

Minimizing Payment Risks for Merchants Using Integrators/Resellers

Webinar

17 June 2015



VISA

Stoddard Lambertson – Cyber Intelligence and Investigations
Mamie Lee – Third Party and Processor 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 for Small Merchants and Integrators
- Organized campaigns attacking remote access vulnerabilities
- Small Merchant Safeguards and Mitigation
- Merchant Agents and POS Integrators
- Questions and Answers



The Data Compromise Landscape for Small Merchants and their Integrators / Resellers

Stoddard Lambertson



Merchant Data Compromises

Typical data breach and counterfeit cycle



Entry

- Hackers targeting internet-exposed remote access systems as initial intrusion points
- Once in, attackers conduct network reconnaissance using diagnostic tools/techniques to identify systems with access to payment data and isolate specific user accounts
- They create custom attack scripts and tools to further extend access

Card data theft

- Payment card data is extracted with specialized, difficult to detect malware
- Malware is named to appear as legitimate security software in some cases
- Stolen card data is encrypted to avoid detection
- In many recent intrusions, traces of attacker activity are removed, including self-deleting malware

Monetization

- Payment data is used to commit fraud, often across countries via coordinated criminal activity
 - ATMs
 - Gift cards
 - High-value goods
- Cards carry a typical value of between US\$20–US\$60 on underground markets

Note: There may be a significant lag between a breach and monetization

Current Compromise Landscape

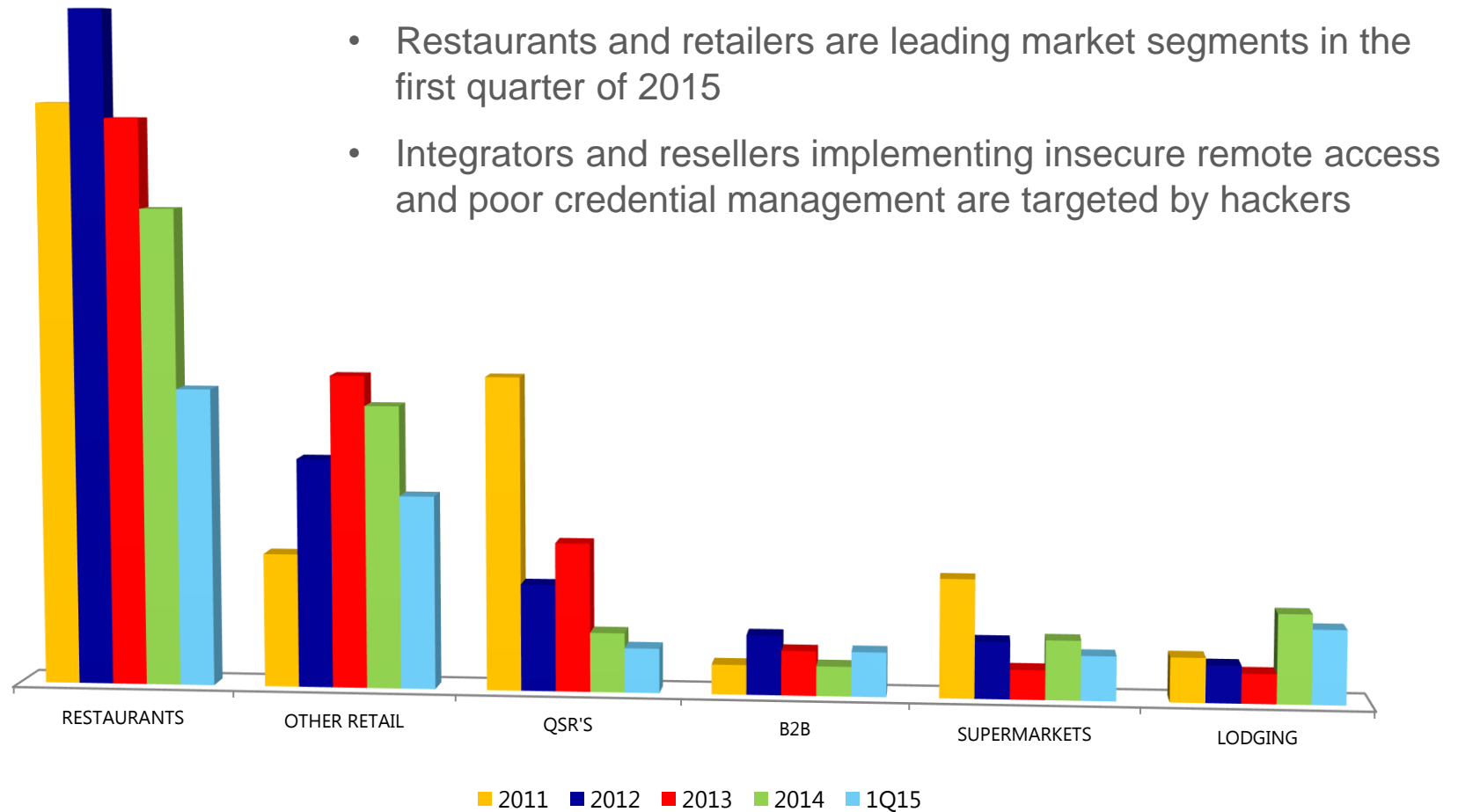
Remote access services used by small brick-and-mortar merchants

