

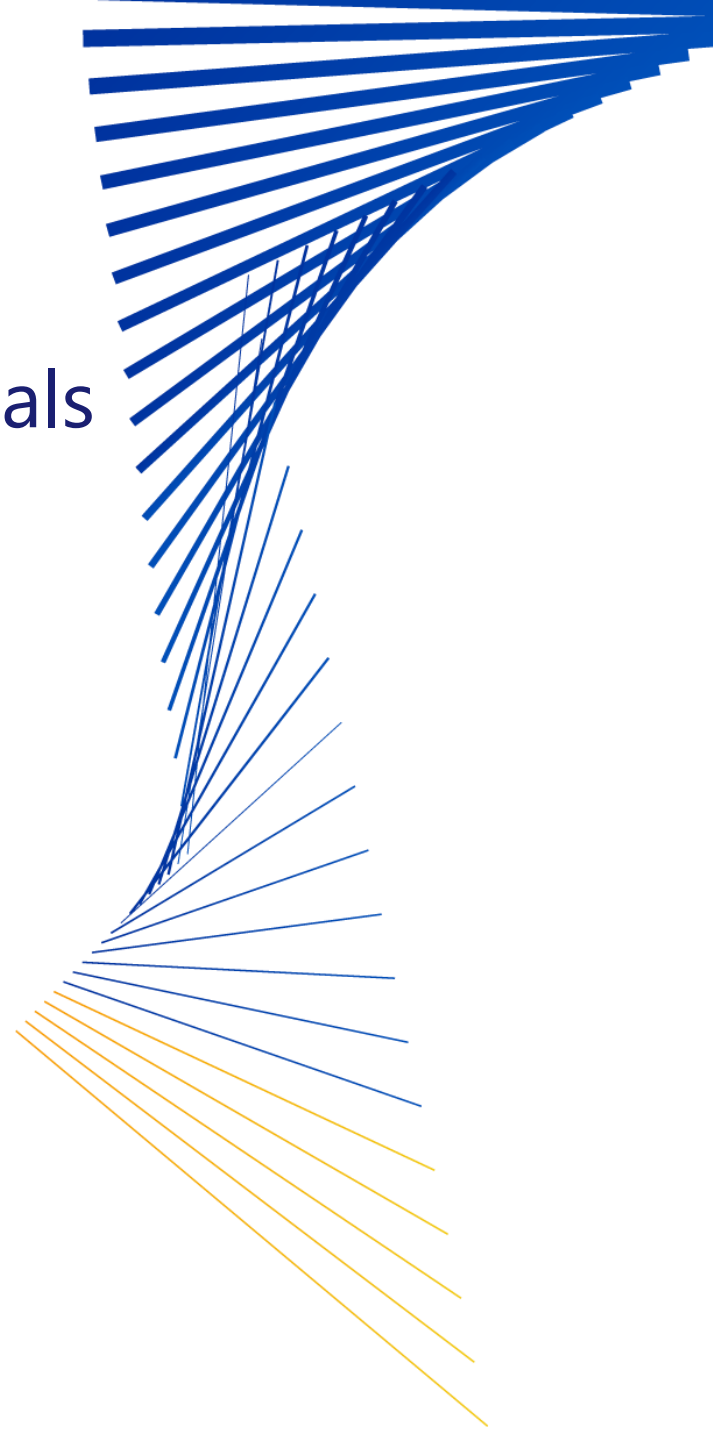
Review PCI Data Security Essentials (DSE) for Small Merchants

15 November 2018

June Qiu

Global Payment System Risk

VISA



Disclaimer

Notice

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.

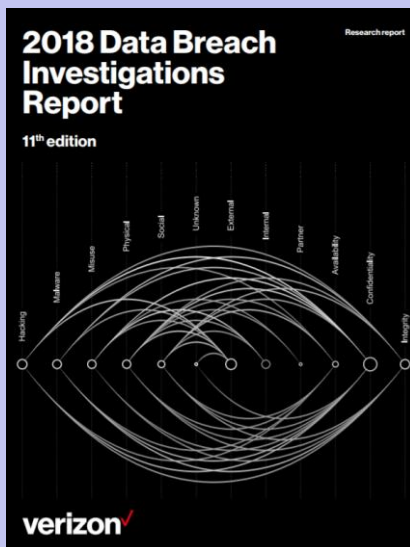
Agenda



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”

