PAYMENT PROTECTION RESOURCES FOR SMALL MERCHANTS

Questions to Ask Your Vendors

VERSION 1.0 | JULY 2016

EPS®

PCI Security Standards Council®

Introduction

This document has been prepared as an aid to small-merchant owners and operators. By providing questions to ask your vendors and service providers, this is intended to assist with your understanding of how those entities support the protection of your customers' card data.

Questions to Ask your Vendors was developed as a supplement to the *Guide to Safe Payments*, part of the Payment Protection Resources for Small Merchants. Please refer to the *Guide to Safe Payments* and the other Payment Protection Resources for Small Merchants at the following:

RESOURCE	URL
Guide to Safe Payments	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Common Payment Systems	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glossary of Payment and Information Security Terms	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Vendors and Service Providers, and How They Function

Small businesses/merchants may come into contact with a number of payment vendors or services providers, and it is important for merchants to understand the type of vendor they are working with and ensure the vendor has taken appropriate steps to protect card data.

The table on page 2 describes the most common types of payment vendors and service providers and what merchants should look for with each vendor.

The table starting on page 3 provides merchants with questions they can ask their vendors or service providers to help them understand what the vendor's or service provider's role is in protecting card data.

Vendors and Service Providers

The table below describes the most common type of payment vendors and service providers and what merchants should look for with each vendor.

TYPE OF VENDOR/ SERVICE PROVIDER	FUNCTION	PCI STANDARD OR PROGRAM	LOOK FOR:
Payment application vendor	Sell and support applications that store, process, and/or transmit cardholder data.	Payment Application Data Security Standard (PA-DSS)	Application is on the List of PCI PA-DSS of Validated Payment Applications.
Payment terminal vendor	Sell and support devices used to accept card payments (e.g., payment terminal).	PIN Transaction Security (PTS)	Payment terminal is on the List of PCI Approved PTS Devices.
Payment processors, e-commerce hosting providers/processors	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.	PCI Data Security Standard (PCI DSS)	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
Providers of software as a service	Develop, host and/or manage your cloud-based web application or payment application (e.g., online ticketing or booking application).	PCI DSS	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
Integrators/resellers	Install PA-DSS validated payment applications on your behalf.	Qualified Integrators and Resellers (QIR)	Ask whether vendor is a PCI Qualified Integrator or Reseller (QIR). Vendor is on the List of PCI QIRs.
Providers of services that satisfy PCI DSS requirement(s)	Manage/operate systems or services on your behalf (e.g., firewall management, patching/AV services).	PCI DSS	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

Questions

The table below contains a series of questions for merchants to ask their vendors/service providers to determine whether the proper controls are in place to protect card data.

QUESTION *Asked by the merchant to the vendor*	DESIRED ANSWER FROM VENDOR	RECOMMENDED ACTION *Based on the vendor's response*
HOW SECURE IS YOUR SOLUTION OR PRODUCT?		
1. Does your solution/product ensure the secure capture and transmission of cardholder data?	**For face-to-face card-present payment transactions:** **YES** • Check here to see whether the payment terminal is PCI PTS approved: List of PCI Approved PTS Devices AND/OR • Check here to see whether the payment application is PCI PA-DSS validated: List of PCI PA-DSS of Validated Payment Applications OR • Check here to see whether the encryption solution is PCI P2PE validated: List of PCI P2PE Validated Solutions	If **NO**, ask Question 2.
	For card-not-present payment transactions (including e-commerce, mail order/telephone order): **YES** • Check here to see whether the payment application is PCI PA-DSS validated: List of PCI PA-DSS of Validated Payment Applications OR • Check here to see whether the service provider is a PCI DSS Compliant Service Provider: MasterCard's List of Compliant Service Providers Visa's Global Registry of Service Providers Visa Europe's Registered Member Agents	

Questions

QUESTION *Asked by the merchant to the vendor*	DESIRED ANSWER FROM VENDOR	RECOMMENDED ACTION *Based on the vendor's response*
HOW SECURE IS YOUR SOLUTION OR PRODUCT? *continued*		
2. Does our agreement with you (the vendor) include clauses that state that you will maintain PCI DSS compliance for your product/service (or become PCI DSS validated)?	**YES** Vendors with products/solutions that are or will become PCI DSS compliant should be willing to have that status included in a written agreement. For additional information on evidence to look for regarding PCI DSS compliant products/solutions, refer to Question 1 above.	If **NO**, consider another vendor or solution.
3. Does your product/solution store payment card information locally (in my store/shop location)?	**NO** If it does, merchants can consider a tokenization or encryption solution to better secure card data. See the *Guide to Safe Payments* for more information about encryption and tokenization.	If **YES**, merchant should confirm with vendor that the data is stored per PCI DSS requirements. If not, consider another vendor.
4. Does your product/solution protect payment card information with strong encryption?	**YES** 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.	If **NO**, consider another vendor or solution.

Questions

QUESTION *Asked by the merchant to the vendor*	DESIRED ANSWER FROM VENDOR	RECOMMENDED ACTION *Based on the vendor's response*
HOW SECURE IS THE INSTALLATION OF MY PRODUCT?		
5. If vendor is installing a payment application from the PCI Council's List of Validated Payment Applications, ask: Are you a PCI Qualified Integrator or Reseller (QIR)?	**YES** A QIR is trained and qualified by the Council to install and integrate PA-DSS payment applications, and their installations provide confidence that the PA-DSS payment application has been implemented in a manner that supports your PCI DSS compliance. Check here to see whether the vendor is listed: List of PCI QIRs.	If **NO**, ask follow-up questions at left.
Follow-up questions if response to above is NO: If the application the vendor is installing is not PCI SSC validated, or if the vendor is not a QIR, ask: • Do you provide support during installation to ensure our implementation meets PCI DSS requirements? • Do you provide an implementation guide? • Do you provide installation guidance on how to ensure card data is protected wherever it is stored, processed, or transmitted?	**YES** The vendor should have defined processes to assist you with installation of solution in compliance with PCI DSS requirements. Improper installation can make the solution vulnerable to data compromise. You are seeking a statement from the vendor that explains how they help you ensure PCI DSS requirements are or can be met for the product/ solution.	If **NO**, consider another vendor.

