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

Guide to Safe Payments

Version 3.0 • April 2024

PCI Security Standards Council ®

UNDERSTANDING YOUR RISK

Understanding your risk

As a small business, you are a prime target for data thieves.

When your payment card data is breached, the fallout can strike quickly. Your customers lose trust in your ability to protect their personal information. They take their business elsewhere. There are potential financial penalties and damages from lawsuits, and your business may lose the ability to accept payment cards. A survey of 1,015 small and medium businesses found 60% of those breached close in six months. (NCSA)

50%

OF SMALL BUSINESSES HAVE BEEN BREACHED IN THE PAST 12 MONTHS.
(Ponemon Institute)

£30 billion

COST TO UK BUSINESS DUE TO CYBER SECURITY BREACHES IN 2016
(Beaming UK)

61%

OF BREACHES HIT SMALLER BUSINESSES LAST YEAR, UP FROM THE PREVIOUS YEAR'S 53%
(Verizon 2017)

ONLY **39%**

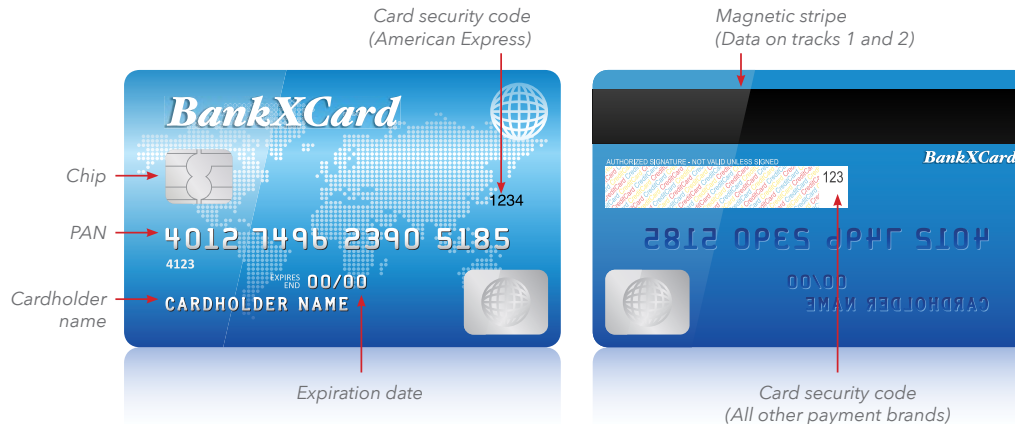OF SMALL FIRMS HAVE FORMAL POLICIES COVERING CYBER SECURITY RISKS IN 2017
(Dept for Culture Media and Sport)

What's at risk?

YOUR CUSTOMERS' CARD DATA IS A GOLD MINE FOR CRIMINALS. DON'T LET THIS HAPPEN TO YOU! Follow the actions in this guide to protect against data theft.

Examples of payment card data are the primary account number (PAN) and three or four-digit card security code. The red arrows below point to types of data that require protection.

TYPES OF DATA ON A PAYMENT CARD

Card security code
(American Express)

Magnetic stripe
(Data on tracks 1 and 2)

BankXCard

Chip

PAN

4012 7496 2390 5185
4123
EXPIRES END 00/00
CARDHOLDER NAME
1234

Cardholder
name

AUTHORIZED SIGNATURE - NOT VALID UNLESS SIGNED

BankXCard

4012 7496 2390 5185
00/00
CARDHOLDER NAME
123

Expiration date

Card security code
(All other payment brands)

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements that can help small merchants to protect customer card data located on payment cards.

Small merchants may be familiar with validating their PCI DSS compliance via a Self-Assessment Questionnaire (SAQ).

For more information on PCI DSS, see the Resources at the end of this guide.

PCi Security Standards Council ®

Understanding your payment system: Common payment terms

Accepting face-to-face card payments from your customers requires special equipment. Depending on where in the world you are located, equipment used to take payments is called by different names. Here are the types we reference in this document and what they are commonly called.

