Compromise Event Reporting and Management

Webinar

Emily Shannon, Craig Johnson & Stoddard Lambertson
Visa Fraud and Breach Investigations

October 23, 2019
Disclaimer

Notice

The information, recommendations or “best practices” 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, programs or “best practices” 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

- Fraud and Compromise Trends and Schemes
- Payment Fraud Disruption (PFD) Capabilities
- Visa’s What To Do If Compromised Version 6.0
  - Requirements for a Compromise Event for Members
  - eCommerce Threat Disruption (eTD)
  - Investigations Fees and Non-Compliance Assessments
- Global Investigations Management Tool (GIMT)
- Q&A
Payment Fraud Disruption: At-A-Glance

- First response to major attacks impacting the payment ecosystem, the Visa brand, and/or Clients
- Identification, analysis and disruption of fraud and crime through early detection and alerting
- Operational prevention and response to client, merchant and third-party breaches
- Management of GCAR loss-allocation program - designed to balance the needs of Visa clients in the event of a large-scale account data compromise event
- Advance key law enforcement and industry partnerships, both domestically and internationally
Global Compromise Trends

Unique Cases (Brick & Mortar vs. eCommerce)

Data Source: VIP

ATM Cash Out Attacks By Region

Data Source: Compromise Account Management System (CAMS) 2019* data until September 30, 2019

Unique Events by Region

Data Source: Compromise Account Management System (CAMS) 2019* data until September 30, 2019

Fraud Schemes by Region

Data Source: Global Investigations Management Tool (GIHT) 2019* data until July 31, 2019
Current and Emerging Fraud Trends
Fraudulent Clearing and Settlement and Purchase Return Authorization Messages

Attack Vectors:
• POS Device or Gateway Cloning
• Merchant Account Takeover

Force Post Batches
Criminals program and connect POS devices or gateways to a merchant processing host. The device or gateway appears to be belong to the merchant and is used to submit fraudulent batches for clearing & settlement.

Purchase Return Fraud
(Purchase Return Authorizations)
Cloned POS devices are used to process purchase returns to prepaid cards. Fraudsters send a PRA and issuers increase Open-To-Buy without a corresponding settlement.
Visa Introduces Suite of Security Capabilities to Help Prevent and Disrupt Payment Fraud

8/20/2019

New payment security services to help defend against emerging and evolving threats targeting financial institutions and merchants

SAN FRANCISCO—(BUSINESS WIRE)—Aug. 20, 2019— Visa today announced a suite of innovative security capabilities to help prevent and disrupt payment fraud, breaking new ground in cybersecurity and fraud prevention. The new payment security services and capabilities help protect the integrity of the payments ecosystem by detecting and disrupting fraud targets financial institutions and merchants, as revealed at the Visa U.S. Security Summit 2019, a forum bringing together payment industry experts from risk, business and operational departments of financial institutions, merchants, processors and other payment service providers. The new capabilities are available to Visa clients at no additional cost or sign-up, but through Visa’s continued investments in intelligence and technology. These add to the long list of benefits financial institution and merchant clients enjoy as participants in the Visa global payment network.

“Cybercriminals attempt to bypass traditional defenses by stealing credentials, harvesting data, obtaining privileged access, and attacking trusted third-party supply chains,” said RL Prasad, senior vice president, Payment System Risk, Visa. “Visa’s new payment security capabilities combine payment and cyber intelligence, insights and learnings from breach investigations, and law enforcement engagement to help financial institutions and merchants solve the most critical security challenges.”

According to a global report by Forrester Consulting commissioned by Visa, ATM cashout attacks that exploit vulnerabilities among financial institutions and processors to remove fraud controls to withdraw money from cash machines fraudulently, and automated testing of values and credentials to gain unauthorized access to information and functionality called “enumeration attacks” were among the most prevalent account-related fraud types identified by respondents. At the same time, card-not-present fraud that includes ecommerce, phone and mail orders was found to be less frequent but caused more damage to businesses—representing nearly 40% of fraud losses and operational costs. Managing payment fraud holistically is imperative to meet these challenges.

