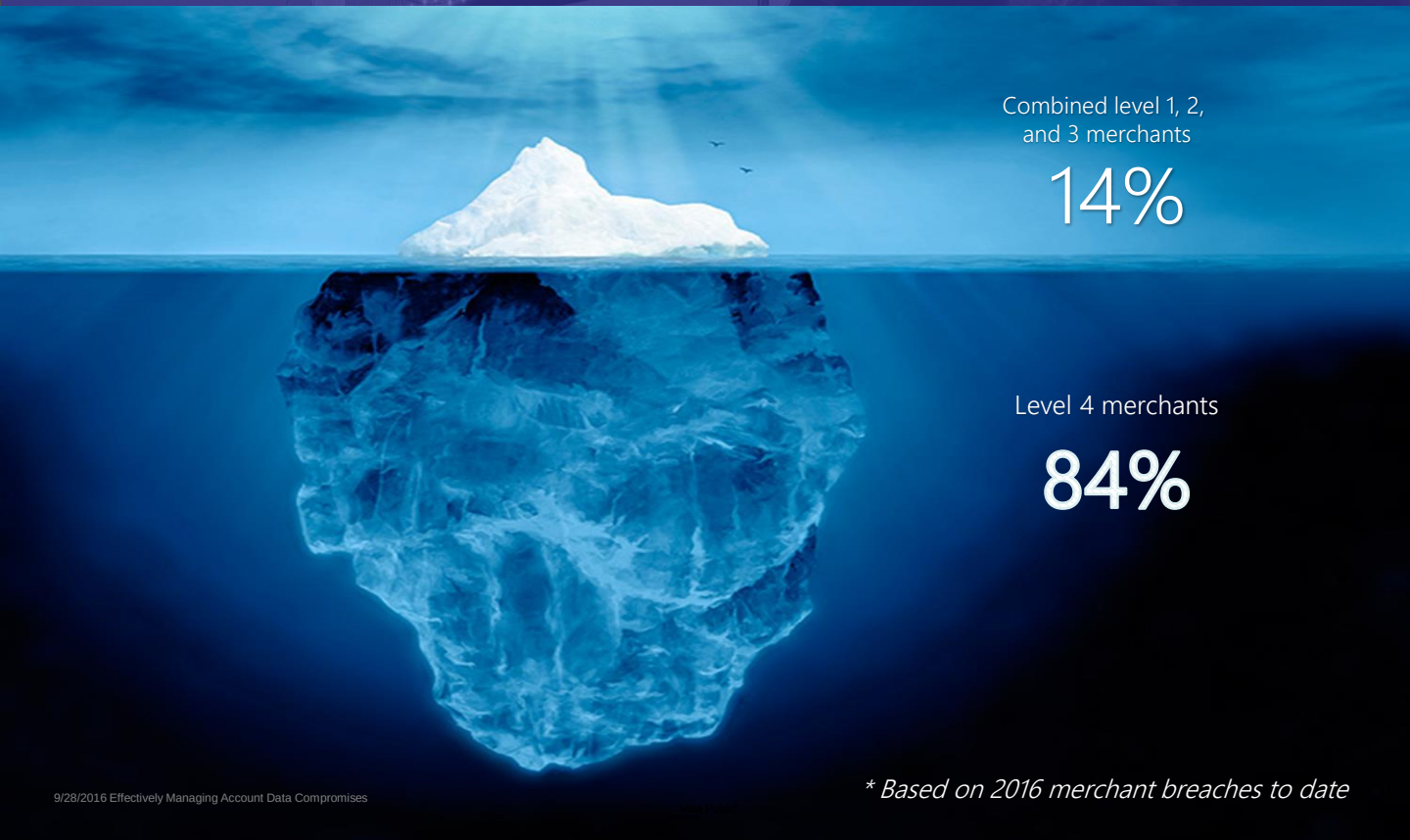
- Notification
  - Immediately report to the Visa Risk Management group any suspected or confirmed unauthorized access to any Visa cardholder data.
- Coordinate the investigation until its completion
  - Organize conference calls with merchant / acquirer / Visa
  - Provide ongoing updates
- Forensic engagement - Work with the entity to obtain an approved PCI Forensic Investigator (PFI)
  - Provide the PFI identity to Visa
  - Avoid Conflicts of Interest (COI) - QSA vs PFI
  - Ensure that the PFI is engaged (or the contract is signed) within five (5) business days
  - Ensure initial work is underway and provide the initial forensic (i.e., preliminary) report to Visa within ten (10) business days from when the PFI is engaged (or the contract is signed)
  - Provide a final forensic report to Visa within ten (10) business days of completion of the review.
- Provide Visa with potential at-risk accounts for distribution to impacted issuing banks
  - All compromised Visa accounts (known or suspected) must be uploaded to Visa within five (5) business days

*Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located at: http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

Investigations Overview / Mitigation and Detection Strategies

Stoddard Lambertson
Fraud and Breach Investigations

Breach Events by Merchant Level*



** Based on 2016 merchant breaches to date*

Investigations

- Most reported Common Point of Purchases (CPP) result in the detection of a small merchant….which often leads to an Integrator Reseller
  - A **Common Point of Purchase** (CPP) is determined when issuers identify a subset of legitimately used cardholder accounts, used at a single common merchant prior to fraudulent activity and not associated with a previous data compromise event
  - Visa's **Payment Fraud Disruption** Team uses other intel and sources to identify CPPs prior to issuer identification
- Visa Fraud and Breach Investigations
  - Engaging issuers to report accurate CPPs via feedback and analytics
  - Providing At-Risk accounts to issuers via CAMS
  - Notifying acquirers quickly of CPPs
  - Providing support to acquirer investigations with Merchant Conversion Rate analytics
  - Identifying key compromise trends:
    - Geography, vendor, agent and merchant types
    - Cyber intelligence community and Law Enforcement engagements
    - Common vulnerabilities being exploited (i.e. remote access)

Common Point of Purchase (CPP) Process Flow

Goal is to contain compromises quickly and mitigate Issuer losses by sending at-risk accounts via Proactive Comprised Account Management System (CAMS) alerts

Visa Investigations

- Receive Suspected Common Point of Purchase (CPP) Reports
- Visa validates Merchant and Acquirer information
- Fraud Incident Tracking Case Created / Updated
- Visa sends CPP details to Acquirer to investigate
- Visa sends At-Risk accounts to Issuers for CPPs reported by 2 or more issuers

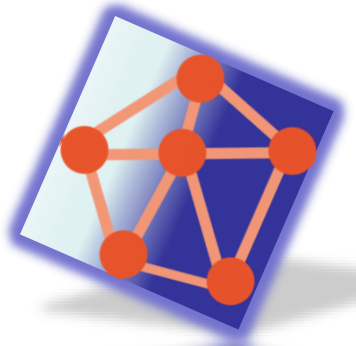
Acquirer Bank Investigations

- Acquirer receives CPP report from Visa
- Acquirer begins investigation & containment process
- Acquirer has 10 days to contain breach
- Once contained acquirer validates merchant is compliant
- Acquirer reports to Visa that case is contained and merchant compliant

New Global CPP Reporting Form

Initial Investigation Process

Understand *all* of the players in the payment ecosystem and how they may be in scope during the initial investigation



Payments is multi dimensional . . . and so are investigations

- How many agents are supporting your merchants?
- What services are they providing?
- How many locations does a single entity own?
- Franchise vs Corporate?
- How many parties have remote access?