- POS integrators / Resellers and Level 4 brick-and-mortar merchants were the most common victims of payment card data theft over the last 18 months
- Concerted criminal effort to target the smallest companies in the payment system
- Targeted attacks on POS Integrator / Resellers to obtain Remote Access credentials of small merchants
- Untrained integrators that deploy weak remote access configurations are the most common reason for small merchant compromises
- Most POS devices affected by these attacks are PC based POS solutions equipped with card readers and applications that are used by merchant staff, such as restaurants, however multiple verticals affected
- Common attack vector: web-based and direct remote access services used by POS Integrators and Resellers



Visa Inc. CAMS Compromise Events

Top Market Segment* (MCC)



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

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

Visa Security Alert – Integrators Under Attack

www.visa.com/cisp



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



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.

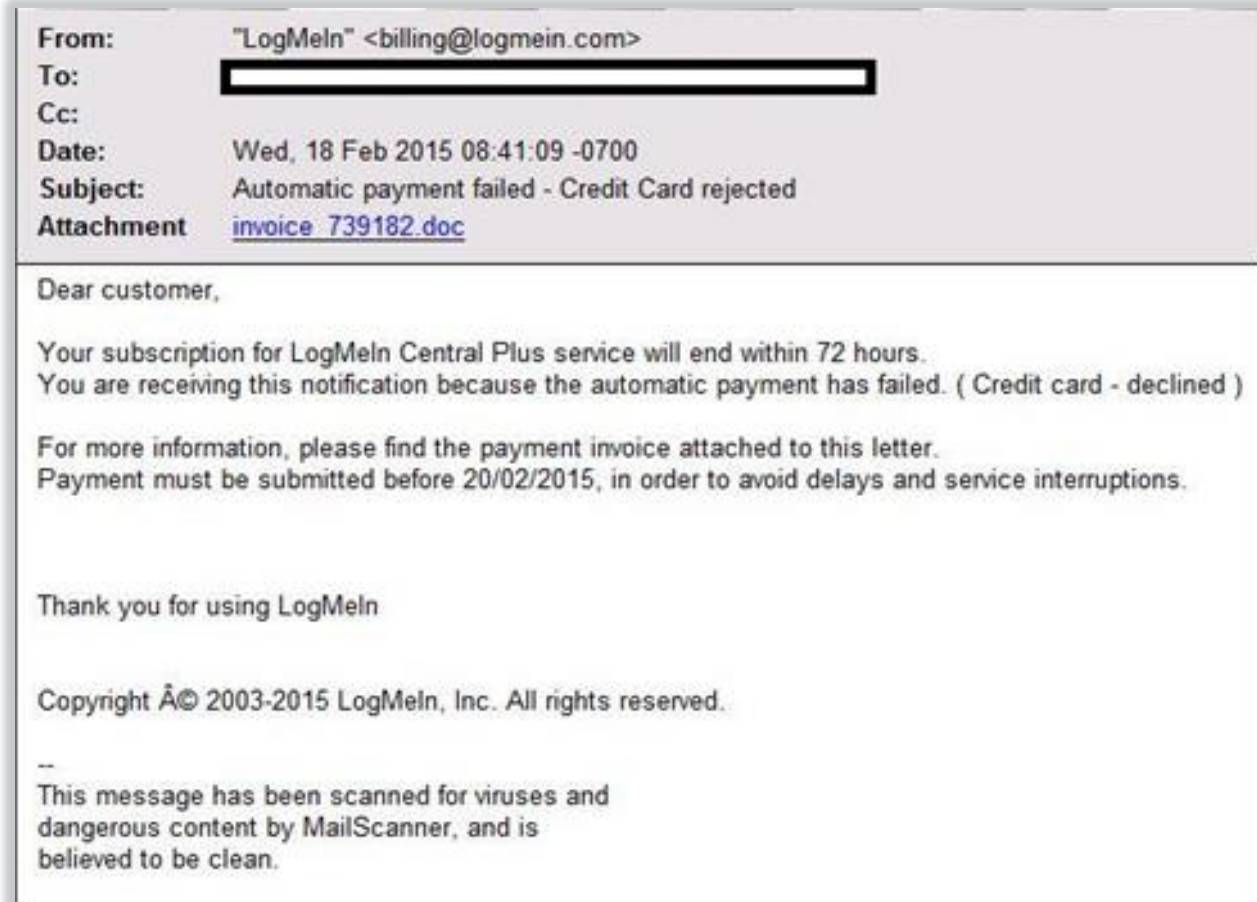
Visa has observed a considerable increase in malicious remote access activity associated with unauthorized access to merchant Point-of-Sale (POS) environments via POS integrators. POS integrators are businesses that resell, install, configure, and maintain POS software and hardware for many different 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