Protecting the Ecosystem from Threats

At the center of every Visa transaction is trust. As threats evolve, Visa’s payment security capabilities help to holistically protect the core components of the ecosystem—people, data and infrastructure—to maintain trust and connect the world through the most innovative, reliable and secure digital payment network. The new security capabilities add to existing protections and include:

- **Visa Vital Signs** – Actively monitors transactions and alerts financial institutions of potential fraudulent activity at ATMs and merchants that may indicate an ATM cashout attack. To limit financial losses for financial institutions, Visa works automatically and in coordination with law enforcement to shutdown threats as quickly as possible.

- **Real-time ATM Cashout defense**

- **eCommerce Threat Disruption**

- **Proactive identification of eCommerce merchant breaches**

- **Risk Operations**

- **24x7 Operational fraud monitoring for clients worldwide**
Visa’s What to do if Compromised (WTDIC) Version 6.0

WTDIC establishes procedures for reporting and responding to a suspected or confirmed account data compromise event. WTDIC guides entities through critical, required compromise event components and procedures that include:

- Providing notification to Visa
- Conducting an initial investigation and providing an incident report to Visa
- Providing exposed payment account data to Visa
- Managing PCI Forensic Investigation / Independent Investigation as required
- Complying with all client requirements for suspected or confirmed compromise events
- Following eCommerce Threat Disruption (eTD) requirements
- Understanding potential impacts of Investigation Fees and non-compliance assessments (NCAs)

WTDIC should be incorporated into Incident Response procedures as applicable
Compromise Event Reporting Requirements

Submit Notification to Visa Within Three (3) Calendar Days

An entity that suspects or confirms unauthorized access to any Visa payment account data, or to any payment system that stores, processes or transmits Visa payment account data, is required to ensure that the Compromise Event is reported to the Visa Risk Management group within three (3) calendar days of:

(a) the discovery of evidence sufficient to raise a reasonable suspicion of a Compromise Event, or
(b) the discovery of evidence sufficient to confirm the existence of a Compromise Event beyond a reasonable doubt.

Visa Member financial institutions are responsible for ensuring compliance with this requirement by their affiliates, agents and customers.

Notification must be provided to the Visa Risk Management Group regional office listed below:

<table>
<thead>
<tr>
<th>Region</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America (NA)</td>
<td><a href="mailto:USFraudControl@visa.com">USFraudControl@visa.com</a></td>
</tr>
<tr>
<td>Latin America &amp; Caribbean (LAC)</td>
<td><a href="mailto:LACFraudInvestigations@visa.com">LACFraudInvestigations@visa.com</a></td>
</tr>
<tr>
<td>Asia Pacific (AP) and CEMEA</td>
<td><a href="mailto:VIFraudControl@visa.com">VIFraudControl@visa.com</a></td>
</tr>
<tr>
<td>Risk Operations Center 24/7 Emergency Assistance</td>
<td>US: +1-844-847-2106   International +1-650-432-3379</td>
</tr>
</tbody>
</table>

Note: Visa Acquirers with access to Visa’s Global Investigation Management Tool (GIMT) should provide notice via GIMT
New Timeframes for Investigations Management Milestones (simplified)

1. Breach detected and reported to Visa
   - 3 calendar days

2. Merchant Acquirer provides Incident Report and updates case via GIMT
   - 3 calendar days

3. At-risk accounts sent to Issuers via the Compromised Account Management System (CAMS)
   - 3 calendar days

4. Visa Investigator creates case in GIMT

5. Visa Issuers receive at-risk accounts and take immediate action to minimize potential fraud losses

6. Acquirer provides at-risk accounts to Visa
   - 3 calendar days
Financial Institution Attacks Increasing

Specific Member Requirements for suspected or confirmed Compromise Events

- Member financial institutions that suspect or confirm unauthorized access to any Visa cardholder data, including those payment systems that store, process, or transmit cardholder data must comply with WTDIC section 6.