Questions

QUESTION *Asked by the merchant to the vendor*	DESIRED ANSWER FROM VENDOR	RECOMMENDED ACTION *Based on the vendor's response*
DO YOU PROVIDE ME WITH ONGOING SUPPORT AND MAINTENANCE FOR YOUR PRODUCT/SOLUTION? IF SO, HOW?		
6. Is your product/solution installed on my network or systems?	**YES** The vendor should provide on-going maintenance and support for software updates and security patches. In addition, they should provide and offer support for future version releases. It is in your best interest to have vendors/suppliers that fully support their products and assist you with installations/patches to ensure any changes to the system align to PCI requirements.	If the response is **YES**, see follow-up questions at left. If **NO**, go to Question 7.
Follow-up questions if response to above is YES: • Do you install patches and updates to the system/solution? • Do you do this in a manner that aligns to PCI DSS requirements? • How do you notify me; how are patches made available; and what support do you provide?	**YES** If the solution is never updated, it may become vulnerable to future compromises.	If **NO**, consider another vendor.
7. Is the solution installed on systems owned and maintained (hosted) by the service provider?	**YES** This is considered a Managed Service. If the service provider is hosting the solution, ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Check that the 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	If **YES**, ask follow-up question at left. If **NO**—if the managed service is not PCI DSS compliant—consider another solution.
Follow-up question if response to above is **YES**: Is the service provider's environment PCI DSS compliant?		

Questions

QUESTION *Asked by the merchant to the vendor*	DESIRED ANSWER FROM VENDOR	RECOMMENDED ACTION *Based on the vendor's response*
DO YOU PROVIDE ME WITH ONGOING SUPPORT AND MAINTENANCE FOR YOUR PRODUCT/SOLUTION? *continued*		
8. Do you require remote access to my payment system/solution to support it?	**NO** Remote access is frequently exploited in payment-data breaches. Remote access functionality should be limited to brief periodic use, and disabled at all other times.	If **NO**, go to Question 9. If **YES**, ask follow-up questions at left.
Follow-up questions if response to above is YES: • Do you require remote access to be always active?	**NO** Remote access functionality should be limited to brief periodic use, and disabled at all other times.	If **YES**—If remote access is required to be always active—consider another vendor or solution.
• What steps do you take to secure remote access connections?	**Your vendor should use multi-factor authentication AND a different username and password for each customer they access remotely.** Remote access connections can be secured through use of unique user IDs and passwords for each person using the system. In addition, multiple ways of verifying the identity of the person accessing the system (multi-factor authentication) should be used. Vendors that use unique username/passwords for each of their customers prevent a compromise of one of their customers from resulting in a compromise of many or all of their other customers via use of a common username and password.	If the product/solution does not offer multi-factor authentication for remote access, consider another solution.
9. Is the solution/product required to integrate with my other systems—for example, payment terminals, accounts receivable, or other systems that contain cardholder data?	**NO** A stand-alone payment terminal is simpler to secure than a more complex payment system that may have numerous connected systems. If the solution does require integration with other systems, does it simplify your processing environment, and/or how will it add value to your business? You should have a strong business need for integration, as using an integrated solution will increase PCI DSS scope because it makes your cardholder data environment larger and more complex.	If **YES**, consider another vendor or product unless there is a strong business requirement for having a more sophisticated solution with connections to other systems.

Questions

QUESTION *Asked by the merchant to the vendor*	DESIRED ANSWER FROM VENDOR	RECOMMENDED ACTION *Based on the vendor's response*
WHAT HAPPENS IF THERE IS A DATA BREACH?		
10. In the event that there is a data breach and your product/solution is involved: • If I experience penalties, do you offer support and protection? • How and when do you notify me if there is a breach? • What monitoring for data breaches and suspicious activities do you provide?	**YES** The vendor/service provider should provide support in the event of a cardholder data breach. The vendor/service provider should agree to cooperate with a forensics investigator, if there are questions about the managed service or solution they provide. The vendor/service provider should indemnify the merchant for fines incurred in the event there is a breach and it is determined that the vendor solution is the root cause.	If **NO**, consider another vendor or solution.
11. Does the vendor/service provider carry insurance to cover data breaches related to their product/solution?	**YES** Having insurance illustrates the vendor/service provider has thought through their responsibility and liability related to card data breaches. If **YES**, ask about the scope of coverage and whether your implementation will be covered.	If **NO**—if the vendor does not have insurance or is not willing to self-insure—consider obtaining your own insurance or using another vendor.
12. Does the vendor/service provider assist with notification of my customers in the event of a data breach and your product solution is the root cause?	**YES** Vendors/service provider should be willing to assist merchants with breach notification when their payment system is the root cause of the breach.	If **YES**, ask follow-up questions at left. If **NO**—if the vendor does not assist with notification—you should develop a plan for notification and/or consider another vendor.
If **YES**, to what degree do you assist with notification? • Do you cover the cost? • Do you send the notifications? • Do you provide credit monitoring for the customers impacted?		