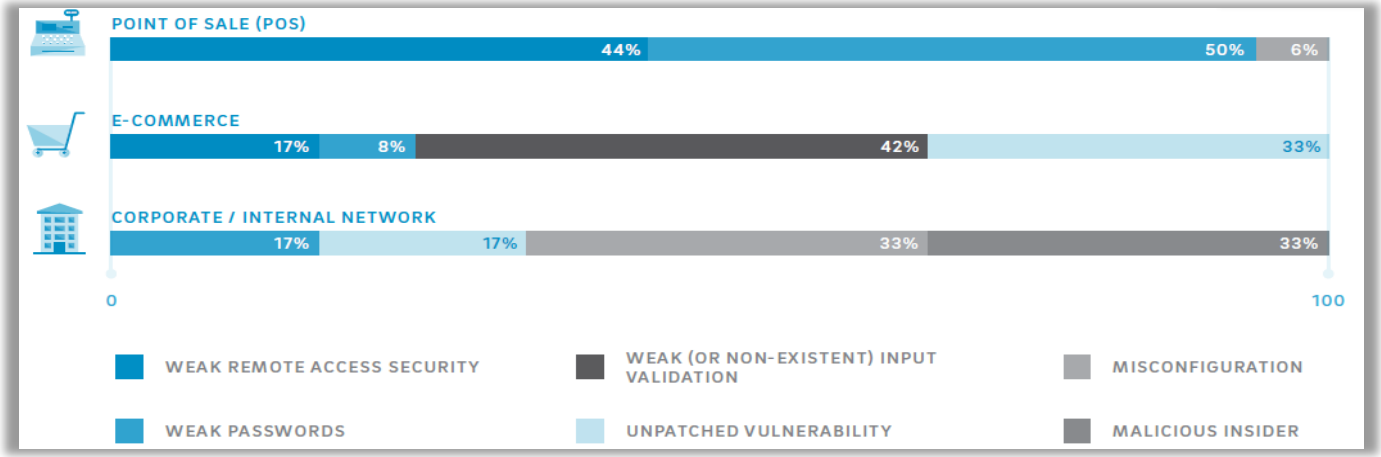
Any entity may be required to conduct an investigation – Goal is to investigate the entity that was the root cause

- Merchants
- VisaNet processors / downstream processors
- Gateways / agents / Integrator Resellers
- Regional or national multi-store chains
- Any incident deemed by Visa to be material

Majority of Compromises Occur at Small Merchants

- Untrained integrators that deploy weak remote access configurations are the most common reason for small merchant compromises
- Common attack vector: web-based and direct remote access services used by POS Integrators and Resellers

According to Trustwave's Global Security Report 2015, 94% of POS compromise are related to ***weak remote access security and weak or default passwords***



Merchant Security Safeguards

	1.	2.	3.	4.	5.
					
	Change Default Passwords	**Install Antivirus**	**Enable Remote Access Only When Needed**	**Use only PCI Approved QIRs**	**Use only Registered Agents**
Ease of Implementation	Easy	Medium	Easy	Easy	Easy
Cost	None	Medium	None	None	None
Effectiveness	Medium	Medium	High	High	High

*Based on PCI Forensic Investigation Reports

Visa Security Alert – Integrators Under Attack

www.visa.com/cisp

Visa Security Alert also published by the U.S. Secret Service

VISA

VISA SECURITY ALERT

June 2015

CYBERCRIMINALS TARGETING POINT OF SALE INTEGRATORS

Distribution: Value-Added POS Resellers, Merchant Service Providers, Point of Sale Providers, Acquirers, Merchants
Who should read this: Information Security managers and staff, IT Support Providers

Summary

To promote the security and integrity of the payment system, Visa periodically prepares informative materials related to securing cardholder data and protecting the payment industry. To ensure continued preparedness for new and emerging cyber security vulnerabilities, please review this urgent Security Alert.

Visa has observed a considerable increase in malicious remote access activity associated with unauthorized access to merchant Point-of-Sale (POS) environments via POS integrators. POS integrators are businesses that resell, install, configure, and maintain POS software and hardware for many different types of merchants. POS integrators often provide IT support and ongoing maintenance over remote network connections, many of which are established through third-party providers of remote desktop access. Properly secured, these connections pose little risk to merchants. Recently, however, cyber criminals have exploited inadequate security controls to

Qualified Integrator Reseller Program

Requirement Clarifications

Vendors that do not sell, support or service PA-DSS apps are not eligible to participate in PCI QIR Program

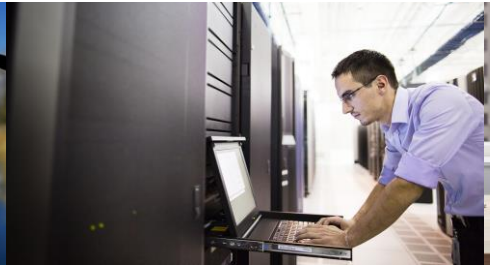
Requirements do **not** apply to merchants:

- Using single-use terminals without Internet
- Not using third-parties for POS system management
- Using IP-based terminals without remote access

QIR certification does **not** apply to vendors:

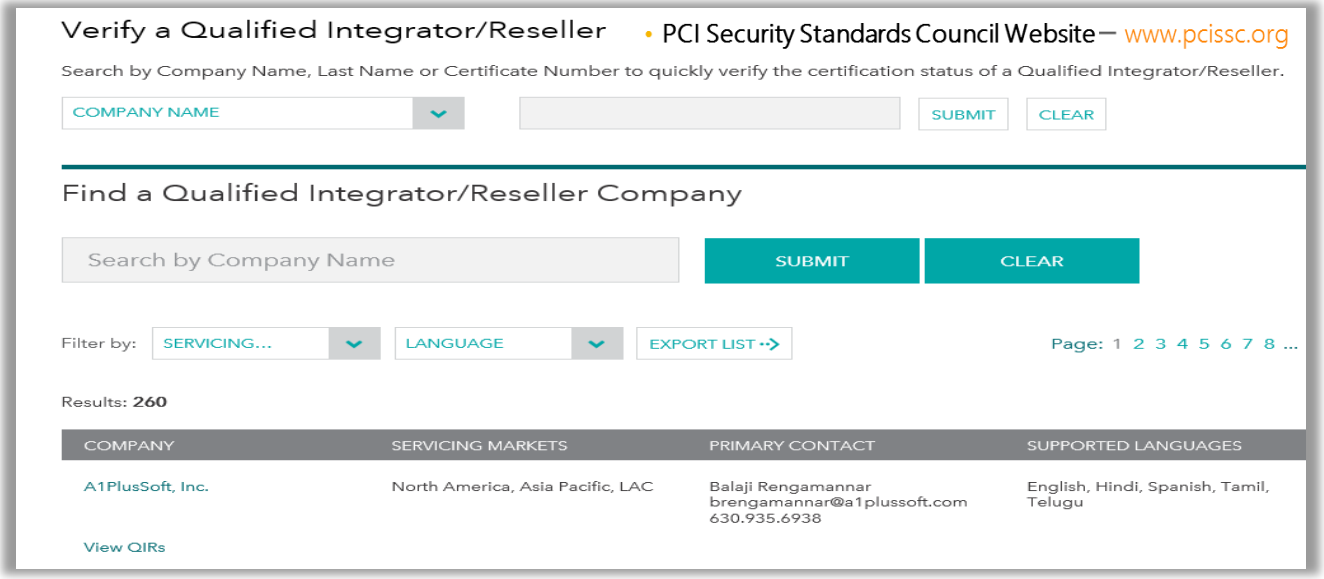
- Only supporting ancillary apps segmented from POS
- Providing plug & play applications without remote access
- Serving as acquirer or affiliated business unit

January 31, 2017	Acquirers must ensure that Level 4 merchants using third parties for PA DSS POS application and terminal installation and integration engage only PCI QIR professionals



Why Use a QIR?

- Using PCI Certified QIRs helps to ensure a merchant's PCI DSS compliance status is not jeopardized
- Help protect your organization and improve **security**
- **Simplifies** the vendor selection process – 260 Now on list!



Key Takeaways

- Merchant breaches continue to occur
- Small businesses, integrators / resellers and hospitality continue to be targets
- Understand the risks to your business, threats, and how data can be stolen
- Implement easy, low-cost, effective security basic controls
- De-value payment card data with EMV chip, tokenization, and P2PE
- Remove cardholder data from your environment
- Use a PCI DSS validated and or PCI QIR service provider if you are outsourcing