6.1. Visa may require a Member to conduct a PFI investigation and provide the same deliverables described in section 4.

6.1.2. Not all instances necessitate a PFI. Visa may require the following in lieu of or prior to a PCI forensic investigation. These actions are required within three (3) calendar days:

   - If Visa notifies the Member of malicious Internet Protocols (IPs) connections, the Member is required to confirm a firewall block is in place for outbound connections.
   - The Member is required to check network logs for which machines connected to malicious IP addresses and provide access to logs, if requested.
   - The Member is required to scan their network for suspicious activity and perform additional investigation on any machines observed communicating with malicious IPs. Visa may request IOCs e.g. malicious files, including malware samples to support the investigation.
   - The Member is required to document above actions and provide an Incident Report to Visa.
   - The Member is required to monitor and report any suspicious or fraudulent activity on any other payment systems the Member operates including but not limited to, SWIFT, ACH, B2B, and P2P services during the investigation.
   - Visa strongly recommends that an independent third party validate the security of the Member’s network. In certain cases, Visa may require third party validation in order to confirm the Member’s network is secure.
Visa’s **eCommerce Threat Disruption (eTD)** is a fee-free proprietary capability that allows Visa to detect and disrupt eCommerce merchant Compromise Events before fraud is reported.

- **eTD** is a global capability that strives to reduce risk and disrupt fraud related to eCommerce Compromise Events.
- **eTD Fact Sheet** on VisaOnline - Payment Systems Intelligence page.

**Revised WTDIC** provides requirements for Members to follow when a merchant has been identified by eTD.
Compromise Event Reporting and Management

Investigation Fee and Assessment Avoidance Strategies
# Investigation Fees

- Investigation Fees incentivize entities to **fully cooperate** with Visa throughout each phase of the investigation and to complete the investigation in a timely manner.
- Full cooperation during an investigation helps to **quickly contain and mitigate** a Compromise Event and minimize the resulting fraud impacting Visa clients.
- Investigation fees are only **applicable to PFI-lead** investigations.

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>Number of Annual Transactions</th>
<th>Investigation Duration – Grace Period</th>
<th>Investigation Duration – Fee Period</th>
<th>Investigation Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuers</td>
<td>N/A</td>
<td></td>
<td>Four full calendar months (partial months not included)</td>
<td>USD 10,000 per month</td>
</tr>
<tr>
<td>Acquirers</td>
<td>N/A</td>
<td></td>
<td>Monthly fee starts with the fifth full calendar month and continues through every complete calendar month until investigation is complete</td>
<td>USD 10,000 per month</td>
</tr>
<tr>
<td>VisaNet Processors</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 1 – Merchants</td>
<td>&gt;6,000,000</td>
<td>Four full calendar months (partial months not included)</td>
<td>USD 10,000 per month</td>
<td></td>
</tr>
<tr>
<td>Level 1 – Agents for Issuers or Acquirers</td>
<td>&gt;300,000</td>
<td>Four full calendar months (partial months not included)</td>
<td>USD 10,000 per month</td>
<td></td>
</tr>
<tr>
<td>Level 2 – Merchants</td>
<td>1,000,001 – 6,000,000</td>
<td>Four full calendar months (partial months not included)</td>
<td>USD 10,000 per month</td>
<td></td>
</tr>
<tr>
<td>Level 2 – Agents for Issuers or Acquirers</td>
<td>&lt;300,000</td>
<td>Four full calendar months (partial months not included)</td>
<td>USD 10,000 per month</td>
<td></td>
</tr>
<tr>
<td>Level 3 – E-commerce Merchants</td>
<td>20,000 – 1,000,000</td>
<td>One-time fee effective the fifth full month</td>
<td>USD 3,000 flat fee</td>
<td></td>
</tr>
<tr>
<td>Level 4 – Merchants</td>
<td>1 – 1,000,000</td>
<td>Four full calendar months (partial months are not included)</td>
<td>USD 10,000 per month</td>
<td></td>
</tr>
</tbody>
</table>

• Investigation Fees incentivize entities to fully cooperate with Visa throughout each phase of the investigation and to complete the investigation in a timely manner.

• Full cooperation during an investigation helps to quickly contain and mitigate a Compromise Event and minimize the resulting fraud impacting Visa clients.