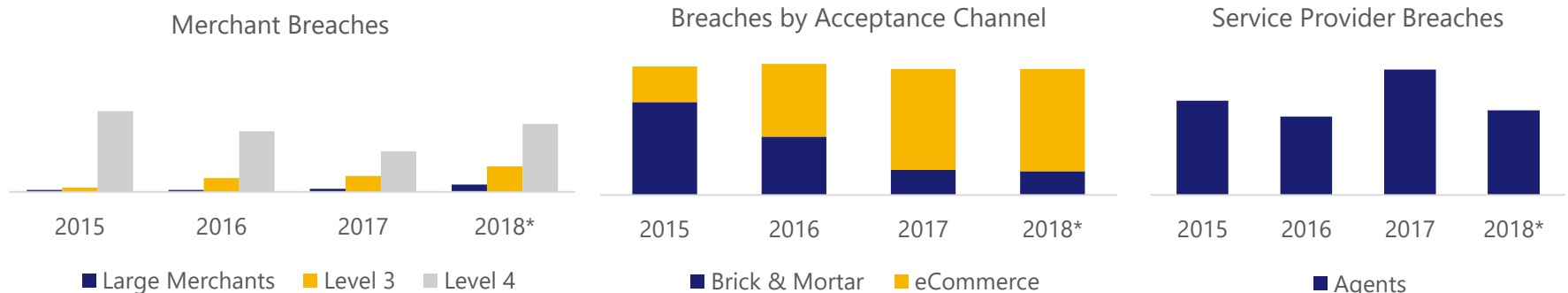
Payments Data Security Landscape

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

Level	Annual Transaction Volume	Minimum Validation Requirements
1	6 million+ Visa transactions (all channels)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Self-Assessment Questionnaire (SAQ) • Attestation of Compliance (AOC)
3	20,000 to 999,999 Visa eCommerce transactions	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

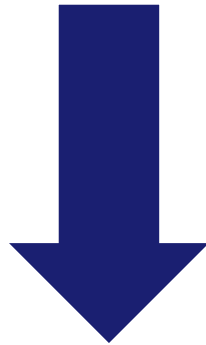


- Not compliant with PCI DSS
- Inadequate verification of service provider compliance

* source: US forensic investigation reports

What Does This Mean for Small Merchants?

Not all bad news...



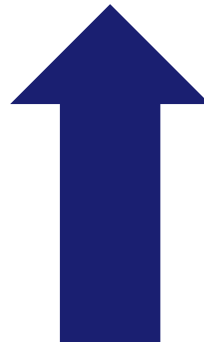
Non-compliant service providers can place small merchants at higher risk of compromise



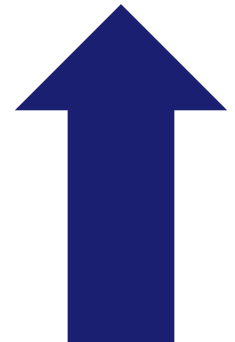
Small merchants continue to be a primary target for criminals



