PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL

Evaluation Form 9

E-commerce merchant with fully outsourced payment page/form

Payments sent by PCI DSS compliant third-party service provider

DATA SECURITY ESSENTIALS FOR SMALL MERCHANTS
A PRODUCT OF THE PAYMENT CARD INDUSTRY SMALL MERCHANT TASK FORCE

VERSION 1.0 | AUGUST 2018

PCi Security Standards Council®

Introduction

To help small merchants address security requirements relevant to the manner in which they handle payments, PCI Security Standards Council has developed Data Security Essentials for Small Merchants, consisting of educational resources as well as an evaluation tool, to help merchants simplify and evaluate their security, and reduce risk.

Before You Begin

As a first step, ensure that you have already:

1. Talked to your acquirer (merchant bank) to confirm that you are eligible to use a Data Security Essentials Evaluation.
2. Reviewed the Data Security Essentials for Small Merchants section of the PCI SSC website including the:
   a. *Guide to Safe Payments* to understand security basics, and
   b. *Common Payment Systems* to find the payment diagram that most closely resembles how you process payments, and to understand the threats and risks associated with that payment system.
3. Followed your acquirer's instructions for obtaining and completing the Evaluation Form

If you have not already accomplished the above, it is recommended you do that before proceeding further.

For your own information, you may optionally use PCI SSC's Data Security Essentials Evaluation Tool to select the payment system that most closely resembles how you process payments, and to download and complete this form. This tool will let you gain insight about relevant security practices, provide your answers, and see your preliminary results. However, you cannot submit this form from PCI SSC's website nor does PCI SSC submit it on your behalf— ***you must contact your merchant bank and follow their completion and submission instructions****.*

Introduction

About this Evaluation

This Data Security Essentials Evaluation 9 has been developed to evaluate security practices applicable to small e-commerce merchants with fully outsourced payment pages/forms. Payments are sent via the Internet by PCI DSS compliant third-party service providers. Merchants completing this validation form will conduct transactions in an e-commerce and/or mail-order/telephone-order environment.

Below, merchants using this approach will confirm that *for this payment channel:*

1. You fully outsource your e-commerce payment page to a PCI DSS compliant third-party service provider.
2. You may host and manage your own website or a third-party service provider may manage it on your behalf. Either way, you have no access to the payment page.
3. Shopping pages may be hosted on your website or by your website hosting provider.
4. Your website has only product information (shopping pages, etc.) available. You have no access to, or ability to control, any card data.
5. When the customer is ready to enter card data, your website sends the request—via URL redirect or iframe—to a PCI DSS compliant third-party service provider that provides a payment page to the customer to collect card data.
6. Card data is sent from the customer's browser to a PCI DSS compliant third-party service provider that sends payment via the Internet.

Understanding the Evaluation

The Security Guidance and Security Practices contained in this evaluation are based on information found in the Guide to Safe Payments, part of the educational resources in the Data Security Essentials for Small Merchants. The Data Security Essentials for Small Merchants include:

Document	Purpose or Content
Guide to Safe Payments	• Addresses twelve security basics attributable to most small merchant data compromises • Easy-to-understand language, minimal use of acronyms • Ranking of security basics based on ease to implement, cost, risk reduction potential
Common Payment Systems	• Diagrams of payment systems most commonly used by small merchants • Overview, threats, risks, and security basics for each payment system
Questions to Ask Your Vendors	• Helps merchants talk to their vendors and understand their responses • Links to PCI SSC and payment brand lists and resources
Glossary of Payment and Information Security Terms	• Easy-to-understand definitions of common payment and security terms
Evaluation Tool	• *This tool is provided for merchant information only.* An option for merchants is to use it as a first step to gain insight about security practices relevant to the way they accept payments, to provide their initial responses, and to see their results. • **Merchants must contact their merchant bank and follow the bank's instructions to formally complete a Data Security Essentials Evaluation as part of the bank's compliance program.** • Merchants cannot use the PCI SSC Evaluation Tool to submit this form to PCI SSC or to their merchant bank, nor does PCI SSC send it to merchant banks on behalf of merchants. • See Evaluation Tool: Acquirer Overview and Evaluation Tool: Merchant Overview for guidance on this evaluation approach.

