PCI Council Small Merchant Security Resources

4 August 2016

Sylvia Auyeung, Director, Merchant Risk
Lester Chan, Director, Merchant Security
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

• Global Data Compromises
• PCI Council Small Merchant Taskforce and Materials
• Guide to Safe Payments
• Common Payment Systems
• Questions to Ask Your Vendor
• Key Takeaways
Global Data Compromises

Breach trends by merchant level

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>Level 1</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Level 2</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Level 3</td>
<td>1%</td>
<td>4%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Level 4</td>
<td>95%</td>
<td>92%</td>
<td>93%</td>
<td>92%</td>
</tr>
<tr>
<td>Agent</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>&lt;1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- At-risk accounts in 2015 were largely attributed to L4 merchants
- Level 4 merchants outnumber L1s in the US

• Fewer level 1 and 2 breaches in 2015
• Threat actors are targeting smaller interconnected merchants in large numbers
• Restaurants and “other retail” make up the biggest portion of total known breaches
• Quick service restaurants, supermarkets, and lodging make up the other top MCCs
Small Merchant Taskforce as a Merchant Resource

Formed to help improve payment data security for small businesses

Purpose
- Communicate unique small business security challenges
- Simplify understanding of PCI DSS
- Provide educational materials that relates to small businesses

Participants
- Collaboration from dozens of small merchant owners and franchisees
- Co-chaired by Barclaycard and National Restaurant Association

Products
- Materials that are easy to understand
- Tips for improved security implementation
- Small merchant resources
1 – Guide to Safe Payments

Infographic with easy-to-understand guidance on data security basics

Understanding Your Risk

Protecting Your Business with These Security Basics

Where to Get Help

* Source: PCI SSC Guide to Safe Payments
Helping Small Merchants Understand Risk

Diagrams and illustrations to explain security basics

The impact of breaches to small businesses

What’s at risk?

Understanding data on a payment card

Common payment terms and types of POS terminals

Different risk for different environments and payment systems

$20,752

AVERAGE COST TO A SMALL BUSINESS DUE TO HACKING, UP FROM $8,600 IN 2013 (Visa)

69%

OF AMERICAN CONSUMERS WORRY ABOUT THEFT OF THEIR PAYMENT CARD DATA (Kluck)

A MERCHANT BANK is a bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Acquirer, acquiring bank, and card or payment processor are also terms for this entity.

A PAYMENT SYSTEM encompasses the entire process for accepting card payments in a retail location (including store/pos and e-commerce storefronts), and may include a payment terminal, an electronic cash register, other devices or systems connected to a payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to the merchant bank.

* Source: PCI SSC Guide to Safe Payments
## Protect Your Small Business

**Easy security controls with costs, ease, and risk mitigation scores**

<table>
<thead>
<tr>
<th>How to Safeguard your Business Against Breaches</th>
<th>Cost</th>
<th>Ease</th>
<th>Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use strong passwords and change default ones</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Protect your card data and only store what you need</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Inspect payment terminals for tampering</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Install patches from your vendors</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Use trusted business partners and know how to contact them</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Protect in-house access to your card data</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Don’t give hackers easy access to your systems</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Use anti-virus software</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Scan for vulnerabilities and fix issues</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Use secure payment terminals and solutions</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>Protect your business from the Internet</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
<tr>
<td>For the best protection, make your data useless to criminals</td>
<td>☺</td>
<td>🔝</td>
<td>🛡🛡🛡🛡🛡</td>
</tr>
</tbody>
</table>

*Source: PCI SSC Guide to Safe Payments*
# Where to Get Help?

