

Effectively Managing Data Breaches

May 27, 2015

Stoddard Lambertson – Cyber Intelligence and Investigations
Justina Jow – Cyber Intelligence and Investigations



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
- Compromise Event Trends and Segments
- Merchant Servicer (POS) Integrator Threats and Best Practices
- PCI Qualified Integrators and Resellers (QIR)
- Common Point of Purchase Process Flow
- Small Merchant Investigations and Common Point of Purchase Process
- Large Merchant Investigations (Acquirer and Merchant Responsibilities)
- Upcoming Events and Resources
- Questions and Answers



Recent Fraud Trends and Small Merchant Investigations

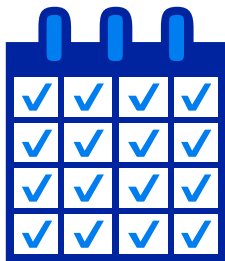
Stoddard Lambertson

Cyber Intelligence and Investigations



Trends in Data Compromises

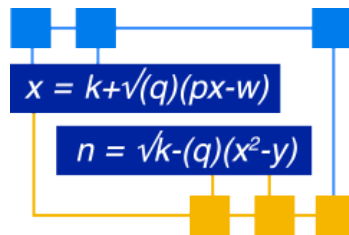
Criminals are launching more sophisticated attacks targeting small merchants