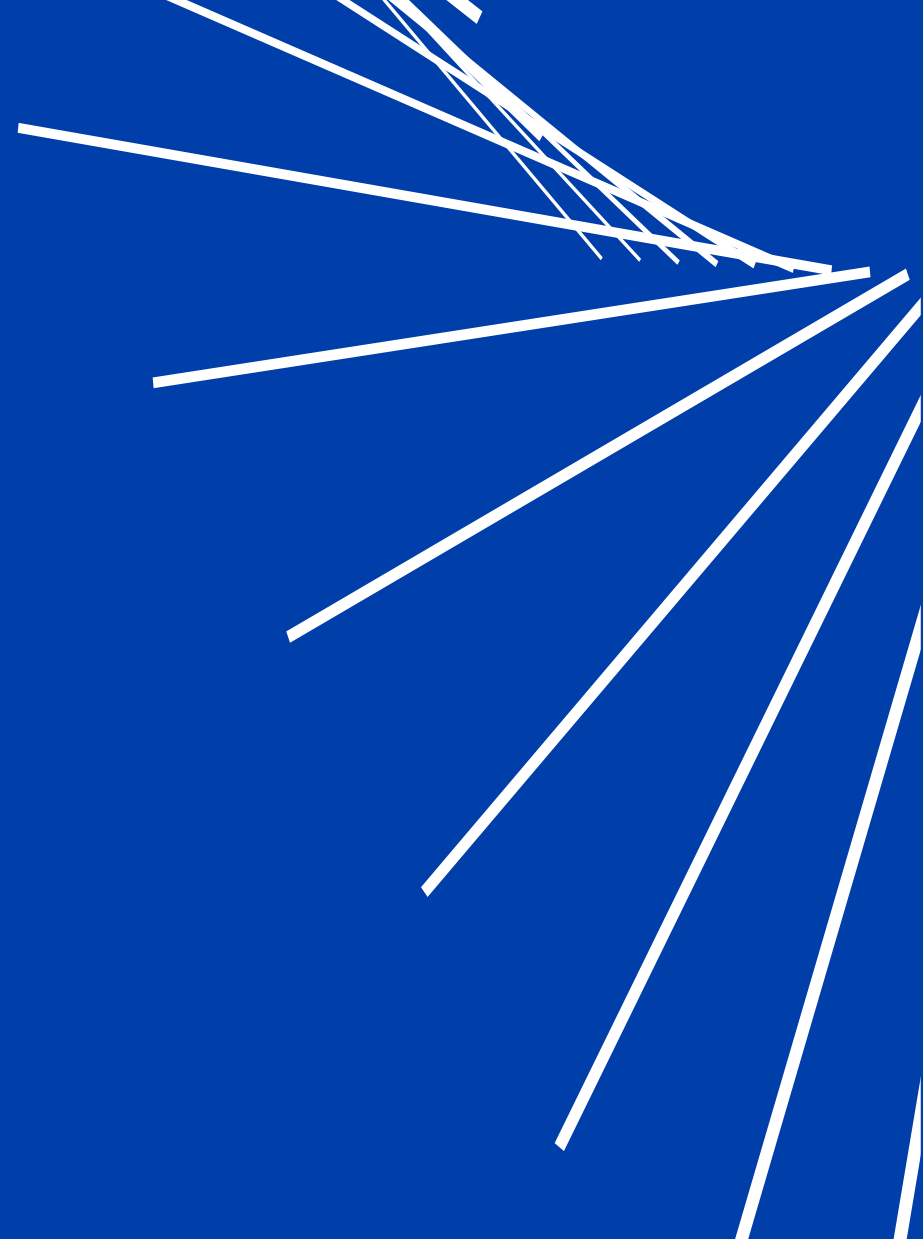
Visa maintains and publishes the **Global Registry of Service Providers** that includes registered, validated agents



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

The more features your payment system has, the more complex it is to secure.

Think carefully about whether you really need extra features such as Wi-Fi, remote access software, Internet-connected cameras, or call recording systems for your business. If not properly configured and managed, each of these features can provide criminals with easy access to your customers' payment card data. If you are an e-commerce merchant, it is very important to understand how or if payment data is captured on your website. In most cases, using a wholly outsourced third party to capture and process payments is the safest option.



TYPE 1 Dial-up payment terminal. Payments sent via phone line.

RISK PROFILE: LOWER

TYPE 1 OVERVIEW | TYPE 1 RISKS | TYPE 1 THREATS | TYPE 1 PROTECTIONS

YES
This is my payment system, and I have reviewed the Risks, Threats, and Protections table. I've made the necessary changes to my system to reduce the risk to an acceptable level. I can further protect my business.

NO
I'm not positive this is my payment system. Please see the overview again.

DIAL-UP PAYMENT TERMINAL: Dial-up payment terminal allows it to dial for each transaction. (Paper documents with card data)

PHONE LINE: The payment terminal is connected to bank by a dial-up telephone line.

BANK

PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL

Questions to Ask Your Vendors

DATA SECURITY ESSENTIALS FOR SMALL MERCHANTS
A PRODUCT OF THE PAYMENT CARD INDUSTRY SMALL MERCHANT TASK FORCE
VERSION 2.0 | AUGUST 2018

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

Acquirers, help your small merchants understand payment security and simplify security evaluation

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 merchant to evaluate and report how they are meeting these security basics for safe payments.

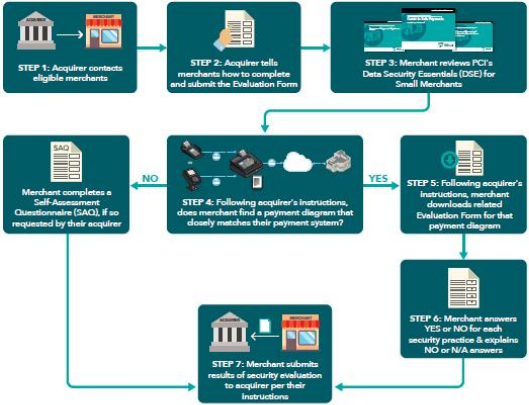
It is up to each acquirer, in coordination with the applicable payment brands, to determine which small merchants are eligible to use Data Security Essentials evaluations.

Merchants are only eligible to use a Data Security Essentials evaluation if they have been notified by their acquirer that it is appropriate for them to do so. We encourage acquirers to review Data Security Essentials for Small Merchants, ask your eligible small merchants to read these materials too, and then start these merchants on the path to simpler validation today.



