Data Security Basics for Small Merchants

28 October 2015

Stan Hui – Director, Merchant Risk
Lester Chan – Director, Merchant 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.

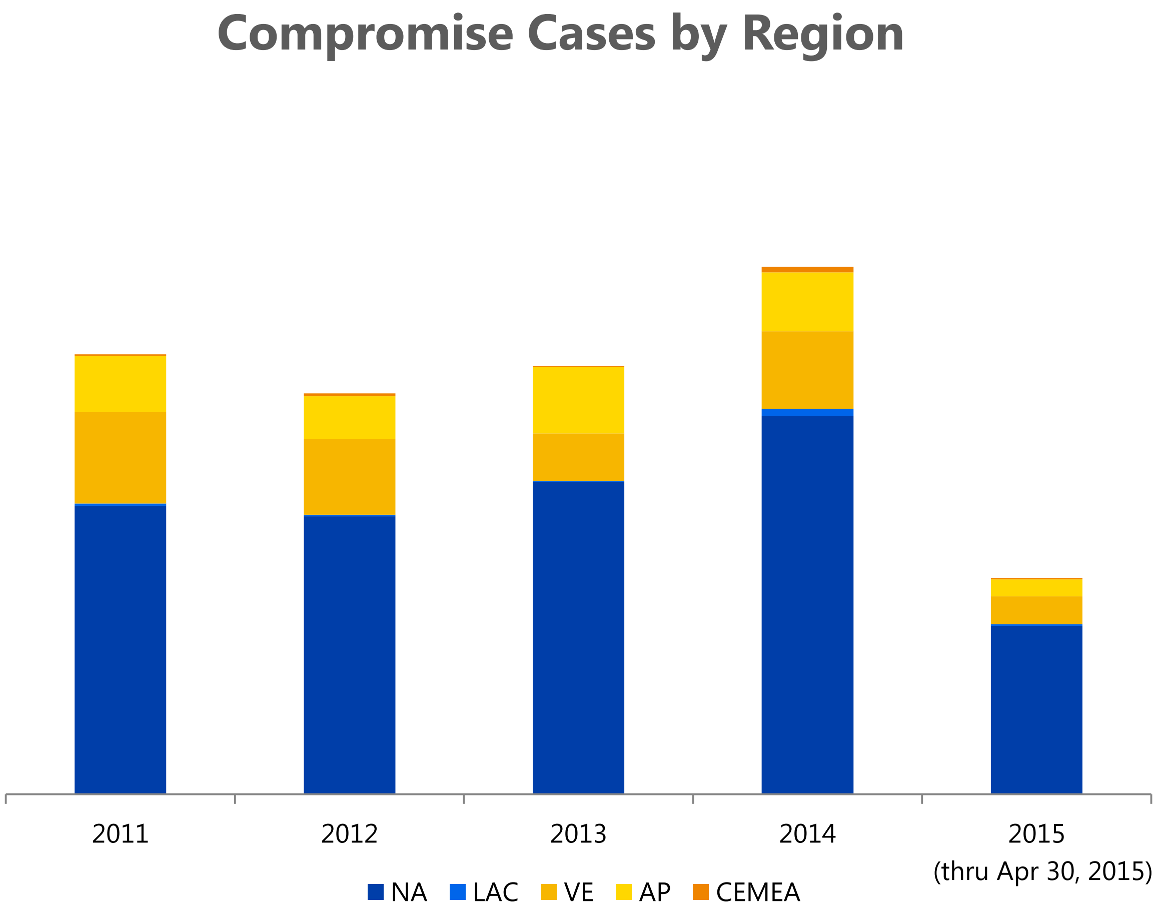
Agenda

- Compromises and Small Businesses
- Impacted Industries and Merchants
- The PCI Data Security Standard
- All Stakeholders Have A Role
- Small Business Challenges and Security Basics
- Utilizing Secure Technologies and Service Providers
- Key Takeaways
- Resources

Global Data Compromise Landscape and PCI Data Security Standard

Stan Hui – Director, Merchant Risk

Global Data Compromises



- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- Payment ecosystem attackers continue to target POS integrators via third-party IT support connections
- Targeting of hotel industry merchants is accelerating and we are seeing technical similarities in the POS malware used across multiple hotel breaches, possible indication of an organized campaign against hotels