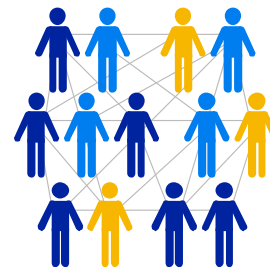
FREQUENCY



MAGNITUDE

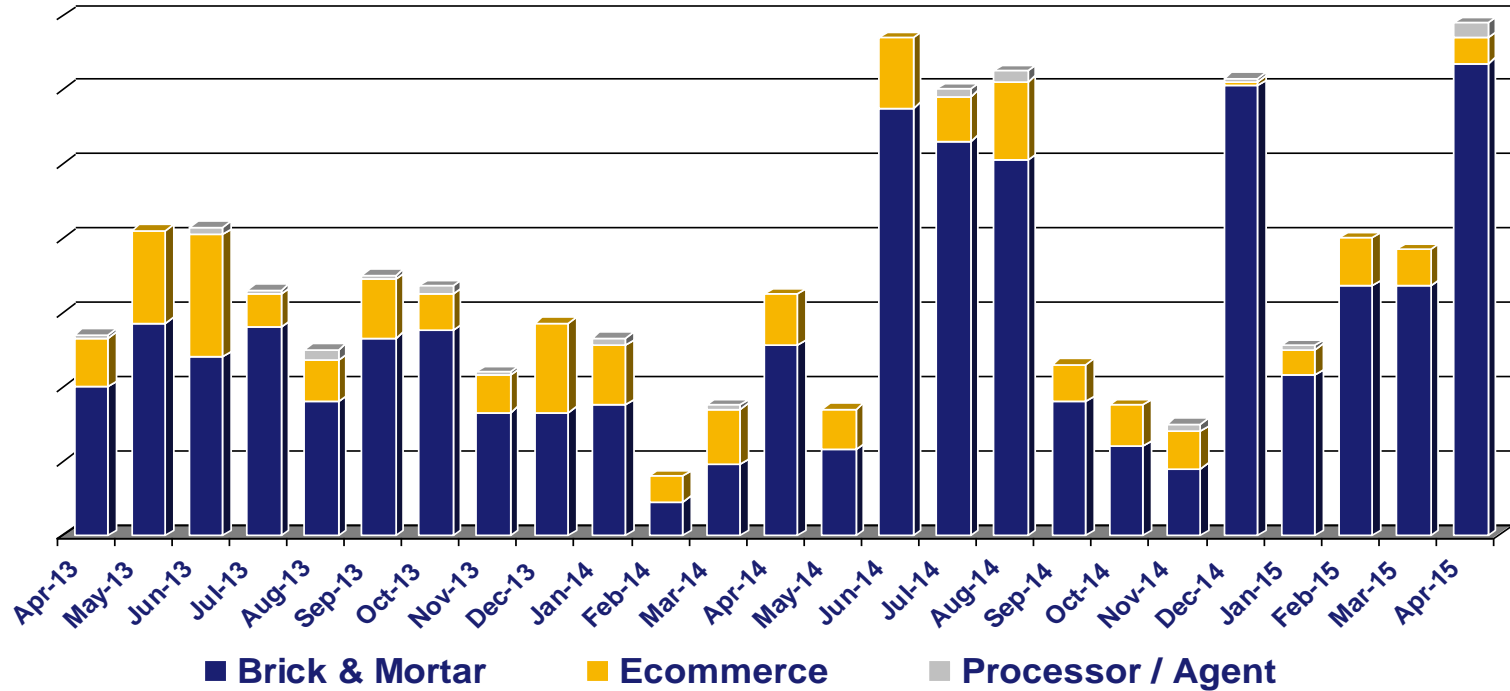


SOPHISTICATION



ORGANIZATION

Visa Inc. CAMS Compromise Events – Entity Type by Month

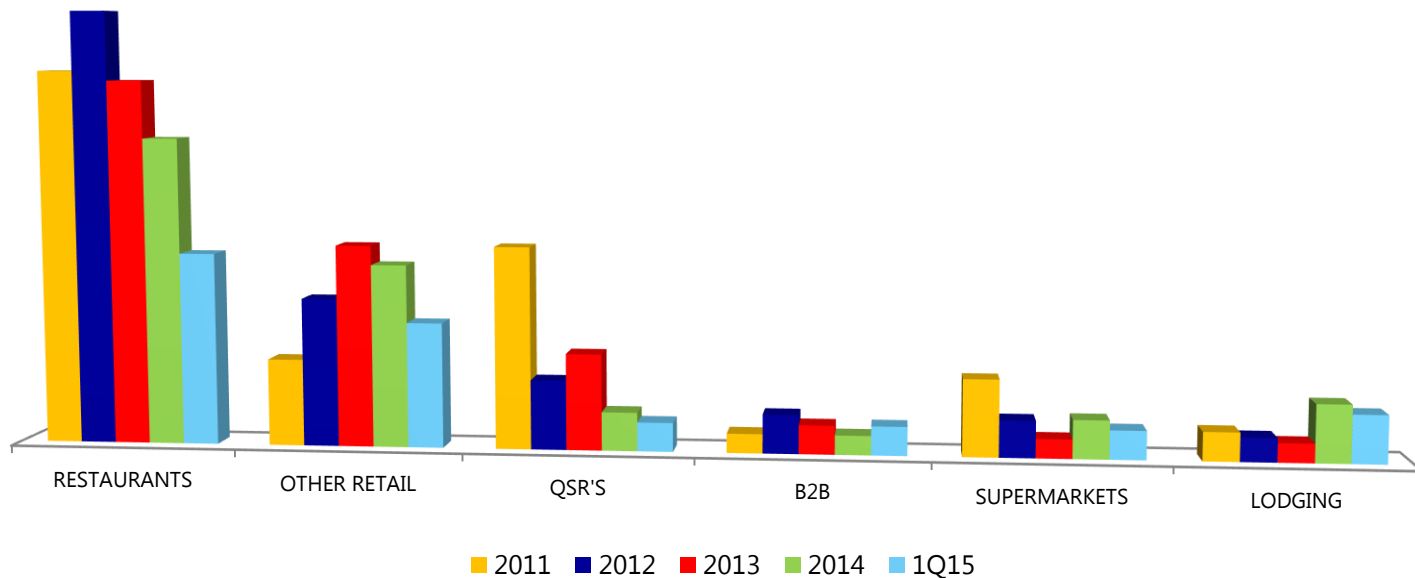


Source: Compromised Account Management System (CAMS) – Original 'IC' and 'PA' Alerts for Visa Inc.

