Review PCI Data Security Essentials (DSE) for Small Merchants

15 November 2018

June Qiu

Global Payment System Risk
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

1. Payments Data Security Landscape
2. Visa Validation Requirements
3. Introduction to DSE Resources
   • Guide to Safe Payments v2.0
   • Common Payment Systems v1.1
   • Questions to Ask Your Vendors v2.0
   • DSE Overview for Small Merchants/ Acquirers
4. PCI DSE for Small Merchants Evaluation Tool
Payment Security Landscape

Threat and Impact of Data Breach Remain Significant for Small Merchants

“58% of victims are small businesses”

“SMBs in the U.S. and Canada have the highest recovery cost, at $149K on average (up 27% or $32,000 from $117K in 2017).”

- 2018 B2B Survey

“... average cost increased from $141 to $148 per lost or stolen record”
Payments Data Security Landscape

Breach Types
- Small merchants targeted more frequently than other organizations
- Number and impact of e-commerce compromises is increasing

Moving Beyond Merchants
- Criminals increasingly targeting service providers and data aggregators
- Financial institutions targeted for access to cash (ATM Processor Attacks)

*1 January 2018 – 30 June 2018
Payment Card Industry Data Security Standard

Compliance
- Visa requires **ALL** organizations that store, transmit or process Visa account data to comply with PCI DSS
- PCI DSS applies to all payment channels, including card present, mail/telephone order, eCommerce, in-app, etc.

Validation
- Separate and distinct from the requirement to comply with PCI DSS is the validation of compliance
- Validation is the exercise of verifying and demonstrating compliance status against the PCI DSS requirements
## PCI DSS Validation Requirements for Merchants

<table>
<thead>
<tr>
<th>Level</th>
<th>Annual Transaction Volume</th>
<th>Minimum Validation Requirements</th>
</tr>
</thead>
</table>
| 1     | 6 million+ Visa transactions (all channels) | • Report on Compliance (ROC) by Qualified Security Assessor (QSA) or internal resources if signed by officer of the company  
• Attestation of Compliance (AOC) |
| 2     | 1 million to 6 million Visa transactions (all channels) | • Self-Assessment Questionnaire (SAQ)  
• Attestation of Compliance (AOC) |
| 3     | 20,000 to 999,999 Visa eCommerce transactions | • Self-Assessment Questionnaire (SAQ)  
• Attestation of Compliance (AOC) |
| 4     | Less than 20,000 Visa eCommerce transactions and all other merchants processing less than 1 million Visa transactions | • Self-Assessment Questionnaire (SAQ) or alternative validation as defined by acquirer |
Challenges that Small Merchants Face

- Third-party remote access for POS management (e.g. LogMeIn)
- Always-on remote access
- Single-factor authentication for remote access

- Insecure user access controls (e.g., common/shared passwords)
- Vulnerability to phishing attacks

- Limited network security controls
- Little to no security monitoring

- Lack of application white-listing
- Anti-malware software not in place or outdated

- Not compliant with PCI DSS
- Inadequate verification of service provider compliance

* source: US forensic investigation reports
What Does This Mean for Small Merchants?

Not all bad news...

- Non-compliant service providers can place small merchants at higher risk of compromise.

- Visa maintains and publishes the **Global Registry of Service Providers** that includes registered, validated agents.

- Small merchants continue to be a primary target for criminals.

- Majority of small merchant breaches may be prevented with basic controls.
Intro to Data Security Essentials Resources
PCI’s Updated Data Security Essentials
Simple Guidance for Keeping Payment Data Safe

**Guide to Safe Payments v2.0**

- What are the security basics?
- Which ones are simple to implement, least cost or have highest amount of risk reduction?

**Common Payment Systems v1.1**

- What are the different payment types?
- Do you know the associated risks, threats and protection?