Global Data Compromises

Breach trends by merchant level and Merchant Category Code

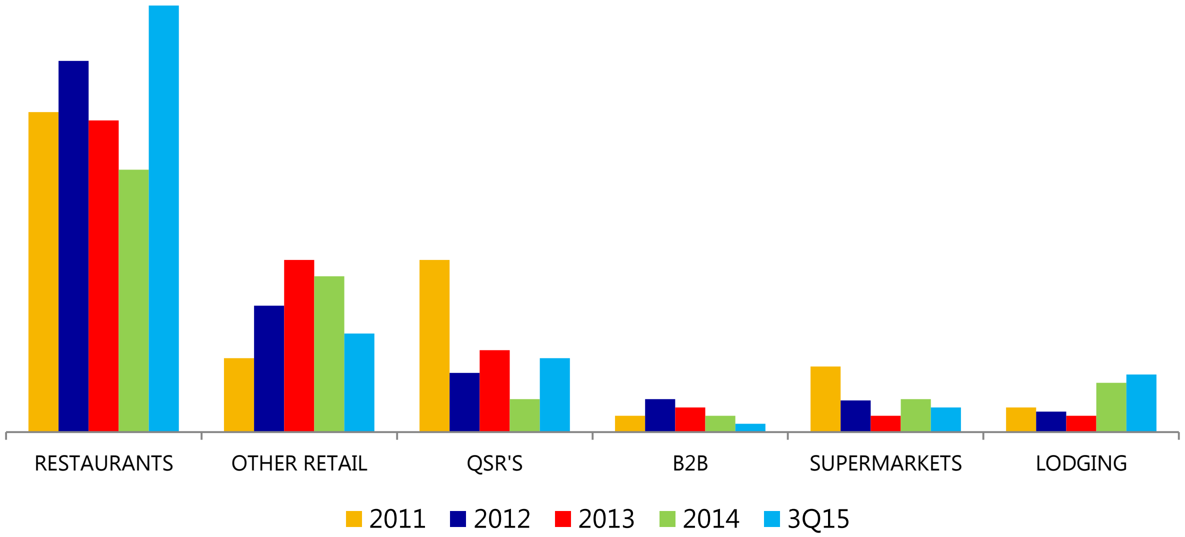
Breach Events by Merchant Level

Entity Type		2012	2013	2014	2015*
		%	%	%	%
Merchant	Level 1	<1%	1%	1%	<1%
	Level 2	<1%	1%	1%	<1%
	Level 3	1%	4%	4%	4%
	Level 4	95%	92%	93%	93%
Agent		<1%	1%	1%	2%
Other		2%	<1%	0%	0%
Total		**100%**	**100%**	**100%**	**100%**

- While level 4 (small) merchants account for the largest number of known breach events (94% to date in 2015), the largest impact comes from Level 1 (large) merchant breaches

Source: Compromised Account Management System (CAMS); data is for Visa Inc. only and represents breach events for which a CAMS was sent.
*Data as of April 30, 2015

Percent of Breach Events by MCC



- Restaurants and "other retail" make up the biggest portion of total known breaches (over 50% and 10%, respectively, in 2015)
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs
- High-volume restaurants and retailers continue to be targeted

Who Are The Targets?

Hackers and fraudsters target specific industries and victims

Small Businesses

- Large population (~5MM+)
- Low/no security controls

Actionable Items

- Implement secure technology – EMV chip, P2PE, tokenization
- Perform security basics: password management, patching systems / applications
- Employ a Qualified Integrator / Reseller (QIR)

Integrators & Resellers

- Frequently targeted by hackers
- Improper Point-of-Sale (POS) implementation
- Always-on remote access connectivity
- Common username / passwords

Actionable Items

- Become a QIR
- Ensures PCI DSS and PA DSS applications are installed properly

Hospitality Industry

- Increased focus on hotels and restaurants
- Typically, back of house servers or property management systems
- Common breach methods include social engineering or spear phishing attacks
- Malware on systems allows attackers to gain access

Actionable Items

- Deploy anti-malware and file integrity monitoring tools

PCI Security Standards Council (PCI DSS)

Security Standards Council®

- Industry-wide standards group founded in 2006
  - Visa, American Express, Discover, JCB and MasterCard
- Responsible for development and management of PCI Security Standards
  - PCI DSS, PA-DSS, P2PE and PTS
- Trains and certifies data security companies and personnel
  - QSA, PA-QSA, ISA, PCIP, PFI, and ASV
- Trains and certifies service providers on the secure installation of PA-DSS validated payment applications
  - Qualified Integrators and Resellers (QIR)
- PCI Data Security Standard applies to any entity that stores, processes, or transmits cardholder data
  - Version 3.1 released April 2015