A **PAYMENT TERMINAL** is the device used to take customer card payments via swipe, dip, insert, tap, or manual entry of the card number. Point-of-sale (or POS) terminal, credit card machine, PDQ terminal, or EMV/chip-enabled terminal are also names used to describe these devices.

An **ELECTRONIC CASH REGISTER** (or till) registers and calculates transactions, and may print out receipts, but it does not accept customer card payments.

An **INTEGRATED PAYMENT TERMINAL** is a payment terminal and electronic cash register in one, meaning it takes payments, registers and calculates transactions, and prints receipts.

A **MERCHANT BANK** is a bank or financial institution th t processes credit and/or debit card payments on behalf of merchants. Acquirer, acquiring bank, and card or payment processor are also terms for this entity.

ENCRYPTION (or cryptography) makes card data unreadable to people without special information (called a key). Cryptography can be used on stored data and data transmitted over a network. Payment terminals that are part of a PCI-listed P2PE solution provide merchants the best assurance about the quality of the encryption. With a PCI-listed P2PE solution, card data is always entered directly into a PCI-approved payment terminal with something called "secure reading and exchange of data (SRED)" enabled. This approach minimizes risk to clear-text card data and protects merchants against payment-terminal exploits such as "memory scraping" malware. Any encryption that is not done within a PCI-listed P2PE should be discussed with your vendor.

A **PAYMENT SYSTEM** includes the entire process for accepting card payments. Also called the cardholder data environment (CDE), your payment system may include a payment terminal, an electronic cash register, other devices or systems connected to a payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), and the connections out to a merchant bank. It is important to use only secure payment terminals and solutions to support your payment system. See page 22 for more information.

Understanding your E-commerce Payment System

When you sell products or services online, you are classified as a e-commerce merchant. Here are some common terms you may see or hear and what they mean.

An **E-COMMERCE WEBSITE** houses and presents your business website and shopping pages to your customers. The website may be hosted and managed by you or by a third party hosting provider.

Your **SHOPPING PAGES** are the web pages that show your product or services to your customers, allowing them to browse and select their purchase, and provide you with their personal and delivery details. No payment card data is requested or captured on these pages.

MERCHANT
E-COMMERCE
WEBSITE

PCI DSS COMPLIANT
THIRD-PARTY
SERVICE PROVIDER

BANK

MERCHANT
SHOPPING
PAGES

INTERNET

MERCHANT
PAYMENT
PAGE

Your **PAYMENT PAGE** is the web page or form used to collect your customer's payment card data after they have decided to purchase your product or services. Handling of card data may be 1) managed exclusively by the merchant using a shopping cart or payment application, 2) partially managed by the merchant with the support of a third party using a variety of methods, or 3) wholly outsourced to a third party. Most times, using a wholly outsourced third party is your the safest option - and it is important to make sure they are a PCI DSS validated third party.
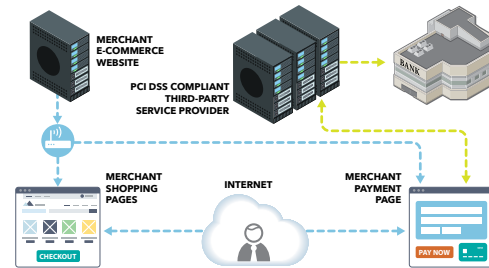
An **E-COMMERCE PAYMENT SYSTEM** encompasses the entire process for a customer to select products or services and for the e-commerce merchant to accept card payments, including a website with shopping pages and a payment page or form, other connected devices or systems (for example Wi-Fi or a PC used for inventory), and connections to the merchant bank (also called a payment service provider or payment gateway). Depending on the merchant's e-commerce payment scenario, an e-commerce payment system is either wholly outsourced to a third party, partially managed by the merchant with support from a third party, or managed exclusively by the merchant.
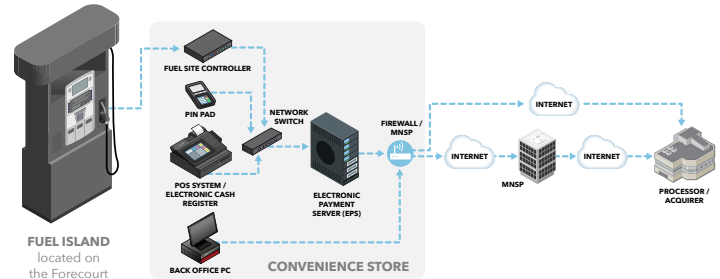
Understanding your Petroleum & Fuel System

