Third Party Risk Management Basics

Webinar

26 February 2015

Stan Hui – Payment System Security
Oscar Munoz – Third Party Risk
Roxanne Baumann – Third Party Risk
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
- Merchant Due Diligence
- Third Party Risk
- Agent Registration and the MSSIP
- Questions and Answers
Data Breach Landscape

Stan Hui
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
Recent Threats due to POS Integrators

- POS Integrators support merchant POS software installations
- Typically merchant setup includes Remote Access Services (RAS) for monitoring and software support
- Integrators have access to POS system - however PCI compliance not maintained
- Multiple POS Integrator related compromises since June 2014
- Merchants infected with ‘Backoff’ family of malware
- Remote Access Services and Applications Exploited
  - Currently LogMeIn users targeted (other RAS include: Remote Desktop Protocol, PCAnywhere, TeamViewer and VNC)
  - Brute forces login credentials
  - Creates a ‘backdoor’, logs keystrokes and collects credit card data
  - Extremely low anti-virus detection rates
  - Exfiltration to remote IP addresses
- Non-Compliant Integrators / Merchants set up with default / shared remote access IDs without two-factor authentication or regular password changes
  - Entities not following PCI compliant practices
POS Malware Mitigation Strategies

• Confirm all of your POS vendors, resellers and integrators are employing sufficient measures to prevent attacks and unauthorized access.

• Ensure that overall payment processing environment is securely configured and maintained in accordance with the PCI DSS.
  • Ensure that firewall rules only allow remote access from known IP addresses.
  • If remote connectivity is required, enable it only when needed.
  • Contact your support provider or POS vendor and verify that a unique username and strong password exists for each of your remote management applications.
  • Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment.
  • Plan to migrate away from outdated or unsupported operating systems like Windows XP.

• Remote access applications best practices
  • Enable logging and examine logs regularly.
  • Do not use default or easily-guessed passwords.
  • Restrict access to only the specific IPs and only for established time periods.
  • Only use remote access applications that offer strong security controls.
  • **Always use two-factor authentication.** If remote access is required by your POS integrator, insist on two-factor authentication.
POS Malware Early Warning Signs and Best Practices

- Unexplained remote POS logins - Is it normal for a user to login at 3:00 AM?
- Unexplained outbound HTTP web traffic from the POS
- Look for the existence of new, unexplained executables on the POS

Best Practices

- Identifying, Containing, & Mitigating the Backoff Malware Webinar – 24 September 2014
- Use only PCI Qualified Integrators and Resellers (QIRs)
  - PCI 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
  - QIRs listed by the PCI SSC
    [www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php](http://www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php)
  - Demand that your POS Integrator be qualified and listed by the PCI SSC
  - Will help protect your organization and maintain PCI compliance
Merchant Due Diligence

• Requirement 2.6 – Shared hosting providers must protect each entity’s hosted environment and cardholder data

• Requirement 12.3.9 – Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use

• Requirement 12.8 – Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data
  • 12.8.1 – Maintain a list of service providers
  • 12.8.2 – Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit
  • 12.8.3 – Ensure there is an established process for engaging service providers including proper due diligence prior to engagement
  • 12.8.4 – Maintain a program to monitor service providers’ PCI DSS compliance status at least annually
  • 12.8.5 – Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity

• Requirement 12.9 – Additional requirement for service providers (currently a best practice until 30 June 2015, then it becomes a requirement)
Third Party Risk

Oscar Muñoz
Third Party Agent Program Objective

Visa operates a globally consistent Third Party Agent program across all Visa Inc regions. Its main objectives are:

• Identify payment system participants

• Elevate security and transparency in the Visa payment system
  • Ensures consistent financial, operational, security and reputational due diligence is performed
  • Minimize risk exposure and stakeholder impact arising from compromises
  • Promotes a sound, dynamic payment system
  • Protect the goodwill of the Visa Brand
  • Incents compliance with Visa Rules, industry data security standards and regulatory requirements

Visa Rules require Visa Clients to register all Third Party Agents
Main Players in the Visa Payments Ecosystem

**Third Party Agent (TPA):** An entity, not defined as a VisaNet processor, that provides payment related services, directly or indirectly, to a Visa client and / or stores, processes or transmits cardholder account numbers.