## Resources and links

### PCI Council Listings

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Validated Payment Applications</td>
<td>PCI Council’s Validated Payment Applications</td>
<td><a href="https://www.pcisecuritystandards.org/assessors_and_solutions/vpsa_agreement">https://www.pcisecuritystandards.org/assessors_and_solutions/vpsa_agreement</a></td>
</tr>
<tr>
<td>List of Approved PTS Devices</td>
<td>PCI Council’s Approved PTS Devices</td>
<td><a href="https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices">https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices</a></td>
</tr>
<tr>
<td>List of Approved Scanning Vendors</td>
<td>PCI Council’s Approved Scanning Vendors</td>
<td><a href="https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors">https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors</a></td>
</tr>
<tr>
<td>List of Qualified Integrators / Resellers</td>
<td>PCI Council’s Qualified Integrators Resellers</td>
<td><a href="https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers">https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers</a></td>
</tr>
<tr>
<td>List of P2PE Validated Solutions</td>
<td>PCI Council’s P2PE Validated Solutions</td>
<td><a href="https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions">https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions</a></td>
</tr>
</tbody>
</table>

### Payment Brand Lists

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>URL</th>
</tr>
</thead>
</table>

### PCI DSS and Related Guidance

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>More about PCI DSS</td>
<td>How to Secure with PCI DSS</td>
<td><a href="https://www.pcisecuritystandards.org/pci_security/how">https://www.pcisecuritystandards.org/pci_security/how</a></td>
</tr>
</tbody>
</table>

---

* Source: PCI SSC Guide to Safe Payments
2 – Common Payment Systems

*Source: PCI SSC Common Payment Systems*

Identify which visual most closely represents the merchant’s payment system

Protect card data and merchant business with security basics

Identify risks and threats
Dial-Up Payment Terminal Diagram (Simple Model)

**OVERVIEW**

The payment terminal is connected to the bank by a dial-up telephone line.

**RISKS**

- Hardcopy card data, for example on paper receipts or reports
- Electronic card data inside payment terminal

**THREATS**

- They steal receipts or paper reports that you don’t secure, that you keep when you no longer need, or that you don’t dispose of securely.
- They steal card data via “skimming” equipment they attach to (or embed into) your payment terminal.
- They may also steal your terminal, replacing it with a modified one used to get your card data.

**PROTECTIONS**

- Inspect your payment terminals for damage or changes
- Ask your vendor partners for help if you need it
- Protect card data and only keep what you need

*Source: PCI SSC Common Payment Systems*
Secure Card Reader Diagram (Sophisticated Model)

Descriptions of more complex point of sale environments

With thorough explanations of risk, threats and controls to protect these more complex environments

For merchants when at non-fixed locations (flea market, trade show, etc.)
Card data and PIN are encrypted in the secure card reader and PIN entry device before sending to phone/tablet; phone/tablet only has access to encrypted card data
Merchant has no ability to manually enter card data

PIN ENTRY DEVICE
SECURE CARD READER (PAYMENT TERMINAL)

WIFI OR CELLULAR NETWORK

Different devices are used to read magnetic stripe card data, enter personal identification number (PIN), and read chip card data

Secure card reader attached to merchant-owned off-the-shelf mobile phone/tablet

PIN ENTRY DEVICE
SECURE CARD READER (PAYMENT TERMINAL)

LOCAL AREA NETWORK

Use strong passwords
Inspect your secure card readers and PIN entry devices for damage or changes
Install patches from your payment terminal vendor
Ask your vendor partners for help if you need it

Protect in-house access to your card data
Limit remote access for your vendor partners - don’t give hackers easy access
Use anti-virus software
Use a secure card reader and PIN entry device

Protect your business from the Internet
Make your card data useless to criminals

* Source: PCI SSC Common Payment Systems
3 – Questions to Ask your Vendors

Helps small merchants know what is needed from vendors and service providers

• Explains the function of vendor or service provider
• Depending on the type, the applicable PCI standard or program
• Includes what to look for and helpful links to card brand programs
• 12 simple questions to ask