These and other resources can be found on the PCI SSC website (www.pcisecuritystandards.org). Organizations are encouraged to review the Data Security Essentials for Small Merchants before beginning their assessment.

Completion Steps

1. Confirm the payment acceptance method used in your business in Section 1 below.
    - If you have any "no" answers in Section 1, return to *Common Payment Systems* and search for another appropriate payment diagram that best matches your payment acceptance method.
2. Read the security guidance and security practices in Section 3 to understand the security practices required and to determine whether you have those practices in place.
3. Contact your merchant bank (acquirer) for completion and submission instructions.
4. Complete Sections 1 through 4 and review your results in Section 5.
    - Section 1 – Payment Acceptance Method
    - Section 2 – Merchant Information
    - Section 3 - Data Security Essentials Evaluation Form
    - Section 4 - Confirmation of Status
    - Section 5 - Data Security Essentials Evaluation Results

    Optionally, merchants can elect to use PCI SSC's Data Security Essentials Evaluation Tool. With this tool, merchants can gain insight about security practices relevant to how they accept payments. The merchant:

    a. Selects the payment system that most closely matches how they accept payments
    b. Downloads the relevant Evaluation Form
    c. Provides preliminary responses
    d. Reviews their results
    e. Can print or save the resulting PDF for future use

    *This tool is provided for merchant information only. Merchants cannot submit the evaluation form from PCI SSC's website, nor does PCI SSC submit it on your behalf—**you must contact your merchant bank and follow their completion and submission instructions.***
5. Following your merchant bank's (acquirer's) completion and submission instructions, submit the completed Evaluation Form, including the completed and signed Information and Confirmation sections, along with any other requested documentation—such as ASV scan reports—to your acquirer, payment brand, or other requester.

Completing the Evaluation

For each security practice, there is a choice of responses to indicate your status in implementing that practice. *Select only one response for each question.* The meaning for each response is provided in the table below.

Response	Use this response when:
I do this consistently.	You have formal processes in place to make sure this is practice performed regularly.
I do this sometimes.	You may have performed this practice occasionally on an ad-hoc basis, but you have no defined processes to make sure it always happens.
This is not applicable to my business environment (explain).	The practice does not apply to your business environment. For example, your business practice is to never store paper receipts with card numbers; therefore, you can answer N/A to practice B2 since making card numbers unreadable on paper receipts is not applicable to your business environment. *This response requires that you provide a clear explanation of why this practice does not apply to your business in the "Additional Information as Needed" column.*
I do not know / **I do not understand.**	If your response is "I do not know," this means you do not know whether this practice is implemented. For example, it is not your area of responsibility or was performed by a previous employee. If you responded "I do not understand," this means you do not understand the practice as it is stated and/or you do not know how to implement the practice.
I do not do this (explain).	This practice is applicable to your business environment but either you have not yet implemented all parts of the practice or you have no plans to implement the practice. *This response requires that you provide additional information about whether you are planning to implement the practice—and if so, when you expect the practice to be implemented—in the "Additional Information as Needed" column.*

After you complete this evaluation, review your results and provided tips on the last page and see whether there are any actions you need to perform to keep your business secure, or to make it more secure.

Information

1. Payment Acceptance Method for this Payment Channel

All transactions are conducted via e-commerce. My payment page/form is fully outsourced and payments are sent by a third-party service provider:			
1.	My e-commerce payment page is fully outsourced to a PCI DSS compliant third-party service provider.	□ Yes	□ No
2.	I have no access to the payment page regardless of whether my website is hosted internally or by a third-party service provider.	□ Yes	□ No
3.	Shopping pages are hosted on my website or by my website hosting provider.	□ Yes	□ No
4.	My website has only product information (shopping pages, etc.) available. I have no access to, or ability to control, any card data.	□ Yes	□ No
5.	When the customer is ready to enter card data, my website sends the request (via URL redirect or iframe) to a PCI DSS compliant third-party service provider that provides a payment page to the customer to collect card data.	□ Yes	□ No
6.	Card data is sent from the customer's browser to a PCI DSS compliant third-party service provider that sends payment via the Internet.	□ Yes	□ No
If you answered "Yes" to all the questions above, continue with Section 2 below. If you answered "No" to any question, return to the *Common Payment Systems* document and search for another appropriate payment diagram for your payment acceptance method.			