Organized Campaigns Attacking Remote Access

POS Integrators / Resellers are the target

- Recent account data compromise events have been traced back to spoofed LogMeIn phishing emails which then leads to the compromise of user credentials at the POS integrator

The emails often contains either a malicious link or an attached document with a malicious payload that implants malware or steals LogMeIn usernames and passwords



Organized Campaigns Attacking Remote Access

POS Integrators / Resellers are the target

- Once the credentials are stolen, the attacker traverses the POS integrator network to access to the integrator's merchant customer base, thus infecting merchant POS systems with "RAM scraping" malware designed to collect payment card track data
- Used correctly, remote management applications are an efficient and cost effective method of providing technical support among large numbers of merchants
- However, if exploited, they potentially expose payment card data and other sensitive information to cybercriminals
- Insecurely deployed remote access applications create a conduit for cybercriminals to log in, establish additional "back doors" by installing malware, and steal payment card track data
- The risk of data compromise is increased when remote access applications are configured in a manner that does not comply with the Payment Card Industry Data Security Standard (PCI DSS)

FindPOS Malware

Common family of Malware

- The most common family of POS malware attached to these phishing attacks is called by several names, including “FindPOS”
- Two sites that explain the behavior of this malware are:
 1. <http://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/>
 2. <http://blogs.cisco.com/security/talos/poseidon>
- Both sites contain numerous helpful Indicators of Compromise (IOCs)
- Integrators and Resellers should carefully review these IOCs as part of their general information security practices

Types of POS malware functionality

- RAM-scraping
- Keystroke logging
- Command-and-control communication
- Data exfiltration
- Download additional data (tools, scripts)
- Upload keystroke logs
- Malware kill switch – self deletion and anti forensics

PCI Data Security Standard – Remote Access

Requirement 8: Identify and authenticate access to system components

- Merchants must understand their part to protect their business and customer cardholder data
- Ensure your Integrator / Reseller is an approved PCI QIR and work with them to ensure your remote access is compliantly configured
- Remote access solutions are commonly used to provide remote management and support for retailers e.g., LogMeIn, PCAnywhere, VNC, and Microsoft Remote Desktop
 - *Understand how to use them securely and only use remote access applications that offer strong security controls*

PCI Data Security Standard 8.3

Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).



Remote Access Vulnerabilities

Remote access vulnerabilities that are enabling attackers to gain access to merchant POS environment

- **Remote access services always on and available on the Internet** - An attacker only needs to perform a port scan against a merchant's IP address space to identify potential targets of opportunity. *Remote access applications running all the time are particularly at risk of attack.*
- **Single-factor authentication** - Remote access can be vulnerable to brute force and password-guessing attacks, particularly when authentication only requires a username and password.
- **Outdated or un-patched applications and systems** - Older versions of application and operating system software are known to be susceptible to attack and are easily exploited to gain unauthorized access.
- **Use of default passwords or no password** - Using default settings and passwords to access system components will increase the likelihood of a compromise. New hardware devices and software generally arrive from vendors configured with default settings. These default settings must be changed prior to production deployment, as they can be easily guessed and information about these settings is readily available on the Internet.
- **Use of common usernames and passwords** - Often, a vendor or service provider will use a common username and password at multiple client locations to facilitate service calls
- **Improperly configured firewalls** - In some cases, the POS system has a public IP address that is directly accessible from the Internet

