Strategies to Effectively Manage Data Compromise Events

Glen Jones and Justina Jow
Cyber Intelligence & Investigations
Visa, Inc.

12 November 2014

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

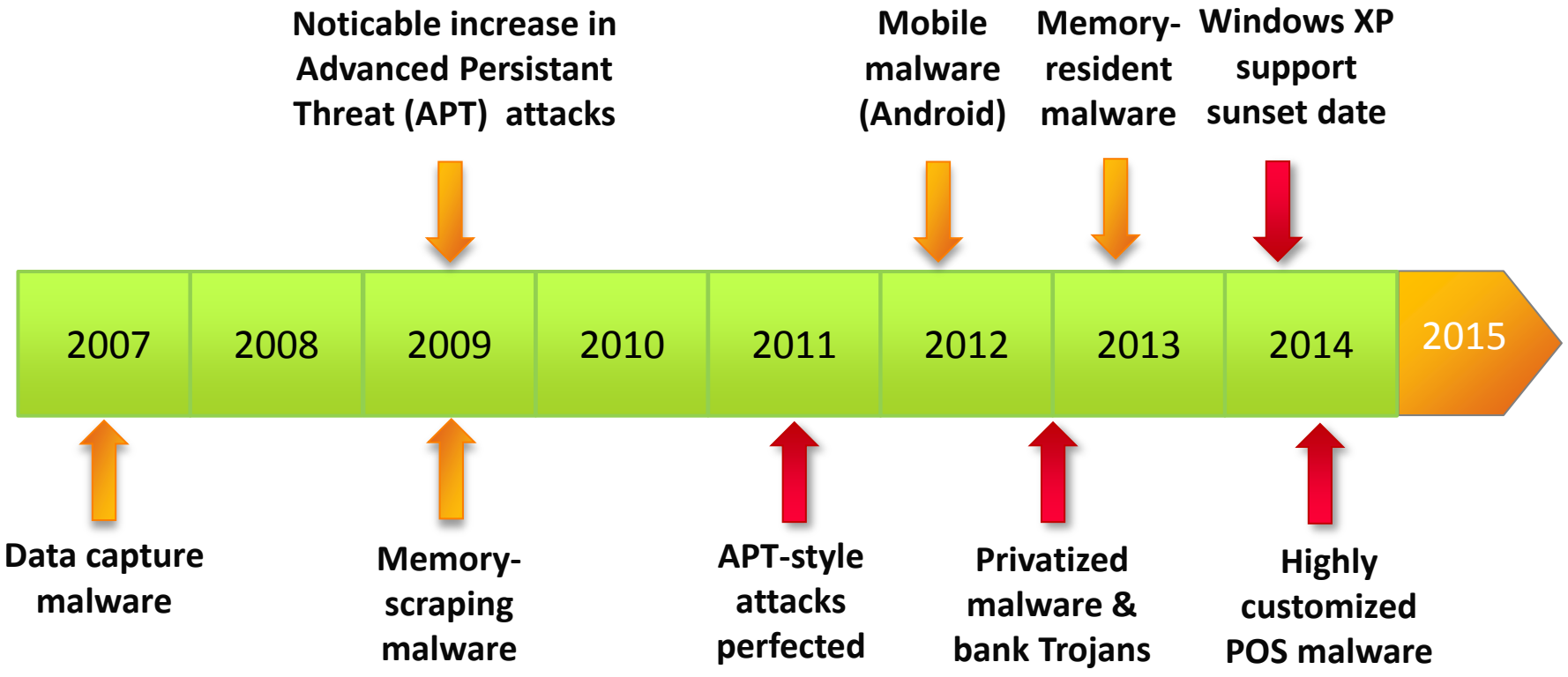
- Data Breach Landscape
  - Cyber Threat Landscape
  - Point-of-Sale (POS) Malware
  - Data Compromise Trends
- Investigation Process
  - Prevention and Detection Strategies
  - Investigation Procedures
- Upcoming Events and Resources