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):				
□ Retailer	□ Grocery and Supermarkets	□ Mail order/telephone order (MOTO)	□ Restaurants	□ Travel and Entertainment
□ Petroleum	□ E-Commerce	□ Others (please specify):		

What types of payment channels does your business serve? □ Mail order/telephone order (MOTO) □ E-Commerce □ Card-present (face-to-face)	Which payment channels are covered by this form? □ Mail order/telephone order (MOTO) □ 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).	□ Yes □ No

3. Data Security Essentials Evaluation

Some lettered sections are intentionally missing. The security practices below are specifically chosen for your type of payment system, and are part of a larger complete set. In addition, some numbers in each section may also be missing. Read the guidance in each of the lettered sections to understand why each security practice is important. For more information about these practices, see the *Guide to Safe Payments*.

GUIDANCE & SECURITY PRACTICES—*For each security practice below, select the answer that most closely reflects how you have implemented this practice for your business. If you choose a response that indicates further explanation is needed, or you would like to add more information for any other response, please explain in the Additional Information as Needed column.*

Security Practice	How have you implemented this practice?	Additional Information as Needed
A. Use strong passwords and change default ones Passwords are vital for security of your payment systems and card data. The confidentiality of all passwords should be protected and passwords should be changed if there is any suspicion of misuse. This includes all passwords you and your staff (including permanent full-time and part-time workers, contractors, consultants, etc.) use to log into or connect to your payment systems, computers, and other equipment. In addition, much equipment comes with default passwords "out of the box" (like "password" or "admin"). Hackers easily guess these out-of-the-box passwords since they are commonly known and often left unchanged. See "It's time to change your password" at www.PCISecurityStandards.org.		
1. You and your staff change passwords for computer access regularly, at least every 90 days.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
2. You and your staff make all passwords for computer access in your business unique and hard to guess: 7 or more characters and a combination of upper- and lower-case letters, numbers, and symbols. Consider using a passphrase as your password; you can make it personal and easy for you to remember.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
3. Immediately, you change out-of-the-box default passwords from your equipment and/or software suppliers. If you do not know where these passwords are or how to change them, find out from your payment system vendor or supplier, the individual who set up your payment system, or your merchant bank.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	

3. Data Security Essentials Evaluation *(continued)*

GUIDANCE & SECURITY PRACTICES—*For each security practice below, select the answer that most closely reflects how you have implemented this practice for your business. If you choose a response that indicates further explanation is needed, or you would like to add more information for any other response, please explain in the Additional Information as Needed column.*

Security Practice	How have you implemented this practice?	Additional Information as Needed
B. Protect your card data and only keep what you need The best way to protect against data breaches is not to store card data at all. Consider outsourcing your card processing to a PCI DSS compliant service provider or your merchant bank. Alternatively, talk to your merchant bank or payment terminal supplier about where your systems store data and how you can simplify the way you process payments. Also ask them for guidance if you need to conduct specific transactions (for example, for recurring payments—those for which you regularly charge your customers each month, quarter, etc.)		
2. If you need to keep paper with card numbers, or card numbers along with card security codes, you make the number unreadable, and you secure the paper in a locked drawer or safe with limited access. For example, to make the number unreadable, mark through the number with a thick, black marker such that you cannot see the number from front or back of page if you hold it to the light, or cut the number out.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
4. You periodically destroy or shred paper reports and/or receipts when no longer needed.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
5a. You only accept payment details in person or via phone, fax, or regular mail. If you accidentally receive card data via e-mail, you remove it and let the sender know your preferred method to receive card details—which is in person or via phone, fax, or regular mail.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	

3. Data Security Essentials Evaluation *(continued)*

GUIDANCE & SECURITY PRACTICES—*For each security practice below, select the answer that most closely reflects how you have implemented this practice for your business. If you choose a response that indicates further explanation is needed, or you would like to add more information for any other response, please explain in the Additional Information as Needed column.*