• Investigation fees are only applicable to PFI-lead investigations.
## Investigation Fee Example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant detects Data Compromise &amp; informs Acquirer May 6</td>
<td></td>
<td></td>
<td></td>
<td>PFI Investigation continues throughout all of October</td>
<td>Acquirer Billed Investigation Fee for month of October</td>
<td></td>
</tr>
<tr>
<td>Acquirer discloses to Visa May 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PFI completes investigation, sends final report Nov 16</td>
<td></td>
</tr>
<tr>
<td>Visa Requests PFI May 9</td>
<td></td>
<td></td>
<td></td>
<td>Fees Apply Full Calendar Month</td>
<td>Visa accepts report, sends IC CAMS and closes case in GIMT Nov 20</td>
<td></td>
</tr>
</tbody>
</table>

**4 Month Grace Period**

**Fees don’t apply in November - Partial Month**

©2019 Visa. All rights reserved. Visa Public.
Non-Compliance Assessments

Members are subject to a non-compliance assessment of USD 100,000 per incident for failing to adhere to requirements specified in WTDIC

- Non-Compliance Assessments (NCA) are avoidable and designed to incentivize swift notification and cooperation during all phases of an investigation.
- NCAs designed to deter entities from failing to comply with the required procedures and timelines for reporting and responding to a suspected or confirmed compromise event.
The Visa difference

Global Investigations Management Tool

Connecting over 2,700 clients globally with a central platform for Investigations management

Intelligence Driven, Predictive, Authoritative
The Visa difference

Global Investigations Management Tool (GIMT) launched in 2018

GIMT
A centralized platform for efficiently managing global investigations and payment card data compromises

Secure
Available on Visa Online for all clients and has built-in security

Central
A central repository for acquirer event management and issuer compromise reporting

Global
Available to issuer and acquirer clients in all countries
Key Benefits

Differentiating Visa from its competitors with immediate benefits for key stakeholders

**Issuers**

- Incentivizes reporting by removing logistical barriers commonly reported by large financial institutions
- Ensures globally consistent reporting with QA performed on all submissions; instantaneous accept/reject responses
- Offers secure transmission and personalized dashboards for Common Point of Purchase reporting

**Visa**

- External investigative platform that provides bi-directional compromise information - key differentiator. Platform for future enhancements.
- Automates select phases of investigations, resulting in rapid notification, containment and CAMS alerts
- Enhances the suite of intelligence capabilities by establishing a centralized platform to notify clients of identifications and threats

**Acquirers**

- Diminishes the burden borne by providing investigative updates that vary in stage and complexity
- Equips acquirers with dashboards that provide a holistic view to improve compromise risk management strategies
- Allows acquirers to update cases with at-risk accounts and to self report new cases
Contacts & Resources: Questions? Comments?

Contact:

• Visa Risk Operations Center 24X7
  US: 1.844.847.2106
  INT: 1.650.432.3379

• Fraud and Breach Investigations:
  NA: usfraudcontrol@visa.com

Resources:

• Visa OnLine: Data Compromise & Fraud Investigations
  • https://secure.visaonline.com/SitePages/Content.aspx?pageid=6.0.1.2.0
  • New WTDIC v6.0 posted on 10 October.

• Visa.com: Visa Data Security Website www.visa.com/cisp
  https://usa.visa.com/support/small-business/data-security.html
  • New WTDIC v6.0 posted on 10 October (view ‘Data Breach Guidelines’).
Data Security Resources

Visa Global Registry of Service Providers [www.visa.com/onthelist]
- List of registered, PCI DSS validated third-party agents

PCI Security Standards Council Website [www.pcissc.org]
- PCI Approved list of Forensic Investigators
- Qualified list of Integrator Resellers
- Data Security Standards
- Qualified Assessor Listings
- Data Security Education Materials
Webinar Survey
Q&A

Visit us at Visa OnLine:
Search for “Data Compromise & Fraud Investigations”

24x7 emergencies:
Visa Risk Operations Center
  US +1.844.847.2106
  International: +1.650.432.3379
Thank you for attending!