**VisaNet Processor (VNP):** A Visa client, or a Visa-approved non-client who is directly connected to VisaNet, and provides authorization, clearing or settlement services for merchants and / or Visa clients.

**Types of Third Party Agents (TPA):**

- Independent Sales Organization (ISO)
- Third Party Servicer (TPS)
- Merchant Servicer (MS)
- Payment Facilitators (PF)
- Encryption Support Organization (ESO)
- Corporate Franchise Servicer (CFS)
- Distribution Channel Vendor (DCV)
- Instant Card Personalization Issuing Agent (ICPIA)
- Dynamic Currency Conversion (DCC)
Key Initiatives

We group our initiatives into three areas:

- **Education and Awareness**
- **Transparency**
- **Direct Engagement**
Drive Education and Awareness

Empower Third Party Agents and clients with knowledge so that their business thrives

**Third Party Agents**
Help Third Parties stay informed about industry best practices, payment system risk management news and initiatives, and policy information relevant to their businesses

**Clients**
Help clients effectively manage Third Party relationships and mitigate risk to the payments system through supportive documentation – e.g. Visa Global Acquirer Risk Standards Guide, Visa Third Party Due Diligence Risk Standards, etc.
Increase Transparency

Empower clients and merchants to make informed decisions

Visa Global Registry of Service Providers

- Valuable source of information for registered service providers who meet Visa program and industry requirements.

- The listed agents have been registered with Visa by at least one Visa client and certified compliant with Visa and applicable industry standards.
Foster Partnership

Engage Third Party Agents directly and build strong partnerships

Visa Processor and Agent Conference

• Individual breakout sessions specially tailored to Payment Facilitators, VisaNet Processors

• Interactive platform with panel discussions and networking opportunity with Third Party Agents

• Held every two years since 2011
Client Benefits

- Provides an additional risk reduction framework
  - Drives compliance with industry data security standards such as the PCI DSS
  - Establishes a brand risk reduction baseline to mitigate possible bad business practices that may occur in the ISO sales process
- Complements regulatory guidance on the use of third parties
- Faster identification of impacted clients due to a breach
- Invitation to conferences, events, webinars, and data security alerts
Agent Benefits

- Publication on the Visa Global Registry of Service Providers ([www.visa.com/splisting](http://www.visa.com/splisting))
  - The industry source to find registered and compliant agents
  - A dynamic, searchable, exportable, filterable, and interactive directory of agents
  - Includes over 3400 unique agents and growing
  - Promotes services offered providing global visibility
  - Proclaims PCI DSS validated compliance status
  - Differentiator to potential clients

- Access to Information and Resources
  - Visa-hosted events and webinars
  - Visa Online (VOL) access for technical specs, program materials, historical archives

- Visa Business News Email Communication
  - Receive notifications on fraud trends, policy information, industry best practices, and risk related announcements
Agent Registration and the Merchant Servicer Self Identification Program (MSSIP)

Roxanne Baumann
Third Party Agent Registration

TPA Registration 101

The Third Party Agent Registration Program is a Visa-mandated program established to ensure that Visa clients comply with the Visa Rules, Payment Card Industry Data Security Standard (PCI DSS) and other applicable security standards regarding their use of Third Party Agents (TPAs).

Who can register TPAs?

- Only Visa clients can register third party agents with Visa
- Registration must be submitted via the Visa Membership Management (VMM) application
- VMM is an online tool accessible on Visa Online (VOL)
- Agents cannot register themselves
- Agents cannot get listed on the Registry without client registration
- Registration fees are assessed to clients per agent registered
- Agents must be registered by the client even if they are already registered by another client and listed on the Registry (registration fees apply per client)

What about Merchant Servicers?