www.pcisecuritystandards.org

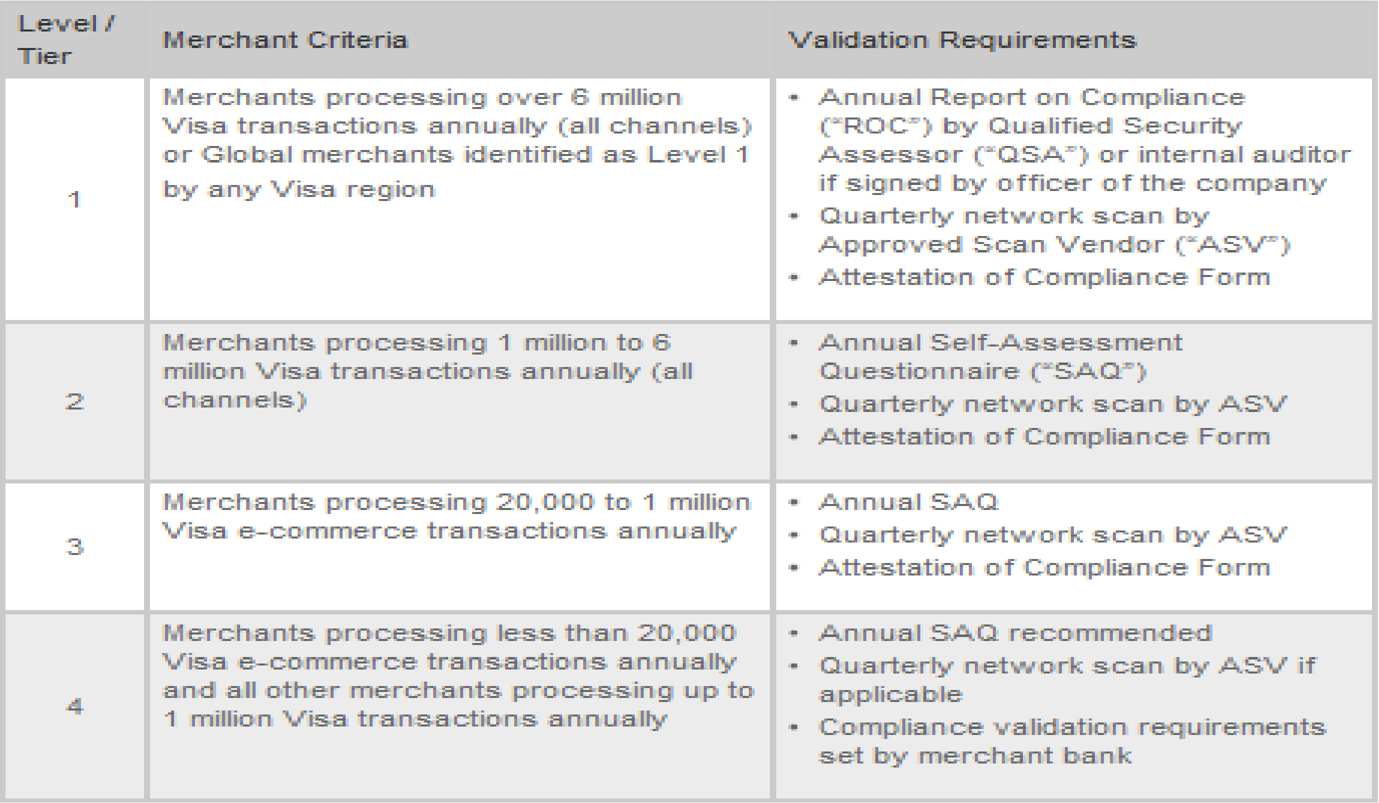
Roles and Responsibilities

- PCI Security Standards Council
  - Manages and maintains the standards and validation tools
  - Answers questions regarding the intent of the standards
- Visa
  - Works with banks to ensure merchants and service providers protect cardholder data in accordance to the PCI DSS
  - Manages data security compliance programs
- Merchant Bank (Acquiring Bank)
  - Ensures merchants are PCI DSS compliant
  - Establishes validation requirement for Level 4 merchants
- Merchant
  - Responsible for protecting their customers’ cardholder data according to the PCI DSS
- Service Provider
  - Must be registered with Visa and be PCI DSS compliant

Source: Tips and Tools for Small Merchant Businesses – www.visa.com/cisp

Merchant Classification and Validation

- Visa has prioritized and defined levels of compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the payment system by merchants and service providers.
  - Merchant classification process should account for all DBAs and sub-business units;
  - All processing channels (brick-and-mortar, e-commerce, mail order/telephone order, etc.)