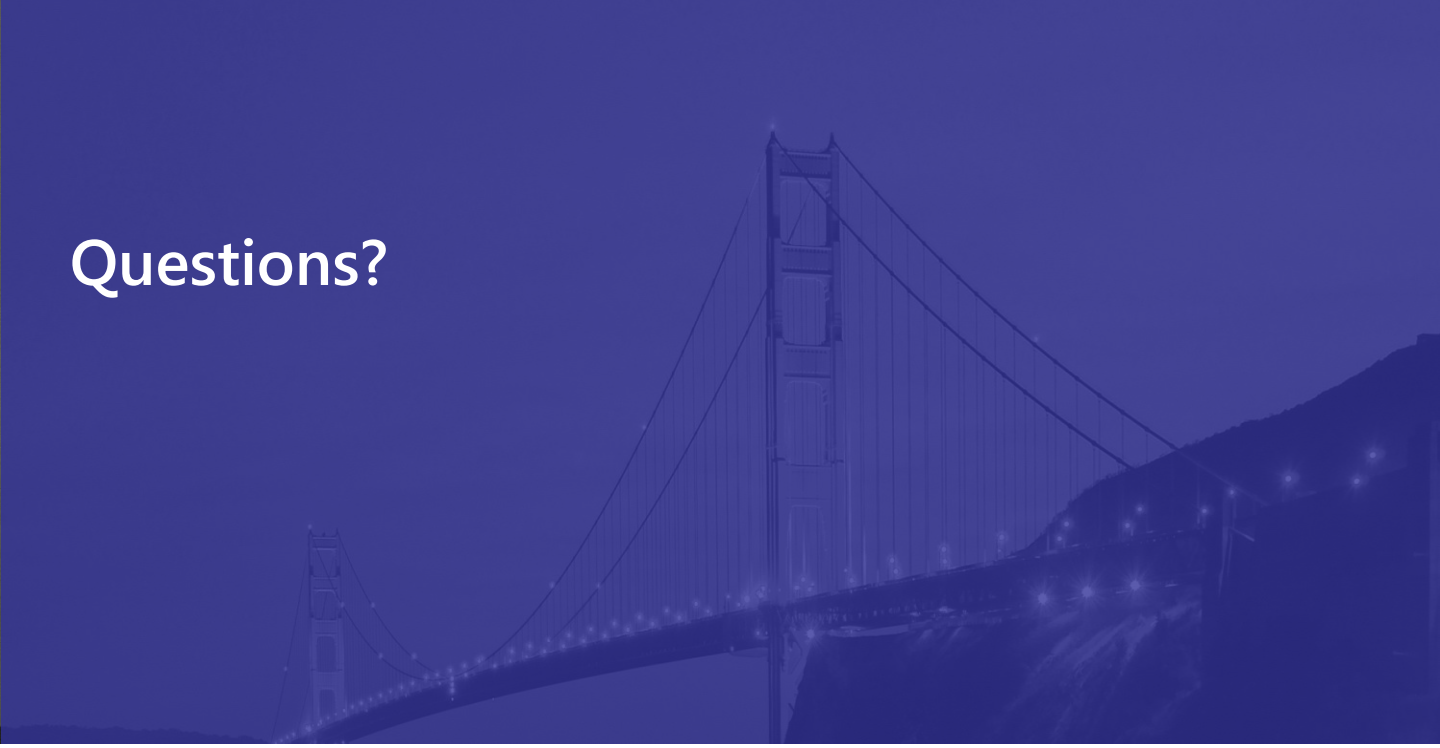
What To Do *Before* You Are Compromised

- Review and understand the fraud investigation procedures: *What To Do If Compromised*
  - Located under Resources at www.visa.com/cisp
  - http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf
- Ensure an Incident Response (IR) plan is in place
  - Prepare and regularly test plan
  - Know what steps to take and who and when to call
- Implement Secure Technology
  - Implement Point to Point Encryption
    - Secures the payment card transaction from swipe to processor
    - Implement an approved PCI PTS terminal
    - Reduces overall PCI scope
  - Implement EMV Chip Terminals
    - 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

- Actively review Alerts & Bulletins
  - *Visa Data Security Alert: Oracle MICROS Compromise* – 12 August 2016
  - *Visa Data Security Alert: ATM Malware Compromise* – 30 August 2016
  - *Visa Data Security Alert: Protect Against ATM Cash-Out Fraud* – 26 September 2016

Upcoming Events and Resources

- Upcoming Webinars – www.visa.com/cisp
  - October 13, 2016 – Third Party Agent Registration Tool Review
- 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?