Note - most of these are violations of the PCI DSS

Mitigation

Security Practices to Help Mitigate this Threat

- Always use two-factor authentication for remote access - Two factor authentication can be something you *have* (a device) as well as something you *know* (a password)
- Ensure proper firewalls rules are in place, only allowing remote access from known IP addresses
- If remote connectivity is required, **enable it only when needed** - Contact your POS vendor or integrator to take immediate steps to disable remote access when not in use
- Restrict access to only the service provider and only for established time periods
- Contact your POS Integrator and verify that a unique username and 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
- Enable logging in remote management applications and examine the logs regularly for signs of unknown activity
- Do not use default or easily-guessed passwords
- Only use remote access applications that offer strong security controls
- Plan to migrate away from outdated or unsupported operating systems like Windows XP

Examples of Small Merchant Security Safeguards

Protect your business and take these steps

1



**Change
Default
Passwords**

2



**Only enable
remote access
with 2 factor
authentication**

3



**Only Enable
Remote
Access When
Needed**

4



**Use only PCI
Approved QIRs**

5



**Use only
Visa
Listed
QIRs**

Ease of Implementation	Easy	Easy	Easy	Easy	Easy
Cost	None	None	None	None	None
Effectiveness	Medium	High	High	High	High

Implement Secure Technology

- Benefits of EMV Chip 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

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.

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

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

Implement Point to Point Encryption



- Secures the payment card transaction from swipe to processor
- Implement an approved PCI PTS terminal
- Reduces overall PCI scope

Merchant Agents and POS Integrators

Mamie Lee



Payment Card Industry Security Standards Council

Qualified Integrators and Resellers (QIR) Program

Program Overview

- The QIR Program provides payment application developers, integrators and resellers with the training to help merchants and industry participants **install** and **configure** validated PA-DSS **payment applications** in a manner that **ensures PCI DSS compliance**.
- The training program outlines the challenges surrounding payment card **security** and explains how the integrator or reseller should remediate them.
- By completing the training program, the integrator or reseller will know how to **access, install, maintain and support payment applications** (and dependent software) **securely** and in accordance with the information provided by the application vendor in the implementation guide to ensure the **merchant** maintains **PCI DSS compliance**.
- Integrators and resellers that successfully complete the program will be listed on the list of **PCI SSC Approved Qualified Integrators and Resellers**.
www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php
- Visa will list a QIR on the **Visa Global Registry of Service Providers**
www.visa.com/splisting

Why Use a QIR?

Visa Recommends

- Only using the QIRs listed on the PCI SSC QIR website to ensure a merchant's PCI DSS compliance status is not jeopardized
- Help protect your organization and improve **security**
- **Simplify** the vendor selection process

The screenshot shows the PCI Security Standards Council website. The header includes the PCI Security Standards Council logo, navigation links (Home, Contact, FAQs, Change Your Language), and a search bar. Below the header is a navigation bar with links: For Merchants, PCI Standards & Documents, Approved Companies & Providers, Training, News & Events, About Us, and Get Involved. The main content area is titled 'QIR Companies' and features a sidebar menu with links: Overview, U.S. EMV VAR Qualification Program, Verify QSA Employee, Qualified Security Assessors (QSA), Payment Application QSAs (PA-QSA), and Approved Scanning Vendors (ASV). The main content area has a search bar with the text 'Search by Company Name, Place of Business and Supported Languages.' and a search button. Below the search bar, it says 'Results: 6' and 'Page: 1'. A table of results is shown with columns: Company, Place of Business, Primary Contact, and Supported Languages.