**Questions to Ask Your Vendors**

- What are the common types of payment vendors
- Is your vendor supporting your protection efforts?
Data Security Essentials Overview
For Acquirer and Merchant

PCI Data Security Essentials for Small Merchants

The PCI Data Security Essentials for Small Merchants provide security basics to protect against payment data theft and to help small merchants simplify their security and reduce their risk. The Data Security Essentials evaluations provide an alternative for eligible small merchants to evaluate and report how they are meeting these security basics for safe payments.

It is up to each acquirer, in coordination with the applicable payment brands, to determine which small merchants are eligible to use Data Security Essentials evaluations.

In addition to the educational resources included in PCI Data Security Essentials, PCI SSC provides resources to help small merchants with Data Security Essentials evaluations, so they can learn more about their security posture and complete a preliminary evaluation. Optionally, small merchants can use the PCI Security Essentials Evaluation Tool (PSET) to find the payment system that most closely matches theirs, download the related Evaluation Form, answer the security questions, and review and save their preliminary results. Merchants may then reference these preliminary results to complete the official Evaluation Form, per instructions from their acquirer.

Follow these steps to help your small merchants evaluate their security:

1. Acquirer identifies eligible merchants.
2. Acquirer tells merchants how to complete the Preliminary Evaluation.
5. If NO for small merchants, go to step 6.
6. If YES for small merchants, go to step 7.
7. Merchant submits Preliminary Evaluation Tool to Acquirer.
8. Acquirer uses Preliminary Evaluation Tool to determine eligibility for PCI DSS.
9. Acquirer confirms eligibility for PCI DSS.
10. Acquirer tells merchants how to complete the Evaluation Form.
12. Merchant submits Evaluation Form to Acquirer.
13. Acquirer reviews evaluation form and makes determinations based on results.

Follow these steps to better understand and evaluate payment security:

1. Acquirer identifies eligible merchants.
2. Acquirer tells merchants how to complete the Evaluation Form.
4. Merchant submits Evaluation Form to Acquirer.
5. Acquirer reviews evaluation form and makes determinations based on results.

Visit www.pcisecuritystandards.org/merchants

© 2018 PCI Security Standards Council LLC.

https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Acquirers.pdf

https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf
Data Security Essentials Evaluation Tool

What is it?
• Online tool to help merchants gain insight about security practices relevant to payment acceptance

Can I use the tool to report compliance?
• Visa does not collect PCI DSS compliance documentation for small merchants and allows acquirers to determine PCI DSS validation requirements
• Completed results cannot be submitted directly from the online tool – contact your acquiring bank regarding eligibility and next steps

How does this simplify validation effort?
• The tool is shorter than the SAQs and each form is tailored to evaluate security practices applicable to small merchants using specific acceptance models
Getting Started: Step 1

Acknowledgement
(contact bank)

Review DSE
Resources

Identify Payment
System

Download applicable
Evaluation Form

Data Security Essentials Evaluation Tool

This Data Security Evaluation Tool is provided by PCI SSC for merchant information only. You can use this PCI SSC tool to gain insight about security practices relevant to the way you accept payments, to provide your responses and to see your results. However, you must contact your merchant bank and follow their instructions to formally complete a Data Security Essentials Evaluation as part of their compliance program. You cannot use this tool to submit this form to PCI SSC or to your merchant bank, nor does PCI SSC send it to your merchant bank on your behalf.

Do you acknowledge that you are using this tool for your information only, and to contact your merchant bank about next steps?

YES  NO
Getting Started: Step 2

Acknowledgement (contact bank)

Review DSE Resources

Identify Payment System

Download applicable Evaluation Form

Have you reviewed the following Data Security Essentials Resources?

- Guide to Safe Payments
- Questions to Ask Your Vendors

How do you protect your business?

The good news is, you can start protecting your business today with these security basics:

- Use strong passwords and change defaults
- Protect your card data and only store what you need
- Inspect payment terminals for tampering
- Use trusted business partners and know how to contact them
- Install patches from your vendors
- Protect in-house access to your card data
- Don’t give hackers easy access to your systems
- Use antivirus software
- Scan for vulnerabilities and fix issues
- Use secure payment terminals and solutions
- Protect your business from the Internet
- For the best protection, make your data useless to intruders

Which questions apply to which vendors/solution providers?