Data Breach Landscape

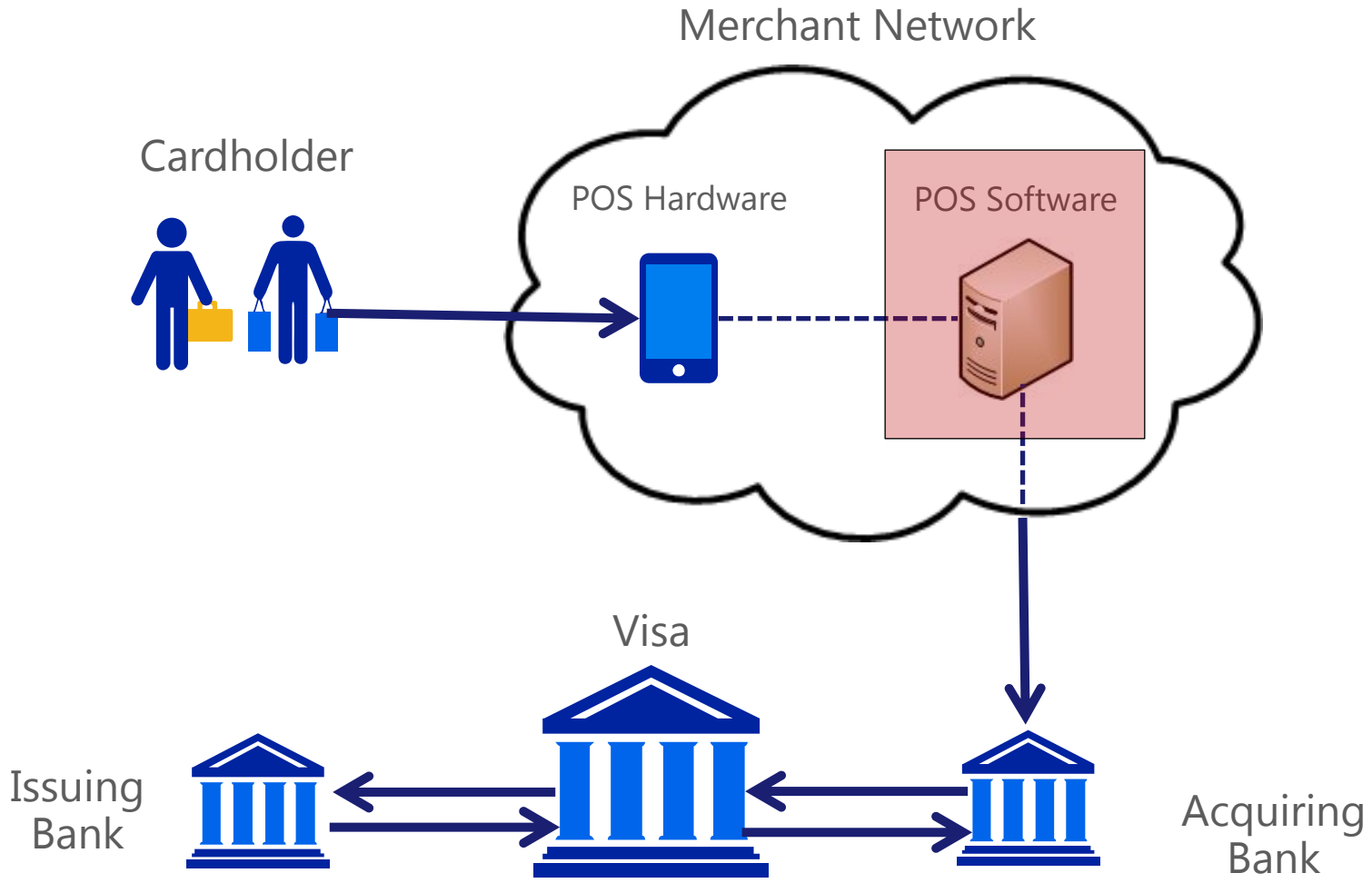
Glen Jones, Senior Director
Global Forensic Intelligence, Visa Inc.