A Merchant Servicer (MS) agent stores, processes, or transmits Visa account numbers on behalf of the client’s merchants. The MS may have a contract with the merchant but not with the client (the merchant’s acquiring bank). Registration of a MS agent closes the loop between the merchant, processor and acquirer.

- Merchants must ensure the service providers they use are registered by their Visa acquirer
- Merchants should check the Visa Global Registry of Service Providers to see if their service provider is PCI DSS compliant
- Merchants must tell their acquiring bank about the service provider they use so their acquirer can register the agent
- Merchants should direct their service provider to MSSIP
The MSSIP allows Merchant Servicer Agents to easily provide their business information, merchant information and Payment Card Industry Data Security Standards (PCI DSS) compliance validation documentation directly to Visa. In turn, Visa can assist in identifying the merchant’s acquiring bank and facilitate the acquirer’s registration of the Merchant Servicer Agent with Visa. Merchant Servicer Agents that are registered by acquirers, validate compliance via a PCI DSS Attestation of Compliance, and meet program requirements, will be listed on the Visa Global Registry of Service Providers.
Merchant Servicer Self-Identification Program (MSSIP)

**MSSIP Overview**

- MS provides their information to Visa via the MSSIP tool on Visa.com
- Company information, PCI DSS compliance validation materials, merchant customer information (so Visa can identify the merchant’s acquirer)
- Registration by the Visa acquirer, PCI DSS compliance validation via QSA onsite assessment, and MS payment is required before publication on the Visa Global Registry of Service Providers
- MS pays once regardless of how many acquirers are identified and register the agent
- MS revalidates PCI DSS compliance annually in MSSIP and pays annual renewal fee directly to Visa through the tool

MSSIP participants enjoy the following benefits:
- Publication on the Visa Global Registry of Service Providers
- Visa assistance to identify the merchants’ acquiring bank
- One fee per Merchant Servicer agent instead of per acquiring relationship
- Eligibility to subscribe to Visa security alerts, bulletins, publications, resources and documentation
- Invitations to Visa events and conferences
- Access to Visa Online Ability to manage merchant/acquirer relationships

---

**Acquirer Processes**
- MS submits MSSIP case to Visa
- Visa reviews / identifies the Acquirer
- Acquirer registers the MS in VMM
- Acquirer review and due diligence
- Visa notifies MS of acquirer registration
- MS pays fee on or before PCI DSS due date
- Visa notifies MS of acquirer registration
- MS is published on the Registry

---

*Only service providers that validate PCI DSS compliance via QSA onsite assessment are listed on the Registry*
Upcoming TPA / VNP Events and Resources

Visa at the **2015 ETA** in San Francisco – www.electran.org

Save the Date: **2015 Visa Payment Security Symposium** – August 12-13, 2015

**Visa Third Party Agent Website** – www.visa.com/third-party-agent
- Alerts, Bulletins
- Best Practices, FAQs
- Latest News

**The Visa Global Registry of Service Providers** – www.visa.com/splisting
- Payment industry's designated source for information on registered and compliant agents
- Merchant Servicer Self-Identification Program (MSSIP)

**Contact Us:**
- Agent Registration US and Canada: AgentRegistration@visa.com
- Agent Registration Latin America and the Caribbean: AgentRegistrationLAC@visa.com
Upcoming Merchant Events and Resources

**Upcoming Webinars** – Training tab on [www.visa.com/cisp](http://www.visa.com/cisp)
- Data Breach Findings for Small Merchants
  - 25 March 2015, 10 am PST

**Visa Data Security Website** – [www.visa.com/cisp](http://www.visa.com/cisp)
- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

**PCI Security Standards Council Website** – [www.pcissc.org](http://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...