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

PCI Security Standards Council®

INTRODUCTION 1

VENDORS AND SERVICE PROVIDERS 2

QUESTIONS 3

APPENDIX: Which questions are applicable to which vendors/solution providers? 9

Introduction

Questions to Ask your Vendors is a supplement to the *Guide to Safe Payments*, part of the Data Security Essentials for Small Merchants. 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.

Please refer to the *Guide to Safe Payments* and the other Data Security Essentials 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
Evaluation Tool	https://www.pcisecuritystandards.org/merchants/ 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.

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 types of payment vendors and service providers, their functions, and PCI standards or programs that apply to those functions. See the Appendix for a list of questions applicable to each type of vendor or service provider.

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 vendors, payment solution vendors	Sell and support devices or solutions (e.g., payment terminals or encryption solutions) used to accept card payments.	PIN Transaction Security (PTS) PCI Point-to-Point Encryption	Payment terminal is on the List of PCI Approved PTS Devices Encryption solution is on the List of PCI P2PE Solutions
Payment processors, e-commerce payment service providers, payment gateways, contact centers	Store, process, or transmit cardholder data on your behalf.	PCI Data Security Standard (PCI DSS)	Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Is Service Provider on one of these lists: MasterCard's List of Compliant Service Providers Visa's Global Registry of Service Providers Visa Europe's Registered Merchant Agents
E-commerce hosting providers	Host and manage your e-commerce server/website and/or develop and support your website. This provider may only provide hosting services or may additionally perform payment processing.		
Providers of software as a service, cloud-based hosting provider	Develop, host and/or manage your cloud-based web application or payment application (e.g., online ticketing or booking application).		
Providers of services that may help you meet PCI DSS requirements	Manage/operate systems or services on your behalf (e.g., data centers, co-location center providers, and information technology services such as firewall management, patching, or anti-virus services).		
Integrators/resellers	Install merchant payment systems.	Qualified Integrators and Resellers (QIR)	Ask whether the vendor is a PCI Qualified Integrator or Reseller (QIR). Vendor is on the List of PCI QIRs.

Glossary

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.

Note: If a vendor or solution provider does not provide you with positive answers to applicable questions in this table, you should strongly consider looking for another vendor or solution provider.

Ask:	Analyzing Vendor Answers – Helpful Steps and Additional Information for Merchants
Is the vendor's solution or product secure?	
1. Does the vendor's solution/product securely capture and transmit payment card information? *When a product or service is listed by PCI SSC or the payment card brands, it means that product/service has been validated according to a PCI security standard. Inclusion on these listings is an indication that the vendor or service provider has taken extra steps to provide secure products or services.*	**For solutions or products with payment terminals or payment applications:** • 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
	For card-not-present payment transactions (including e-commerce, mail order/telephone order): • 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 Merchant Agents OR • Check here to see whether the payment application is PCI PA-DSS validated: List of PCI PA-DSS of Validated Payment Applications

Questions

Ask:	Analyzing Vendor Answers – Helpful Steps and Additional Information for Merchants
Is the vendor's solution or product secure?	
2. Does the vendor's product/solution store payment card information in my systems (for example, those in my store/shop locations, with my web application, or with my e-commerce website). If so, how does that product/solution protect the data?	Products or solutions that tokenize or encrypt payment card information provide a way for merchants to secure card data. See the *Guide to Safe Payments* for more information about encryption and tokenization.
3. Does the vendor's product/solution protect payment card data during transmission with strong encryption?	Encryption converts information into a format that is unusable except to holders of a specific digital key. Securing payment card data in this way makes it less likely that it can be stolen and used fraudulently. **For payment terminals & integrated payment terminals:** • If you can, select from the List of PCI P2PE Validated Solutions for a product/solution in which card data is encrypted. Use of a PCI listed P2PE solution means payment card data is protected soon when you receive it and as it travels through your network and to your payment processor. **For payment applications:** • Check with your vendor, reseller, or integrator that the payment application is PCI PA-DSS validated. **For hosted e-commerce websites, web applications or payment applications:** • Ask your service provider whether they use a secure version of Transport Layer Security (TLS) to protect transmissions of payment card data.
4. Is the vendor's solution/product required to be integrated with my other systems—for example, with my payment terminals, accounts receivable, or other systems that contain cardholder data?	A stand-alone or isolated payment terminal is simpler to secure than a more complex payment system that may have many connected systems. **If the solution requires integration with other systems in your environment, consider the following:** • Does it simplify your processing environment? • How does it add value to your business? • Do you need this type of solution? Consider that it will increase your business risk and complexity by making your cardholder data environment larger and harder to secure. You may want to consider another vendor or product unless there is a strong business requirement for having a more sophisticated solution with connections to your other systems.

Questions

Ask:	Analyzing Vendor Answers – Helpful Steps and Additional Information for Merchants
Does the vendor help me securely install or set up the product or solution?	
5. If the vendor is installing a payment application or system in my environment, ask: • Is the vendor a PCI Qualified Integrator or Reseller? • If the vendor does not install the payment application or system, are you expected to install it?	QIRs are integrators and resellers specially trained by the Council to address critical security controls while installing merchant payment systems. QIRs reduce merchant risk and mitigate the most common causes of payment data breaches by focusing on critical security controls. Check here to see whether the vendor is listed: List of PCI QIRs.
6. Regardless of whether the vendor is a QIR, if the vendor is installing a payment application or system, ask: • Does the vendor support me during installation and ensure installation is done securely? • Does the vendor provide an implementation guide to help me set up the application securely?	Improper installation can make your system vulnerable to compromise. The vendor should either install the application or system in a secure manner or help you by providing you with implementation guidance. The implementation should cover, at a minimum, how to change default passwords and establish strong ones, how to manage patches and updates, and a description of how the vendor uses remote-access software to access your business (and what your role is with such software). More detail about each of these three areas is included at Questions 7-9 below.