Cyber Threat Landscape

Payment card data theft over last 8 years



Point-of-Sale (POS) RAM Scraping



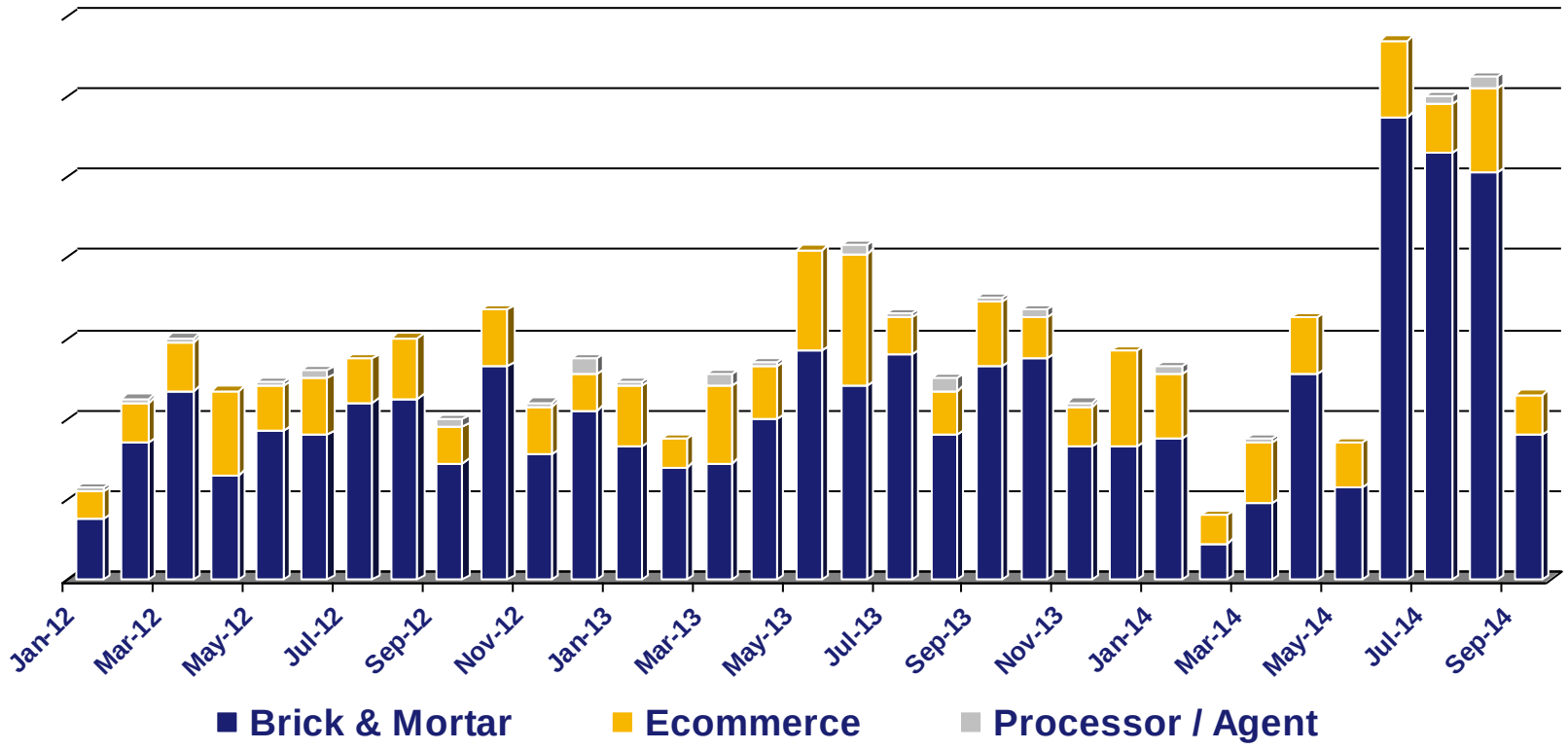
Point-of-Sale (POS) RAM Scraping (cont.)