Visa Inc. CAMS Compromise Events

Top Market Segment* (MCC)

- Restaurants and retailers are leading market segments in the first quarter of 2015
- 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

Recent Threats due to Merchant Servicers

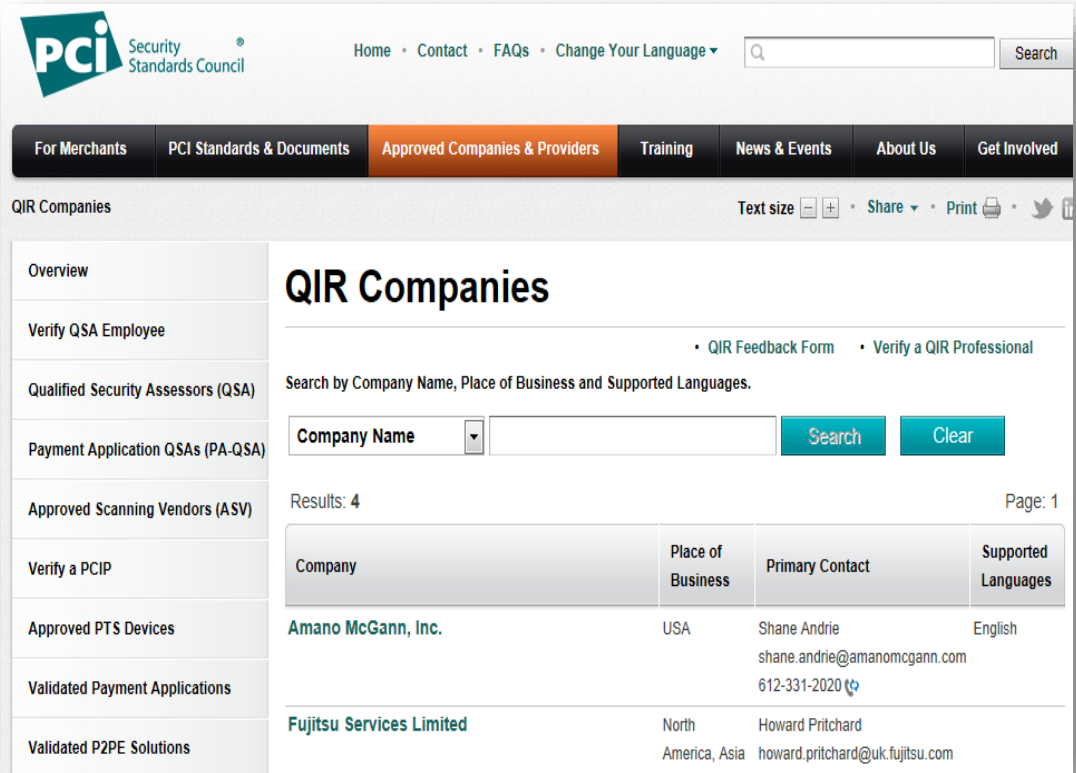
- POS Integrators/Resellers may provide merchant POS software installation and ongoing enterprise support for your POS system
- Merchant setup may include Remote Access Services (RAS) for monitoring and software support etc.
- Use of remote management products comes with an inherent level of risk that may create a virtual backdoor on your POS system
- Results in installation of malware to capture card data
- Integrators may have access to POS system - however PCI compliance not maintained
- Multiple POS Integrator related compromises since June 2014
- Non-Compliant Integrators / Merchants set up with default / shared remote access IDs without two-factor authentication or regular password changes

PCI Qualified Integrators and Resellers (QIR)

- QIRs receive training and qualification on the secure installation of PA-DSS validated payment applications into merchant environments in a manner that supports PCI DSS compliance
- Demand that your POS Integrator be qualified and listed by the PCI SSC

Use of a QIR will:

- Help protect your organization
- Improve security
- Reduce risk and help maintain PCI DSS compliance
- Simplify the vendor selection process



The screenshot shows the PCI Security Standards Council website. The top navigation bar includes links for Home, Contact, FAQs, and Change Your Language. Below this is a search bar. The main navigation tabs are: For Merchants, PCI Standards & Documents, Approved Companies & Providers (highlighted), Training, News & Events, About Us, and Get Involved.