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 either the [Data Security Essentials Evaluation Tool](#) OR the [Common Payment Systems](#) PDF to find the payment system that most closely matches theirs, download the related Evaluation Form, answer the security practices, 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:



www.pcisecuritystandards.org/merchants © 2018 PCI Security Standards Council LLC.

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


PCI Data Security Essentials for Small Merchants

Small merchants, understand payment security and simplify your security evaluation

The PCI Data Security Essentials for Small Merchants provide security basics to protect small merchants 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.

Your merchant bank (acquirer), in coordination with the applicable payment brands, will determine which small merchants are eligible to use Data Security Essentials evaluations, so talk to your acquirer today about how you can simplify security and better protect your business.

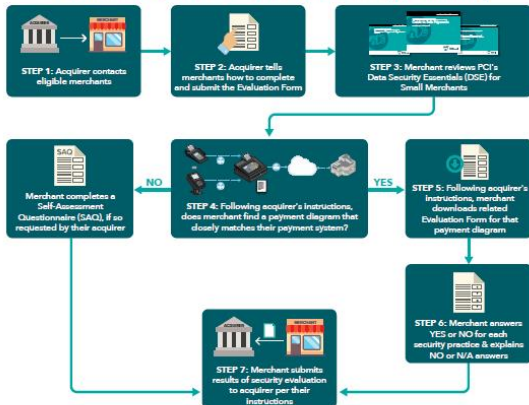
Merchants are only eligible to use a Data Security Essentials evaluation if they have been notified by their acquirer that it is appropriate for them to do so. Eligible merchants should read this document as well as PCI SSC's Data Security Essentials for Small Merchants, and then talk to your acquirer to get their instructions to start the path to better security and simpler validation today.



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 either the [Data Security Essentials Evaluation Tool](#) OR the [Common Payment Systems](#) PDF to find the payment system that most closely matches theirs, download the related Evaluation Form, answer the security practices, 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.

Merchants, contact your acquirer for instructions about how to complete and submit the evaluation form as this may differ between acquirers.

Follow these steps to better understand and evaluate payment security



www.pcisecuritystandards.org/merchants © 2018 PCI Security Standards Council LLC.

<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



The screenshot shows the top of the PCI Security Standards Council website. The header includes the PCI Security Standards Council logo, a 'HOME' link, and a 'PAYMENT TERMS EXPLAINED' link. The main heading is 'Data Security Essentials Evaluation Tool', accompanied by an icon of a document with a lock and a checkmark. Below the heading is an information icon (a lowercase 'i' in a circle) and a paragraph of text: '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.' Below the text is a question: 'Do you acknowledge that you are using this tool for your information only, and to contact your merchant bank about next steps?' and two buttons labeled 'YES' and 'NO'.

Getting Started: Step 2



Have you reviewed the following Data Security Essentials Resources?

- [Guide to Safe Payments](#)
- [Questions to Ask Your Vendors](#)

YES

NO

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 default ones Cost: 1 Ease: 1 Risk Mitigation: 1, 2, 3	 Protect your card data and only store what you need Cost: 1 Ease: 1 Risk Mitigation: 2, 3	 Inspect payment terminals for tampering Cost: 1 Ease: 1 Risk Mitigation: 2, 3	 Use trusted business partners and know how to contact them Cost: 1 Ease: 1 Risk Mitigation: 3	 Install patches from your vendors Cost: 1 Ease: 2, 3 Risk Mitigation: 2, 3, 4	 Protect in-house access to your card data Cost: 1 Ease: 2, 3 Risk Mitigation: 2, 3
 Don't give hackers easy access to your systems Cost: 1, 2 Ease: 2, 3 Risk Mitigation: 2, 3, 4	 Use anti-virus software Cost: 1, 2 Ease: 2, 3 Risk Mitigation: 2, 3	 Scan for vulnerabilities and fix issues Cost: 1, 2 Ease: 2, 3 Risk Mitigation: 2, 3, 4	 Use secure payment terminals and solutions Cost: 1, 2, 3, 4 Ease: 2, 3 Risk Mitigation: 2, 3, 4	 Protect your business from the Internet Cost: 1, 2 Ease: 2, 3, 4 Risk Mitigation: 2, 3, 4	 For the best protection, make your data useless to criminals Cost: 1, 2, 3, 4 Ease: 2, 3, 4 Risk Mitigation: 2, 3, 4

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.

Which questions apply to which vendors/solution providers?