Security Practice	How have you implemented this practice?	Additional Information as Needed
D. Install patches from your vendors Often software (including software on your payment terminal) has flaws or mistakes made by programmers—these are called security holes, vulnerabilities, or bugs. Hackers exploit these weaknesses and break into your systems. Your payment system vendor or supplier will send out—or will notify you about—new "patches" (updates) to correct these flaws. It is important that you protect your systems by installing these updates per your vendors' instructions as soon as possible. Equally important, find out how your software is being regularly updated with patches and who is responsible (it could be you!). If you are not sure how patches get added or who is responsible, make it a point to ask your vendor/supplier.		
1. You know how your payment system, e-commerce payment system, or payment terminal software is updated; and you either receive notifications from your payment system vendor or supplier or you get the updates on your own (for example, by going to their website upon receipt of a notification e-mail).	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
2. You install new security patches or security updates from your payment system hardware and/or software suppliers right away, per their instructions (or your patches install automatically when they become available).	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	

3. Data Security Essentials Evaluation *(continued)*

GUIDANCE & SECURITY PRACTICES—*For each security practice below, select the answer that most closely reflects how you have implemented this practice for your business. If you choose a response that indicates further explanation is needed, or you would like to add more information for any other response, please explain in the Additional Information as Needed column.*

Security Practice	How have you implemented this practice?	Additional Information as Needed
E. Use trusted business partners and know how to contact them You use outside providers for payment-related services, payment devices, and perhaps applications. You may also have service providers that you share card data with, that support or manage your payment systems, or that you give access to card data. You may call them processors, vendors, suppliers, third parties, or service providers. All of these partners impact your ability to protect your card data, so it is critical you know who they are and which security questions to ask them. See *Questions to Ask your Vendors* at www.PCISecurityStandards.org.		
1. You keep a current list of all your internal and external payment business partners and service providers, including all relevant contact information (for example, names, phone numbers, e-mail addresses, website). These partners can include your merchant bank, payment processor, website and hosting provider, payment terminal supplier, software suppliers, IT help desk, etc.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
2. You can find your list of payment business partners and service providers when needed, and you or your staff call the appropriate partner whenever anything suspicious is identified.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
3. You evaluate potential and existing business partners, including determining whether they adhere to PCI DSS requirements.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	

3. Data Security Essentials Evaluation *(continued)*

GUIDANCE & SECURITY PRACTICES—*For each security practice below, select the answer that most closely reflects how you have implemented this practice for your business. If you choose a response that indicates further explanation is needed, or you would like to add more information for any other response, please explain in the Additional Information as Needed column.*

Security Practice	How have you implemented this practice?	Additional Information as Needed
F. Protect in-house access to your card data "Privilege abuse" is when a person uses someone else's privileges to access systems or data that the person is not authorized for, and is the top action leading to breaches. It is important to restrict access to payment card data to only those staff (including permanent full-time and part-time workers, contractors, consultants, etc.) who have a need for the data. A good way to start out is by denying all users access to data on your systems. Then you start with a clean slate, and only grant access to individuals with a specific business need for that access. The result is that the only users with access are those that specifically need that access.		
3. You and your staff read PCI SSC's Guide to Safe Payments annually (and new staff read it when they start), you record that all have read it, and you update that record annually. You also share the Guide with your business partners so they know what you expect.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	
4. You and your staff use your own user accounts and passwords and do not share with one another.	□ I do this consistently. □ I do this sometimes. □ This is N/A to my business environment (explain). □ I do not know / I do not understand. □ I do not do this (explain).	

4. Confirmation of Status

Part 4a. Questions Regarding Completion	
Did you get help to complete this form? If so, did you use: *(check all that apply)*	
□	A payment professional (for example, a Qualified Security Assessor or a Qualified Integrator Reseller) to help you complete this form?
□	A technology or service provider?
□	Someone else? Please describe.

Part 4b. Acknowledgment of Status – To be completed after conducting the Data Security Essentials Evaluation in Section 3	
Signatory(s) confirms: *(check all that apply)*	
□	This Confirmation and my responses within Section 3 fairly represent the results of my Data Security Essentials Evaluation.
□	I recognize that I will need to complete the applicable Data Security Essentials Evaluation Form for any other payment channels that I have.
□	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:	
Merchant Executive Officer Name:	
Title:	
Date:	

Results

5. Data Security Essentials Evaluation Results

Your evaluation had the following results:

Number of questions answered as:		Helpful Tips
0	**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.
0	**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.
0	**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.
0	**I do not know / I do not understand.**	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 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.
0	**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.