- Authorization data is temporarily stored in clear text system memory
- Cybercriminals attack memory space as it's the easiest path to the data
- RAM scrapers generally use logic to identify track 1 and 2 data
- Some malware use the Luhn algorithm to validate payment card data
- Captured data is pulled out of memory as it's passing through the payment processing environment
- Data is often found to be briefly stored on the system it was captured from

Point-of-Sale (POS) Malware Characteristics

- Core Functionality:
  - RAM-scraping
  - Key logging
  - Command-and-Control communications
  - Data exfiltration
- Additional Botnet Functionality:
  - Upload
  - Download
  - Run
  - Self-deletion capability (reported in recent versions)

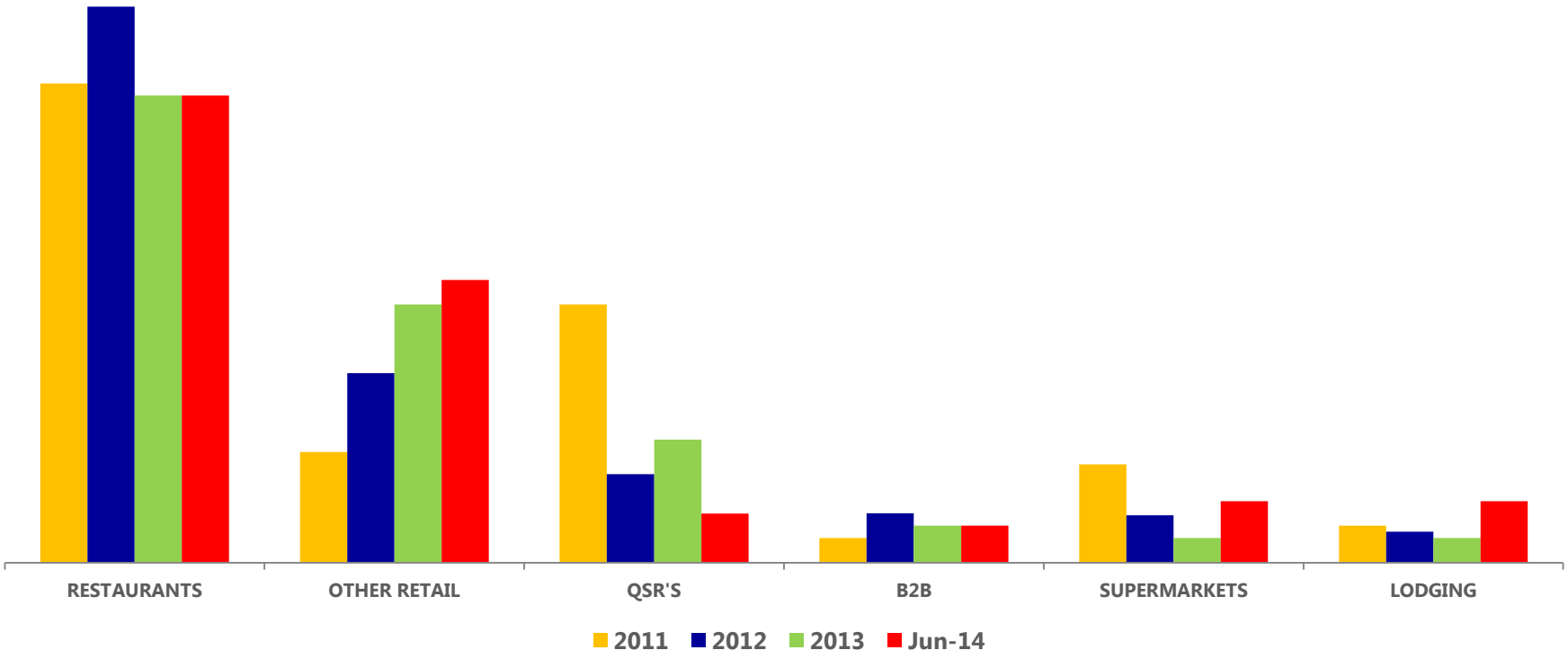
Visa Inc. CAMS Compromise Events – Entity Type by Month