<table>
<thead>
<tr>
<th>TYPE OF VENDOR/SERVICE PROVIDER</th>
<th>FUNCTION</th>
<th>PCI STANDARD OR PROGRAM</th>
<th>LOOK FOR:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment application vendor</td>
<td>Sell and support applications that store, process, and/or transmit cardholder data.</td>
<td>Payment Application Data Security Standard (PA-DSS)</td>
<td>Application is on the List of PCI PA-DSS of Validated Payment Applications</td>
</tr>
<tr>
<td>Payment terminal vendor</td>
<td>Sell and support devices used to accept card payments (e.g., payment terminal).</td>
<td>PIN Transaction Security (PTS)</td>
<td>Payment terminal is on the List of PCI Approved PTS Devices</td>
</tr>
<tr>
<td>Payment processors, e-commerce hosting providers/processors</td>
<td>Store, process, or transmit cardholder data on your behalf. May also host and manage your e-commerce server/website and/or develop and support your website.</td>
<td>PCI Data Security Standard (PCI DSS)</td>
<td>Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Service provider is on one of these lists: MasterCard's List of Compliant Service Providers, Visa's Global Registry of Service Providers, Visa Europe's Registered Member Agents</td>
</tr>
<tr>
<td>Providers of software as a service</td>
<td>Develop, host and/or manage your cloud-based web application or payment application (e.g., online ticketing or booking application).</td>
<td>PCI DSS</td>
<td>Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Service provider is on one of these lists: MasterCard's List of Compliant Service Providers, Visa's Global Registry of Service Providers, Visa Europe's Registered Member Agents</td>
</tr>
<tr>
<td>Integrators/resellers</td>
<td>Install PA-DSS validated payment applications on your behalf.</td>
<td>Qualified Integrators and Resellers (QIR)</td>
<td>Ask whether vendor is a PCI Qualified Integrator or Reseller (QIR). Vendor is on the List of PCI QIRs</td>
</tr>
<tr>
<td>Providers of services that satisfy PCI DSS requirement(s)</td>
<td>Manage/operate systems or services on your behalf (e.g., firewall management, patching/AV services).</td>
<td>PCI DSS</td>
<td>Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Service provider is on one of these lists: MasterCard's List of Compliant Service Providers, Visa's Global Registry of Service Providers, Visa Europe's Registered Member Agents</td>
</tr>
</tbody>
</table>

* Source: PCI SSC Small Merchant Questions to Ask Your Vendor
<table>
<thead>
<tr>
<th>CATEGORY: How secure is your product?</th>
<th>QUESTION: Does your product/solution protect payment card information using strong encryption?</th>
<th>DESIRED ANSWER FROM VENDOR</th>
<th>RECOMMENDATION ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>Encryption is a way of securing information so it is less likely to be stolen. If you can, select from the List of PCI P2PE Validated Solutions, where card data is secured as soon as you receive it and is protected as it travels through your network.</td>
<td>If <strong>NO</strong>, consider another vendor or solution.</td>
<td></td>
</tr>
</tbody>
</table>

* Source: PCI SSC Small Merchant Questions to Ask Your Vendor
Key Takeaways

Easy-to-use toolkit to help small merchants with payment system security

- Small merchant breaches continue to occur
- Simplified PCI DSS validation exercises
- Taskforce formed to address the needs of small businesses and franchisees
- Focused on protecting customer’s cardholder data rather than IT and security
- Guide focuses on risk and includes diagrams, costs, and ease of implementation matrix
- Payment diagrams designed to show data flows from simple to complex systems
- Q&A resource for working with vendors
- Glossary to help with payment terms and information security definitions
- Links for additional references and where to look for help
Resources

Upcoming Webinars – Training page on www.visa.com/cisp
• Protect the Payments System From Account Testing and Fraudulent Authorizations – August 9, 2016
• Guarding Against Card Not Present Fraud – August 24, 2016

Visa Data Security Website – www.visa.com/cisp
• Alerts, Bulletins
• Best Practices, White Papers
• Webinars
• Visa Global Registry of Service Providers – http://www.visa.com/splisting/

PCI Security Standards Council Website – www.pcissc.org
• Small Merchant Resources - https://www.pcisecuritystandards.org/pci_security/small_merchant
• 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…
Thank you for attending!