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

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

<p>You accept payments with a standalone, dial-up payment terminal</p> <p>TYPES 1, 2</p>	<p>You accept payments with a payment device connected only to a processor</p> <p>TYPES 3, 4</p>	<p>You accept payments with a payment terminal connected to an electronic cash register or till, and the electronic cash register/till is connected only to a processor</p> <p>TYPE 5</p>	<p>You accept payments with a payment terminal that is connected to other systems (e.g., servers) in your network</p> <p>TYPES 6, 7, 8</p>
<p>You accept payments via e-commerce</p> <p>TYPES 9, 10, 11</p>	<p>You accept payments via a PCI-listed SCR (Secure Card Reader) attached to a mobile device</p> <p>TYPES 12, 13</p>	<p>You accept payments via a virtual terminal</p> <p>TYPE 14</p>	<p>You accept payments via a PCI-listed P2PE Solution</p> <p>TYPE 15</p>

Getting Started: Step 4



TYPE 1 Dial-up payment terminal. Payments sent via phone line. **RISK PROFILE: LOWER**

OVERVIEW RISKS THREATS PROTECTIONS

DIAL-UP PAYMENT TERMINAL

Dial-up payment terminal shows it is dialing for each transaction

Paper documents with card data

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

PHONE LINE

BANK

125425487540
981250530736
054505740987
582929255846
262910504826
454900926544
155784

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.	<input type="checkbox"/> Yes	<input type="checkbox"/> 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.).	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Section 2: Merchant Information

General Information			
Company name:		Any other company names:	
Contact name:		Title:	
Telephone:		E-mail:	
Business address:		City:	
State/Province:		Country:	Postal code:
URL:			
Type of Merchant Business (check all that apply):			
<input type="checkbox"/> Retailer	<input type="checkbox"/> Grocery and Supermarkets	<input type="checkbox"/> Mail order/telephone order (MOTO)	<input type="checkbox"/> Restaurants
<input type="checkbox"/> Petroleum	<input type="checkbox"/> E-Commerce	<input type="checkbox"/> Others (please specify):	
What types of payment channels does your business serve?		Which payment channels are covered by this form?	
<input type="checkbox"/> Mail order/telephone order (MOTO) <input type="checkbox"/> E-Commerce <input type="checkbox"/> Card-present (face-to-face)		<input type="checkbox"/> Mail order/telephone order (MOTO) <input type="checkbox"/> Card-present (face-to-face)	
My business uses a payment terminal(s) that only accepts magnetic-stripe payment cards (meaning it does not, or is not enabled to, accept EMV/chip cards).		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Completing the Evaluation Form

Section 3: Data Security Essentials Evaluation

- Some lettered sections and numbers in each section are intentionally missing.
 - 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

Part 4a. Questions Regarding Completion	
Did you get help to complete this form? If so, did you use: <i>(check all that apply)</i>	
<input type="checkbox"/>	A payment professional (for example, a Qualified Security Assessor or a Qualified Integrator Reseller) to help you complete this form?
<input type="checkbox"/>	A technology or service provider?
<input type="checkbox"/>	Someone else? Please describe.
<div style="background-color: #e6f2ff; height: 40px;"></div>	
Part 4b. Acknowledgment of Status – To be completed after conducting the Data Security Essentials Evaluation in Section 3	
Signatory(s) confirms: <i>(check all that apply)</i>	
<input type="checkbox"/>	This Confirmation and my responses within Section 3 fairly represent the results of my Data Security Essentials Evaluation.
<input type="checkbox"/>	I recognize that I will need to complete the applicable Data Security Essentials Evaluation Form for any other payment channels that I have.
<input checked="" type="checkbox"/>	I recognize I must re-evaluate my environment and implement any additional security practices that apply if my environment changes.
Part 4c. Merchant Attestation	
Signature of Merchant Executive Officer:	<div style="background-color: #e6f2ff; height: 20px;"></div>
Merchant Executive Officer Name:	<div style="background-color: #e6f2ff; height: 20px;"></div>
Title:	<div style="background-color: #e6f2ff; height: 20px;"></div>
Date:	<div style="background-color: #e6f2ff; height: 20px;"></div>

Interpreting the Evaluation Results

Section 5: Confirmation of status

Number of questions answered as:		Helpful Tips
9	I do this consistently.	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.
1	I do this sometimes.	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.
1	This does not apply to my business.	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.
1	I do not know / I do not understand.	<p>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.</p> <p>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 www.pcissc.org 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.</p>
1	I do not do this.	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.

- Data Security Essentials for Small Merchants Evaluation Form 1, Section 5

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: pciocs@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

VISA