Source: Compromised Account Management System (CAMS) – Original 'IC' and 'PA' Alerts for Visa Inc. *Reporting as of September 2014

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



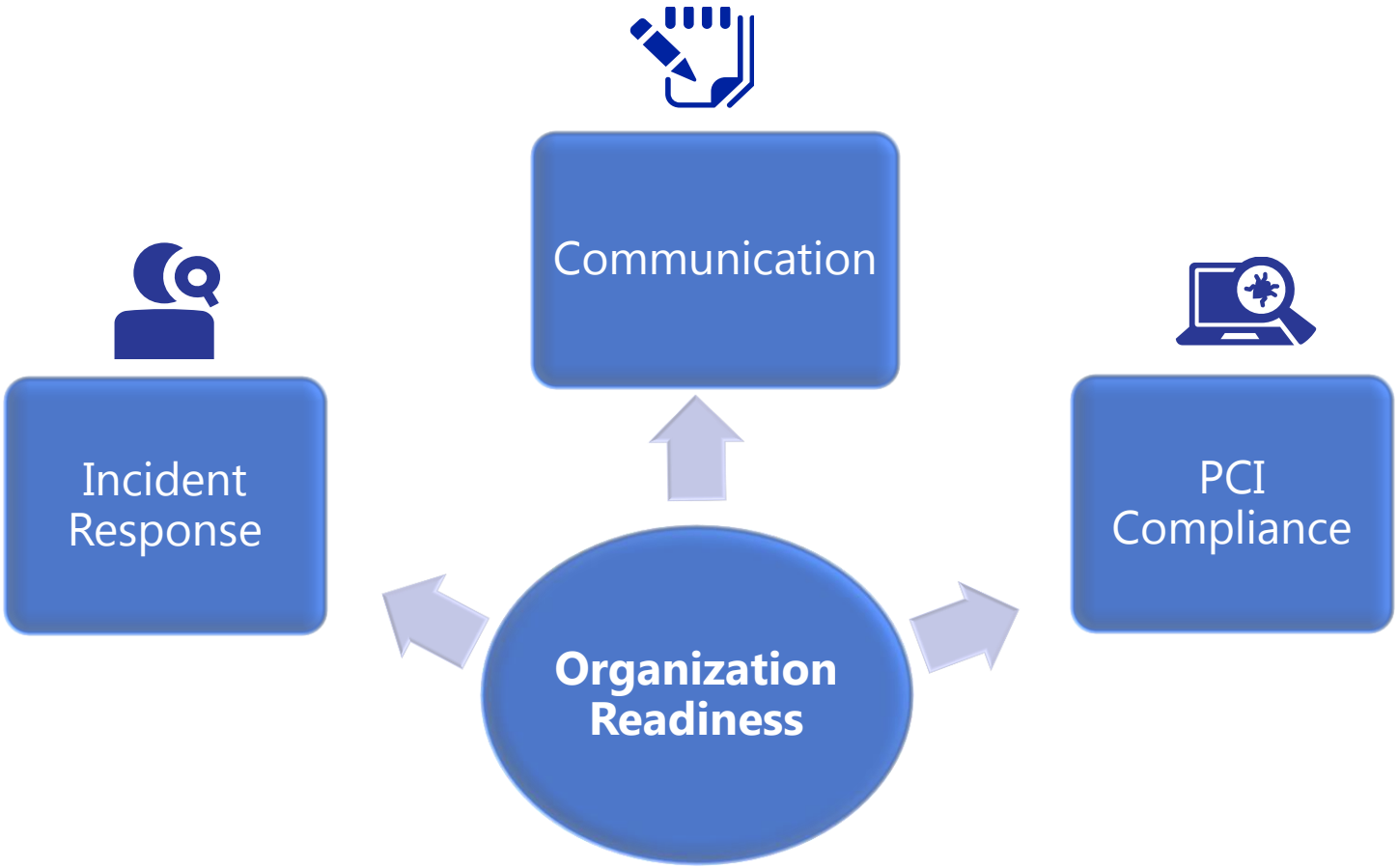
* Market Segment based on Acceptance Solutions MCC "Market Segment" category

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

Investigation Process

Justina Jow, Senior Investigator
Cyber Intelligence & Investigations, Visa Inc.