Level / Tier	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region	• Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or internal auditor if signed by officer of the company • Quarterly network scan by Approved Scan Vendor ("ASV") • Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	• Annual Self-Assessment Questionnaire ("SAQ") • Quarterly network scan by ASV • Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	• Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	• Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by merchant bank

Compliance vs. Validation

- Compliance is required of all entities that store, process, or transmit Visa cardholder data, including financial institutions, merchants and service providers
  - PCI DSS compliance applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce
  - Visa's data security programs are designed to ensure compliance with the PCI DSS
- Separate and distinct from the mandate to comply with the PCI DSS is the validation of compliance
  - Validation is a process whereby entities verify and demonstrate their compliance status
  - It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained
  - Point-in-time assessment
  - Internal assessment vs. Qualified Security Assessor
  - Report on Compliance vs. Self-Assessment Questionnaire
  - Validation documentation sent to merchant bank

Small Business Challenges with PCI DSS and Security Basics

Lester Chan – Director, Merchant Risk

Top Concerns by Small Business Owners

According to State of Small Business Report*

Growing Revenue

Government Regulations

Hiring New Employees

Cash Flow

* 2015 State of Small Business Report

Small Businesses Challenges with PCI DSS

Challenges with understanding PCI DSS

- Long and complicated
- Unsure which requirements are applicable
- Too much technical jargon, acronyms
  - QSA
  - SAQ
  - CDE
  - Etc.

- Lack of resources
  - Time
  - People
  - Budget
- Unsure how PCI DSS relates to securing their business
- Need to better understand risks

- Needs to be easy to understand
- Simple and concise
- Understand the purpose and importance of data security

Importance of PCI DSS for Small Businesses

Impacts and costs of a data breach*

- Cost of forensic analysis and report - $20,000 - $50,000
- Notification to customers can be thousands of dollars
- Credit monitoring and counseling services to impacted customers
- Fines and assessments by Payment Card Brands for breach
- Legal liability and potential lawsuits
- Cost of reissuing payment cards may be levied by banks
- Cost of upgrading POS system
- Loss of consumer confidence
- Negative publicity and press

* Cost of Data Breaches for Small Businesses

Small Merchant Security Basics

Effective, cost efficient and easy to implement

	1 Change Default Passwords/Use Strong Passwords	2 Disable always-on remote access	3 Update system and application patches	4 Use only PCI approved qualified integrators/resellers	5 Conduct training and awareness for employees
Ease of Implementation	Easy	Easy	Easy	Easy	Easy
Cost	None	Low	None	Low	None
Effectiveness	Medium	High	High	High	High

Data Security Next Steps

Beyond basics

Install, configure, and maintain a firewall

Segment cardholder data environment

Implement two-factor authentication for remote access

Install and update anti-virus

Install file integrity monitoring

Control access to payment card data

Implement Secure Technology

EMV Chip Terminals

- EMV chip have an embedded microchip
- Generates a dynamic one-time use code (a cryptogram)
- Prevents the data used to create counterfeit cards
- Reduces overall PCI scope

Tokenization

- Replaces PAN with unique digital token
- Avoids the risk of storing PAN data
- Devalues payment card data

Point to Point Encryption

- Prevents PAN from being intercepted and stolen
- Implement an approved PCI PTS terminal
- Reduces overall PCI scope

Liability Shift

- Effective October 1, 2015, counterfeit liability shift 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.

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

Small Merchant Data Security Incentives

- In May 2014, introduced incentive program in high risk markets to increase use of more secure acceptance solutions by small merchants*
  - Acquirers granted **Safe Harbor** from fines in the event its merchants experience a data compromise
  - To attain safe harbor, compromised merchant must prove implementation of at least one of the following within the 12 months prior to the incident**:

Card Present Merchants	
Option	**Description**
1	Fully enabled EMV terminals at all acceptance locations
2	Visa Ready approved mPOS vendor solution at all acceptance locations
3	PCI-validated P2PE solution
4	PCI DSS onsite validation with QSA or ISA

Card Not Present Merchants	
Option	**Description**
1	PCI-validated **fully hosted** payment gateway or digital wallet
2	PA-DSS validated application, annual network and application pen-test, and quarterly data discovery scan
3	PCI DSS onsite validation with QSA or ISA

* Small merchants defined as Level 3 or Level 4 merchants

** Solutions and eligible merchants may be adjusted based on risk conditions within geography

PCI SSC 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**.