The page title is "QIR Companies". Below the title, there is a search bar with the text "Search by Company Name, Place of Business and Supported Languages." and a "Search" button. To the right of the search bar, there are links for "QIR Feedback Form" and "Verify a QIR Professional".

The search results show 4 results. The table below lists the companies:

Company	Place of Business	Primary Contact	Supported Languages
Amano McGann, Inc.	USA	Shane Andrie shane.andrie@amanomcgann.com 612-331-2020	English
Fujitsu Services Limited	North America, Asia	Howard Pritchard howard.pritchard@uk.fujitsu.com	

www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php

PCI Approved QIR Companies

Ask your Integrator/Reseller to become trained and qualified to be listed as a QIR

Currently the following entities are PCI Approved QIR Companies:

- **Amano McGann, Inc.**
- **eMazzanti Technologies**
- **Fujitsu Services Limited**
- **Reliant Info Security Inc.**
- **Traffic & Safety Control Systems, Inc.**
- **Xpient Solutions LLC**



www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php

Visa Recommends Using PCI SSC Qualified Integrators and Resellers

In support of the PCI SSC Qualified Integrators and Resellers Program, Visa is expanding the definition of a **Merchant Servicer** to be “an entity that stores, processes, transmits **or has access to** Visa account numbers on behalf of a client’s merchants.” Bulletin posted on www.visa.com/cisp

Effective 1 June 2015, Visa will add integrators and resellers to the Visa Global Registry of Service Providers www.visa.com/splisting that have:

1. Successfully completed the PCI Qualified Integrators and Resellers Program
2. Are included on the PCI SSC’s Qualified Integrators and Resellers list
3. Have self-identified with Visa through the Merchant Servicer Self-Identification Program

The merchant servicer program fee will be waived for Qualified Integrators and Resellers that register in 2015



Cyber Intelligence & Investigations - Small Merchant Investigations

Most reported CPPs result in the detection of a small merchant (Level 4) breach

- A **Common Point of Purchase** (CPP) is determined when issuing clients identify a subset of accounts with legitimate cardholder usage, containing a single common merchant identifier prior to fraudulent activity and not associated with a previously reported data compromise event.
- **Level 4 merchants** process less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually

Visa's Small Merchant Investigations primarily focuses on:

- Engaging issuers to report accurate CPPs via feedback and analytics
- Notifying acquirers 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 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 Small Merchant Investigations



Acquirer Bank Investigations



Small Merchant Security Safeguards



**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 of Small Merchants



Large Merchant Investigations



Justina Jow

Cyber Intelligence and Investigations

Prevention and Detection Strategies



Remain vigilant and be prepared!!!

What To Do ***Before*** You Are Compromised*

Review and understand the fraud investigation procedures: *What To Do If Compromised*

- Located on the Protect Your Business section under Merchants on Visa.com
- <http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf>

Actively review Alerts, Bulletins, & Webinars

- *“RawPOS” Malware Targeting Lodging Merchants – March 2015*
- *Carbanak Advanced Persistent Threat – March 2015*
- *Identifying & Mitigating Threats to E-commerce Payment Environments – April 2015*

Ensure an Incident Response (IR) plan is in place

- Prepare and regularly test plan
- Know your business
- Know what steps to take
- Know who and when to call

*Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located on www.visa.com/cisp

What To Do ***Before*** You Are Compromised* (cont.)