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**
  - *SSL 3.0 "Poodle" Vulnerability* – 29 October 2014
  - *Fraudulent Credits Trend: ATM Reversals* – 14 August 2014
  - *Insecure Remote Access and User Credential Management* – July 2014

- **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**

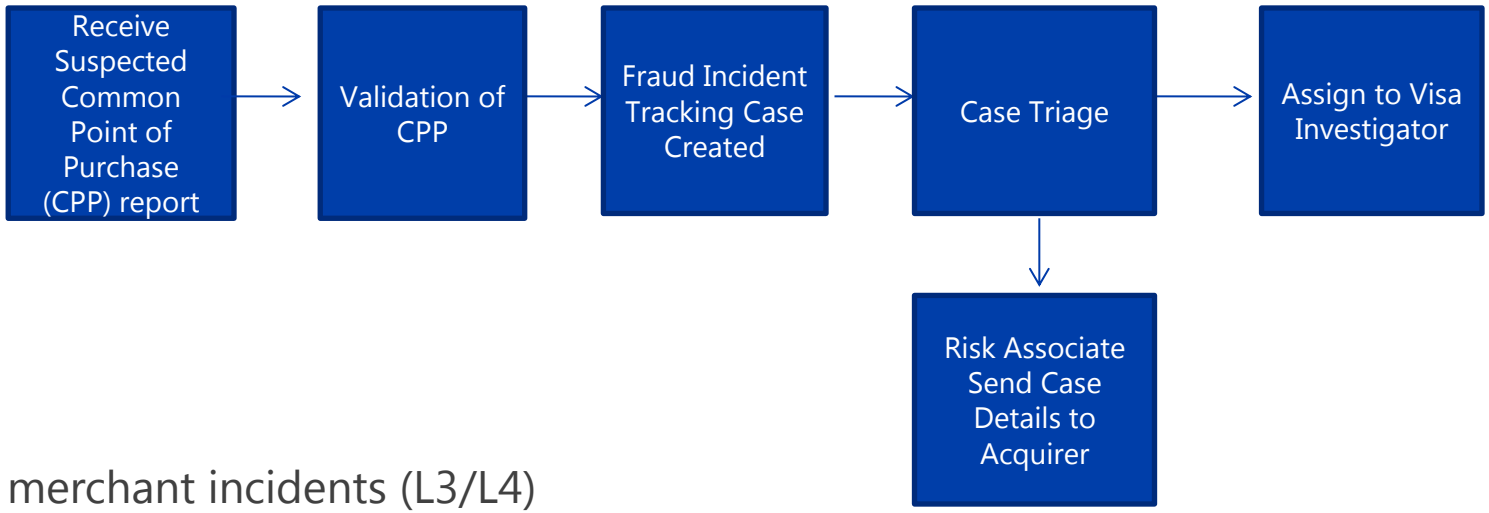
- **Evidence preservation** (page 7 from WTDIC)
  - Do not access or alter compromised systems
  - Preserve all evidence and logs

- **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

Initial Investigation Process



- Small merchant incidents (L3/L4)
  - Visa will notify merchant's acquirer
  - CAMS (PA) alert sent for incidents with ≥ 2 CPPs
  - Acquirer responsible for investigation/containment
  - Acquirer responsible for merchant's PCI compliance

- Visa investigated incidents
  - L1/L2 merchants
  - VisaNet processors/gateways/agents/integrators
  - Regional or national multi-store chains (≥ 25 locations)
  - Any other incident deemed by Visa management to be material

Merchant Responsibilities*

- **Notification**
  - Alert your acquiring bank immediately
- **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**

Upcoming Events and Resources

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

- "BlackPOS" Malware Deconstructed
  - 10 December 2014, 10 am PST
- Secure Technologies for Payments
  - 21 January 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 more…

Questions?