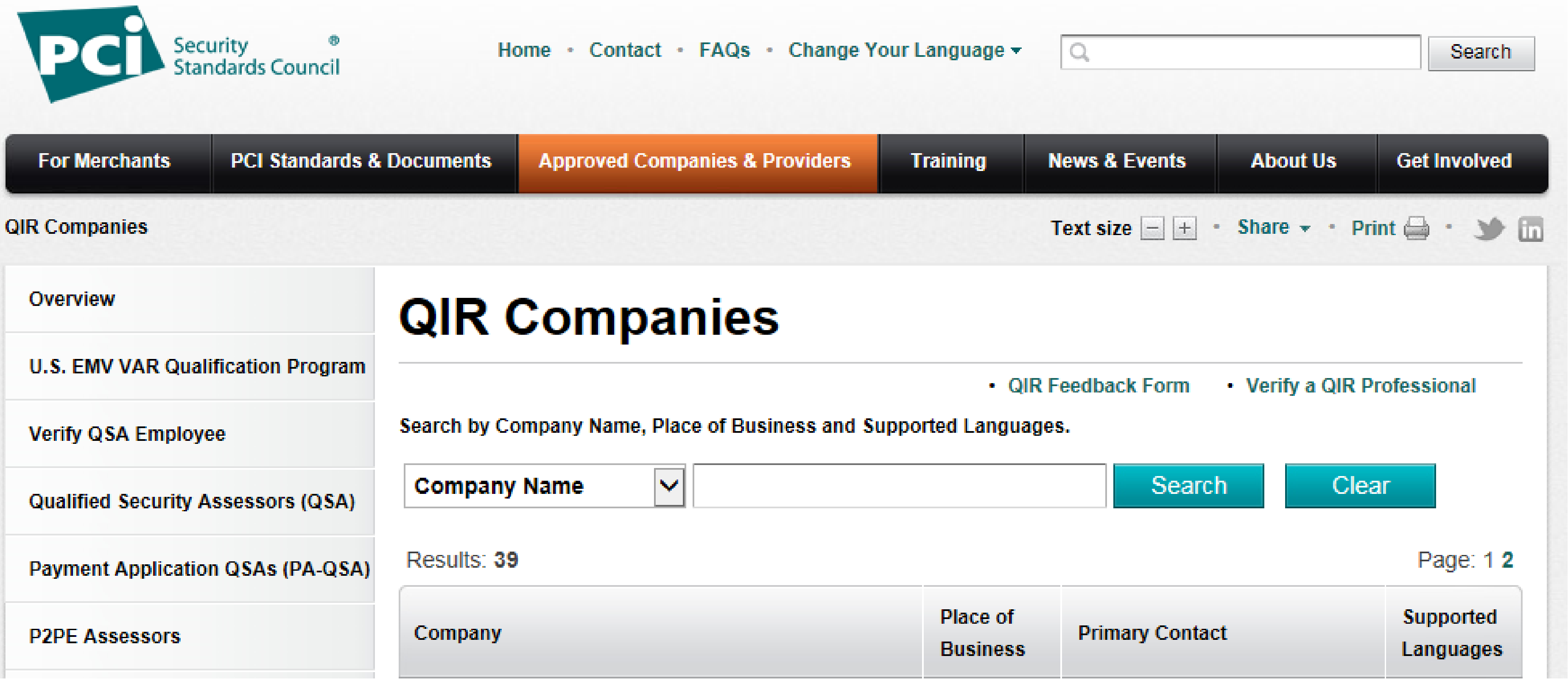
  www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php
- Visa will list a QIR on the **Visa Global Registry of Service Providers**

  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



PCI Security Standards Council
Home
Contact
FAQs
Change Your Language
Search
For Merchants
PCI Standards & Documents
Approved Companies & Providers
Training
News & Events
About Us
Get Involved
QIR Companies
Text size
Share
Print
Overview
U.S. EMV VAR Qualification Program
Verify QSA Employee
Qualified Security Assessors (QSA)
Payment Application QSAs (PA-QSA)
P2PE Assessors

QIR Companies

- QIR Feedback Form
- Verify a QIR Professional

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

Company Name | Search | Clear

Results: 39 Page: 1 2

Company	Place of Business	Primary Contact	Supported Languages

Key Takeaways

- Merchant breaches continue to occur
- Small businesses, integrators / resellers and hospitality continue to be targets
- Understand the risks to your business, threats, and how data can be fraudulently stolen
- Implement easy, low-cost, effective security basic controls
- De-value payment card data with EMV chip, tokenization, and P2PE
- Remove cardholder data from your environment
- Use a PCI DSS validated service provider if you are outsourcing

Resources

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, P2PE, and PTS
- Programs – QSA, ASV, PA-QSA, PFI, ISA, PCIP, and QIR
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…