Questions

Ask:	Analyzing Vendor Answers – Helpful Steps and Additional Information for Merchants
Does the vendor help me securely install or set up the product or solution?	
7. Does the vendor provide support during installation or set-up of the product/solution to help me change vendor-supplied default passwords? • Does the vendor help me set up strong passwords?	Weak passwords and vendor-supplied default passwords comprise one of the three leading causes of merchant data breaches (the other two are covered at Questions 8 and 9 below). Vendor-supplied default passwords are those that come with a product or solution, such as the first-time password for a new system or application, a merchant hosted e-commerce website, or hotel booking application. These vendor-supplied default passwords are often simple and commonly known to hackers (like "admin," "password," or the vendor company or product name). These passwords should be changed to a strong password when the product is installed or set-up for the first time. If you change it to a simple password (like "12345"), it will make it easy for a hacker to get into your payment systems. If the vendor does not change default passwords when installing or setting up the application or system, they should provide you with implementation guidance that explains how to change these passwords and how to establish strong passwords.
Does the vendor securely support and maintain the product/solution?	
8. To understand patches (software security "fixes") and updates for the product/solution, ask the vendor: • What support and guidance does the vendor provide to my business during the patching/updating process? • Are patches and updates provided and installed automatically by the vendor? • Am I expected to obtain and install those patches/updates? • How does the vendor notify me when patches/updates are available or have been automatically applied? • For hosted e-commerce websites, web applications, or payment applications, does the vendor take responsibility for patching/updating the solution they provide to me?	Unpatched applications and systems comprise one of the three leading causes of merchant data breaches (the other two are covered at Questions 7 and 9). Unpatched systems often contain vulnerabilities that hackers use to gain access to your payment card data. The vendor should provide on-going maintenance and support for their applications or systems via software updates and security patches (software security "fixes"). For example, the vendor should send you patches when needed, notify you when they are available, and provide guidance about how to install them. It is in your best interest to have vendors/suppliers that fully support their products/solutions and either take responsibility for or assist you with patches and updates to ensure any changes keep your business secure.

Questions

Ask:	Analyzing Vendor Answers – Helpful Steps and Additional Information for Merchants
Does the vendor securely support and maintain the product/solution?	
9. Does the vendor require remote access into my payment application or system to support the vendor product or solution? • Does the vendor require remote access to be always active? • What steps does the vendor take to secure remote access? • Does the vendor use the same or a different password for each of their customers?	Always available or "always on" remote access is one of the three leading causes of merchant breaches (the other two are at Questions 7 and 8 above). Remote access provides a path from outside a merchant network into the merchant network, which a hacker can easily use to compromise your system (or hosted system) and gain access to cardholder data. This can include remote access into a merchant network, used by the vendor to support a payment terminal or application, or to support a third-party hosted merchant environment or web application. To protect yourself, you should make sure that vendors help you by: • Limiting remote access to brief periodic use • Disabling remote access when it is not being used • Using multi-factor authentication (a way of verifying the identity of a person accessing a system using two or more factors, such as something they know and something they do or are) • Using a different username and password for each customer the vendor accesses remotely (to prevent the use of a commonly-used username and password leading to a compromise of all their customers)
Is the vendor PCI DSS compliant for the service they are offering me?	
10. Is this solution or product run from systems owned and maintained (hosted) by the vendor? This means your vendor is a service provider. **Ask:** • Is the service provider's environment PCI DSS compliant? • Does the service provider's PCI DSS assessment cover the specific services the service provider is offering me?	This is considered a "managed service." Ask for the service provider's PCI DSS Attestation of Compliance and check whether their assessment included the service you are using. Check to see if 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 Merchant Agents
11. Does the vendor's agreement with me include clauses that state that the vendor will maintain PCI DSS compliance for their service (or become PCI DSS validated)?	Vendors with services (also called service providers) that are or will become PCI DSS compliant should be willing to have that status included in a written agreement. Check to see if the service provider is on one of the lists included in Question 10 above.

Questions

Ask:	Analyzing Vendor Answers – Helpful Steps and Additional Information for Merchants
Will the vendor provide support if there is a breach of my cardholder data?	
12. If there is a data breach and vendor's product/solution is involved, ask: • What monitoring for data breaches and suspicious activities do you provide? • How and when do you notify me if there is a breach? • If I experience fines/penalties, do you offer support and protection?	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 product/solution they provide. The vendor/service provider should agree to help you for fines incurred in the event there is a breach and it is determined that the vendor product/solution is the cause.
13. Does the vendor/service provider carry insurance to cover data breaches related to their product/solution?	Having insurance illustrates the vendor/service provider has thought through their responsibility and liability related to cardholder data breaches. If they do carry insurance, ask about the scope of coverage and whether your implementation will be covered.
14. Does the vendor/service provider assist with notification of my customers in the event of a data breach when the vendor product/solution is the cause?	Vendor/service provider should be willing to assist merchants with breach notification when their payment system is the cause of the breach.
15. If yes to question 14, to what degree do does the vendor assist with notification? Does the vendor: • Cover the cost? • Send the notifications? • Provide credit monitoring for the customers impacted?	If the vendor does not assist with notification, you should develop a plan for notifying your customers in the event of a breach of cardholder data.

Appendix

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