When you sell petroleum & fuel, you are classified as a petroleum merchant. Here are some common terms you may see or hear and what they mean.

A **PETROLEUM SYSTEM** encompasses the entire process for a consumer to purchase petroleum either outside at an unattended Fuel Island or inside at a POS Terminal.

An **ELECTRONIC PAYMENT SERVER (EPS)** (may also be part of the Site Controller) is a software payment application, usually present in a semi-integrated system, that gives point-of-sale (POS) systems a way to perform payment transactions in a standard way, independent of the payment networks providing authorization. The EPS separates payment from the POS system or outdoor sales processor (OSP). The EPS manages payment requests from the POS systems and OSP, card data acquisition from the EMV terminals, and payment authorizations for all POS systems and the OSP. Generally, all payment business logic is implemented within the EPS. The POS, OSP, and EMV terminals are considered "dumb" devices programmed to implement only the interface to/from the EPS.

A **FUEL SITE CONTROLLER** is a software application designed to interface with the various forecourt devices of a fuel station, but primarily the fuel dispensers. The fuel site controller handles both physical and logical device control. Typically, it controls the device states, makes sure unauthorized state changes are prevented, and ensures processes follow regulations and specifications.

A **FUEL ISLAND** is the area of a convenience and retail fuel site where fuel dispensers are physically located. Generally, the fuel island is part of the site's forecourt. The fuel island can be either manned or unmanned. Unmanned fuel islands are often described as self-service.

FUEL ISLAND located on the Forecourt — FUEL SITE CONTROLLER, PIN PAD, NETWORK SWITCH, POS SYSTEM / ELECTRONIC CASH REGISTER, BACK OFFICE PC, CONVENIENCE STORE, ELECTRONIC PAYMENT SERVER (EPS), FIREWALL / MNSP, INTERNET, MNSP, PROCESSOR / ACQUIRER

A **MANAGED NETWORK SERVICE PROVIDER (MNSP)** is a service provider who administers site level network connectivity, failover, on premise network device configurations, remote connectivity such as VPN, and/or network security features. The MNSP may be responsible for maintaining the controls that protect network devices from misconfiguration, including insecure configuration. These providers generally have remote access to a site's network, and thus a compromise of a MNSP system could lead to a compromise of the cardholder data environment.

A **BACK OFFICE PC** is a dedicated personal computer used to manage nonconsumer business operations for a convenience and retail fuel site. The back office system supports daily operational activities such as inventory management, price book, product supply, fuel management, site-level accounting, and daily reporting and journaling.

The **FORECOURT** is the area where fuel dispensers are present and accessible to consumers wishing to refuel their vehicle. It is the area outside the salesroom or the convenience store of a fuel station where consumers park their vehicles while dispensing fuel.

How is your business at risk?

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 configu ed 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.

How do you sell your goods or services? There are three main ways:

1. A person walks into your shop and makes a purchase with their card.
2. A person visits your website and pays online.
3. A person calls your shop and provides card details over the phone, or sends the details in the mail or via fax.

COMPLEX ENVIRONMENT   SIMPLE ENVIRONMENT

HARDER TO REDUCE RISK   EASIER TO REDUCE RISK

Understanding your risk: Payment system types

Your security risks vary greatly depending on the complexity of your payment system, whether face-to-face or online.