<table>
<thead>
<tr>
<th>Type of Vendor/Service Provider</th>
<th>Applicable Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment application vendor</td>
<td>1-15</td>
</tr>
<tr>
<td>Payment terminal vendors,</td>
<td>1-15</td>
</tr>
<tr>
<td>payment solution vendors</td>
<td></td>
</tr>
<tr>
<td>Payment processors, e-commerce</td>
<td>1-15</td>
</tr>
<tr>
<td>payment service providers,</td>
<td></td>
</tr>
<tr>
<td>payment gateways, contact centers</td>
<td></td>
</tr>
<tr>
<td>E-commerce hosting providers</td>
<td>1-15</td>
</tr>
<tr>
<td>Providers of software as a</td>
<td>1-4 &amp; 10-15</td>
</tr>
<tr>
<td>service, cloud-based hosting</td>
<td></td>
</tr>
<tr>
<td>provider</td>
<td></td>
</tr>
<tr>
<td>Providers of services that</td>
<td>1-15</td>
</tr>
<tr>
<td>may help you meet PCI DSS</td>
<td></td>
</tr>
<tr>
<td>requirements</td>
<td></td>
</tr>
<tr>
<td>Integrators/resellers</td>
<td>5-9</td>
</tr>
</tbody>
</table>

These security basics are organized from easiest and least costly to implement to those that are more complex and costly to implement. The amount of risk reduction that each provides to small merchants is also indicated in the “Risk Mitigation” column.
Getting Started: Step 3

Now let’s review some payment diagrams and you can select the one that best matches your payment system(s). To protect your business against payment data theft, it is important to first understand how you take payments in your store or shop. What kind of equipment do you use, who are your bank and technology vendor partners, and how do these things all fit together?

Use these real-life visuals to:

- **Identify** what type of payment system you use
- **Learn** about risks associated with your payment system
- **Protect** your system with specific security steps

I'M READY TO IDENTIFY MY PAYMENT SYSTEM

How do you accept payments?
Review all payment diagrams that apply to how your business accepts payments

- You accept payments with a standalone, dial-up payment terminal
  - Types 1, 2

- You accept payments with a payment device connected only to a processor
  - Types 3, 4

- You accept payments with a payment terminal connected to an electronic cash register or POS, and the electronic cash register/POS is connected only to a processor
  - Type 5

- You accept payments with a payment terminal that is connected to other systems (e.g., server) in your network
  - Types 6, 7, 8

- You accept payments via e-commerce
  - Types 9, 10, 11

- You accept payments via a PCI-listed SCR (Secure Card Reader) attached to a mobile device
  - Types 12, 13

- You accept payments via a virtual terminal
  - Type 14

- You accept payments via a PCI-listed P2PE Solution
  - Type 15
Getting Started: Step 4

Dial-up payment terminal. Payments sent via phone line.

OVERVIEW  RISKS  THREATS  PROTECTIONS

DIAL-UP PAYMENT TERMINAL

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

Paper documents with card data

YES, I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

NO, I'm not positive this is my payment system. Show me the overview again.
Completing the Evaluation Form

Section 1: Payment Acceptance Method
If you have answered “No” to any questions in this section, you would have chosen the wrong payment type

- return to Common Payment Systems to choose another payment type

My terminal is a dial-up payment terminal. Payments are sent via a phone line.

1. My payment terminal uses only a dial-out (phone) connection to send payments, it is not connected to the Internet.
   - Yes
   - No

2. I do not have any electronic card data stored by my payment systems. If I have card data, it is only on paper (receipts, etc.).
   - Yes
   - No

Section 2: Merchant Information
Completing the Evaluation Form

Section 3: Data Security Essentials Evaluation

• Some lettered sections and numbers in each section are intentionally missing.
  o The security practices below are specifically chosen for your type of payment system, and are part of a larger complete set.