Designate and empower an internal breach response team

- Educate employees on indicators of compromise and how to respond
- Create mock exercise to test and refine procedures
- Develop breach response communications

Identify and establish relationships and/or agreements with federal law enforcement (i.e., USSS, FBI) and key vendors

- Electronic Crimes Task Force (ECTF)

Establish and maintain an ongoing PCI DSS compliance program

*Summarized from *Responding to a Data Breach: Communications Guidelines for Merchants*, located on www.visa.com/cisp

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)

Requirements for Compromised Entities (pages 7-9 of WTDIC)

- Immediately contain and limit the exposure
- Preserve evidence and facilitate the investigation
- Alert all necessary parties
- Contact the appropriate law enforcement agency
- If deemed necessary, an independent forensic investigation will be initiated

*Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located on www.visa.com/cisp

What To Do *If* Compromised* (cont.)

Notification

- Immediately report suspected or confirmed unauthorized access or data exposure to the Visa Risk group

Visa Cyber Intelligence & Investigations

usfraudcontrol@visa.com or **650-432-2978, option 4**

Evidence preservation (page 7 from WTDIC)

- Do not access or alter compromised systems
- Preserve all evidence and logs

Payment Card Industry Forensic Investigation may be required (page 9 from WTDIC)

Communication 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*

*Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located on www.visa.com/cisp

Merchant Responsibilities*

Notification

- Alert your acquiring bank immediately
- Notify your QIR (Third Party Integrator)

Initial Containment

- Immediately contain and limit the data exposure and minimize data loss

Preservation

- Preserve evidence and facilitate the investigation

Forensic engagement

- Visa may require an onsite forensic investigation for any merchant that has not contained the initial event
- Avoid Conflicts of Interest (COI) - QSA vs PFI

Validate PCI Compliance

*Summarized from *What To Do If Compromised* (WTDIC). For more comprehensive information, please refer to WTDIC, located on www.visa.com/cisp

Acquirer Responsibilities

Notification

- Report any suspected breach to Visa immediately

Coordinate the investigation until its completion

- Organize conference calls with merchant / acquirer / Visa
- Provide ongoing updates

Forensic engagement (work with the merchant to obtain an approved PCI Forensic Investigator (PFI))

- Provide the PFI identity to Visa
- Avoid Conflicts of Interest (COI) - QSA vs PFI
- PFI must be onsite to conduct a forensic investigation as soon as possible from the date the contract agreement is signed
- Confirm with PFI that incident is fully contained
- Provide a copy of the completed forensic report as outlined in the PFI program guide

Provide Visa with potential at-risk accounts for distribution to impacted issuing banks

Implement Secure Technology

Benefits of EMV and Upcoming Liability Shift



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

Liability Shift

- Effective October 1, 2015, counterfeit liability shift will be instituted in the U.S for POS transactions.
- The party that is the cause of a chip transaction not occurring will be held financially liable for any resulting card present counterfeit fraud losses.
- The shift helps to better protect all parties by encouraging chip transactions that use unique, dynamic authentication data.

2015 Visa Payment Security Symposium



The Power of Partnership

Securing the Future of Commerce Together

August 12-13, 2015

Hyatt Regency Hotel

Burlingame, CA



Registration link will be available soon. For more information please contact pciocs@visa.com.

Visa is hosting a must-attend event that will focus on trends and developments related to cyber security, mobile payments, e-commerce and Visa's global authentication strategy. In order to secure the future of commerce all stakeholders including merchants, acquirers, agents and Visa need to collaborate on key initiatives in addressing today's most relevant issues. This event will be held in the San Francisco Bay Area at the Hyatt Regency Hotel just south of San Francisco.



Upcoming Events and Resources

Upcoming Webinars – Under Merchant Resources/Training on www.visa.com

- Minimizing Payment Risks for Merchants Using Integrators / Resellers
- 17 June 2015, 10 am PST

Visa Launches EMV Chip Education Tour for Small Businesses

- 20-City Tour for Small Businesses – www.VisaChip.com

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

- Streamline your chip migration – www.VisaChip.com/business toolkit

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, QIR Listing
- Fact Sheets – Mobile Payments Acceptance, Tokenization, and many more...

Questions?



VISA