DIAL-UP PAYMENT TERMINAL

PHONE LINE

BANK
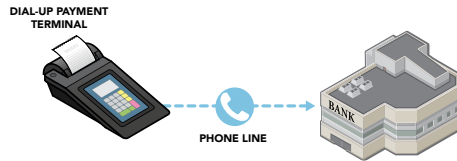
Simple payment system for in-shop purchases

GENERAL USE COMPUTERS

IP PHONES

ELECTRONIC CASH REGISTER

ROUTER/ FIREWALL

INTERNET

BANK

PAYMENT TERMINAL

CAMERAS

Complex payment system for in-shop purchases, with Wi-Fi, cameras, Internet phones, and other attached systems

MERCHANT E-COMMERCE WEB SITE

BANK

MERCHANT ROUTER / FIREWALL

CHECKOUT

INTERNET

PAY NOW

MERCHANT SHOPPING PAGES

MERCHANT PAYMENT PAGE

Complex e-commerce payment system for online shop purchases, with merchant managing their own website and payment page

Use the Common Payment Systems to help you identify what type of payment system you use, your risk, and the recommended security tips as a starting point for conversations with your merchant bank and vendor partners.

PCi Security Standards Council®

PROTECT YOUR BUSINESS WITH THESE SECURITY BASICS

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	🪙
Ease	🔧
Risk Mitigation	✋✋✋

Protect your card data and only store what you need
Cost	🪙
Ease	🔧
Risk Mitigation	✋✋

Inspect payment terminals for tampering
Cost	🪙
Ease	🔧
Risk Mitigation	✋✋

Use trusted business partners and know how to contact them
Cost	🪙
Ease	🔧
Risk Mitigation	✋

Install patches from your vendors
Cost	🪙
Ease	🔧🔧
Risk Mitigation	✋✋✋

Protect in-house access to your card data
Cost	🪙
Ease	🔧🔧
Risk Mitigation	✋✋

Don't give hackers easy access to your systems
Cost	🪙🪙
Ease	🔧🔧
Risk Mitigation	✋✋✋

Use anti-virus software
Cost	🪙🪙
Ease	🔧🔧
Risk Mitigation	✋✋

Scan for vulnerabilities and fix issues
Cost	🪙🪙
Ease	🔧🔧
Risk Mitigation	✋✋✋

Use secure payment terminals and solutions
Cost	🪙🪙🪙
Ease	🔧🔧
Risk Mitigation	✋✋✋

Protect your business from the Internet
Cost	🪙🪙
Ease	🔧🔧🔧
Risk Mitigation	✋✋✋

For the best protection, make your data useless to criminals
Cost	🪙🪙🪙
Ease	🔧🔧🔧
Risk Mitigation	✋✋✋

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.

Use strong passwords and change default ones

Your passwords are vital for computer and card data security. Just like a lock on your door protects physical property, a password helps protect your business data. Also be aware that computer equipment and software out of the box (including your payment terminal) often come with default (preset) passwords such as "password" or "admin," which are commonly known by hackers and are a frequent source of small merchant breaches.

CHANGE YOUR PASSWORDS REGULARLY. Treat your passwords like a toothbrush. Don't let anyone else use them and get new ones every three months.

TALK TO YOUR SERVICE PROVIDERS. Ask your vendors or service providers about default passwords and how to change them. Then do it! Also, if your service provider manages passwords for your systems, ask them if they've changed those vendor default passwords.

MAKE THEM HARD TO GUESS. The most common passwords are "password" and "123456." Hackers try easily-guessed passwords because they're used by half of all people. A strong password has seven or more characters and a combination of upper and lower case letters, numbers, and symbols (like !@#$&*). A phrase can also be a strong password (and may be easier to remember), like "B1gMac&frieS."

DON'T SHARE. Insist on each employee having their own login IDs and passwords – never share!

TYPICAL DEFAULT PASSWORDS THAT MUST BE CHANGED:

[none]

[name of product/ vendor]

1234 or 4321

access

admin

anonymous

company name

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

65% of SMBs that have a password policy do not strictly enforce it

Ponemon Institute

For more about password security, see these resources on the PCI Council website:

INFOGRAPHIC
It's Time to Change Your Password

VIDEO
Learn Password Security in 2 Minutes

Protect card data and only store what you need

It's impossible to protect card data if you don't know where it is.