Company	Place of Business	Primary Contact	Supported Languages

PCI SSC 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:

1. Amano McGann, Inc.
2. eMazzanti Technologies
3. Fujitsu Services Limited
4. Reliant Info Security Inc.
5. Traffic & Safety Control Systems, Inc.
6. Xpient Solutions LLC



www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php

**Special Visa promo code for discounted pricing for the QIR program:
VISA50%OFF**

- **\$197.50** per professional
- Sponsor companies must apply and be approved through the standard process
- Promo code available through **August 11, 2015**

Merchant Agents

POS integrators are merchant agents

- A **Merchant Servicer** (MS) agent stores, processes, transmits, **or has access** to 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 POS integrators they use are **identified** and **listed** on both:
 - PCI SSC **Qualified Integrators and Resellers**
 - **Visa Global Registry of Service Providers**
- For QIRs who self-identify to Visa in **2015**, Visa will **waive** the program **fee**
- Merchants should partner with their **acquirers** to ensure their merchant agents are directed to the PCI SSC for **QIR** program information and to the Visa **Merchant Servicer Self-Identification Portal** for program information and self-identification.

<https://mssip.visa.com/>

Visa Global Registry of Service Providers

- The Visa Global Registry of Service Providers includes **3,400** entities who have met **industry security** and **Visa program** requirements.
- To support the PCI SSC QIR 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.” Merchant servicers have a contract with a client’s merchant, but not necessarily with the client.
- Visa will **not** require **clients** to **register** Qualified Integrators and Resellers.


www.visa.com/splisting



Visa Global Registry of Service Providers

First QIR Listed on both the PCI QIR and Visa Global Registry


Traffic & Safety Control Systems, Inc.



Visa Global Registry of Service Providers

[Home](#)[Learn More](#)[Search Service Providers](#)

Search for specific service providers using a variety of filters. Simply use the select boxes below to narrow your search. You can filter by Company Name, State, Region of Operation, Services, Assessor or Validation date range.

SEARCH CRITERIA 

COMPANY	SERVICE PROVIDER TYPE	VALIDATION TYPE
Traffic & Safety Control Systems, Inc.	AGENT	QUALIFIED INTEGRATOR RESELLER
MI, U.S.A.		


QIR Companies

• [QIR Feedback](#)

Search by Company Name, Place of Business and Supported Languages.

Company Name



Traffic & Safety Control Systems, Inc. 

Results: 1

Company

Place of
Business

Traffic & Safety Control Systems, Inc.

North America

Visa Data Security Bulletin – www.visa.com/cisp

Visa Recommends Using PCI SSC Qualified Integrators and Resellers



VISA SECURITY BULLETIN

15 April 2015

VISA RECOMMENDS USING PCI SSC QUALIFIED INTEGRATORS AND RESELLERS

Distribution: Acquirers, Issuers, Processors, Merchants, Agents

Who should read this: Information Security, Compliance, and Risk

In response to recent merchant breaches caused by payment applications improperly installed by integrators and resellers, the Payment Card Industry Security Standards Council (PCI SSC) has developed the Qualified Integrators and Resellers Program to provide these entities with guidelines, training and certification.



2015 Visa Payment Security Symposium

The Power of Partnership

Securing the Future of Commerce Together

August 12-13, 2015

Hyatt Regency Hotel
Burlingame, CA



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 Security Events and Resources

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

Visa Launches EMV Chip Education Tour for Small Businesses

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

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

- Streamline your chip migration – www.VisaChip.com/businessstoolkit

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...

Resources For Managing Third Party Agents

Merchant Servicer Self-Identification Program – <https://mssip.visa.com/>

- Self-identify to Visa as a merchant agent
- Complete the PCI SSC QIR program

PCI SSC Approved Qualified Integrators and Resellers –

https://www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php

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)

Visa Third Party Agent Website – www.visa.com/third-party-agent

- Alerts, Bulletins
- Best Practices, FAQs
- Latest News

Contact Us:

- Agent Registration US and Canada: AgentRegistration@visa.com
- Agent Registration Latin America and the Caribbean: AgentRegistrationLAC@visa.com

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 - www.visa.com/cisp

- *Insecure Remote Access and User Credential Management - June 2015*
- *Visa Recommends Using PCI SSC Qualified Integrators & Resellers - April 2015*
- *"RawPOS" Malware Targeting Lodging Merchants – March 2015*
- *Carbanak Advanced Persistent Threat – March 2015*
- *Identifying & Mitigating Threats to E-commerce Payment Environments – April 2015*

Ensure a Incident Response plan is in place

- Know what steps to take
- Know who and when to call
 - Sponsoring Visa Acquirer Bank
 - Integrator and Reseller, Law Enforcement

Contact Us

- Visa Cyber Intelligence and Investigations – USFraudControl@visa.com

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

Questions