Section 4: Confirmation of status
Interpreting the Evaluation Results

Section 5: Confirmation of status

<table>
<thead>
<tr>
<th>Number of questions answered as:</th>
<th>Helpful Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 I do this consistently.</td>
<td>Make sure you continue to perform these good practices. Adding them to the “business as usual” processes you perform daily, weekly, or monthly is a good start. Read the PCI DSS section entitled “BAU” or talk to your acquirer if you want more info on BAU. And if you change your payment systems or methods during the year—including how and where you handle card data or payments—do not forget to extend these good practices to cover the new processes and systems, too.</td>
</tr>
<tr>
<td>1 I do this sometimes.</td>
<td>Look at why you do not perform these practices all the time and consider whether there are easy steps you can take to perform these practices consistently. It may help remind you if you add them to your “business as usual” processes that you perform daily, weekly, or monthly. It is important that you implement all practices in this evaluation form to protect your business and keep your customers’ card data secure. Please contact your acquirer or portal provider today for help in understanding why it is important to consistently perform this practice and for tips.</td>
</tr>
<tr>
<td>1 This does not apply to my business.</td>
<td>This means that it is truly not applicable to how you do business so please make sure that is the case. For example, you may not want to do something, have not done it, or you do not understand how to do it, nevertheless, it may be applicable. Also note that your decision on whether a practice is applicable to your business should not be based on your perception of the risk of not implementing that practice; “lower risk” does not mean it is “not applicable.” It is important that you implement all applicable practices in this evaluation form to protect your business and keep your customers’ card data secure. If this practice is truly not applicable to your business now but your business practices change during the year, please come back and look at these areas again to make sure you are still protected. If you need help with implementing these practices, please talk to your portal provider or acquirer.</td>
</tr>
<tr>
<td>1 I do not know / I do not understand.</td>
<td>If you do not know, is this because the person that may have implemented this practice is no longer at the company, or because the practice is addressed by a third party on your behalf? Or does this mean that you do not know because you do not understand the practice? It is important that you implement all practices in this evaluation form to protect your business and keep your customers’ card data secure. Contact your acquirer or portal provider today for help. If you do not understand how to implement this practice, we encourage you to seek assistance. It is important that you implement all practices in this evaluation form to protect your business and keep your customers’ card data secure. Please refer to the small merchant resources available at <a href="http://www.pcissc.org">www.pcissc.org</a> under “Get Started” for help in understanding this practice. Also consider contacting your payment terminal vendor, other vendor, or service provider—they may be able to explain how this practice applies to your business. Or contact your acquirer or portal provider today for help in understanding why this practice is important and how to implement it.</td>
</tr>
<tr>
<td>1 I do not do this.</td>
<td>This item is applicable to, and would help secure, your business. It is important that you implement all practices in this evaluation form to protect your business and keep your customers’ card data secure. Please contact your acquirer or portal provider today for help in understanding why this practice is important and how to implement it.</td>
</tr>
</tbody>
</table>
Data Security Resources

Visa Data Security Website www.visa.com/cisp
- Alerts, Bulletins
- Best Practices, White Papers, Webinars

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
- Data Security Standards, Qualified Assessor Listings, Data Security Education Materials

PCI Resources for Small Merchants https://www.pcisecuritystandards.org/merchants/
- Guide to Safe Payments, Common Payment Systems, Questions to Ask your Vendors
- PCI Data Security Essentials Tool
Visa’s Ecosystem Data Security Team

Questions? Comments?

- Agent Registration: agentregistration@visa.com
- Third Party Compliance: pcirocs@visa.com
- Merchant Compliance: cisp@visa.com
- ACS/AVP: AVPAmericas@visa.com
- PIN security: pinna@visa.com
THANK YOU

For PCI-DSS related enquiries, email us at cisp@visa.com