What can you do?

Another place to consider whether you are storing payment data is in emails. If you receive card details via email, you can still process the transaction, but delete the email immediately and then let the sender know how you prefer to receive cardholder data (and that email is not the best way to send it). Do not simply reply using the original email from your customer. Instead delete the card details from the reply email, otherwise you are further exposing the card data via storing the original email, the sent email, etc.

Tokenization has a similar goal to encryption but works differently. It substitutes card data with meaningless data (a "token") that has no value to a hacker. Merchants can use tokens to submit subsequent transactions, process a refund, etc. without needing to store the actual payment card details. The token is used by your payment processor to look up the card details, which they store instead of you.

ASK AN EXPERT. Ask your payment terminal vendor, service provider, or merchant bank where (or if) your systems store data and if you can simplify how you process payments. Also ask how to conduct specific t ansactions (for example, for recurring payments) without storing the card's security code.

OUTSOURCE. 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. See Resources on page 26 for lists of compliant service providers.

IF YOU DON'T NEED CARD DATA, DON'T STORE IT. Securely destroy/shred card data you don't need. If you need to keep paper with sensitive card data, mark through the data with a thick, black marker until it is unreadable and secure the paper in a locked drawer or safe that only a few people have access to.

LIMIT RISK. Rather than accepting payment details via email, ask customers to provide it via phone, fax, or regular mail.

TOKENIZE OR ENCRYPT. Ask your merchant bank if you REALLY need to store that card data. If you do, ask your merchant bank or service provider about encryption or tokenization technologies that make card data useless even if stolen.

SEE PAGE 24
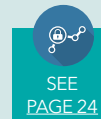
ENCRYPTION PRIMER

Cryptography uses a mathematical formula to render plaintext unreadable to people without special knowledge (called a key). Cryptography is applied to stored data as well as data transmitted over a network.

ENCRYPTION changes plaintext into cyphertext.

DECRYPTION changes cyphertext back into plaintext.

For example:

This is secret stuff

ENCRYPTION KEY

5a0 (k$hQ%...

DECRYPTION KEY

This is secret stuff

Inspect payment terminals for tampering

"Skimming devices" sweep up your customers' card data as it enters a payment terminal. It's vital that you and your staff know how to spot a skimming device, what your payment terminals should look like, and how many you have. You need to regularly check your payment terminals to make sure they have not been tampered with. If there is any suspicion that a terminal has been tampered with, **DO NOT USE it**, and report this immediately to your merchant bank and/or terminal vendor.

See the PCI Council's guide: Skimming Prevention - Overview of Best Practices for Merchants

Be vigilant and follow these steps:

KEEP A LIST of all payment terminals and take pictures (front, back, cords, and connections) so you know what they are supposed to look like.

LOOK FOR OBVIOUS SIGNS of tampering, such as broken seals over access cover plates or screws, odd/different cabling, or new devices or features you don't recognize. The Council's guide (referenced below) can help.

PROTECT TERMINALS. Keep them out of customers' reach when not in use and restrict public viewing of the screens. Make sure your payment terminals are secure before you close your shop for the day, including any devices that read your customers' payment cards or accept their personal identific tion numbers (PINs).

CONTROL REPAIRS. Only allow payment terminal repairs from authorized repair personnel, and only if you are expecting them. Tell your staff too. Monitor any third-parties with physical access to your payment terminals, even if they are there for another reason, to make sure they don't modify your payment terminals.

CALL your payment terminal vendor or merchant bank immediately if you suspect anything!

Use trusted business partners and know how to contact them

Cost   ⓧ
Ease   🔧
Risk Mitigation   ✋

You use outside providers for payment-related services, devices and 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, third parties, or service providers. All of these impact your ability to protect your card data, so it's critical you know who they are and what security questions to ask them.

KNOW WHO TO CALL. Who is your merchant bank? Who else helps you process payments? Who did you buy your payment device/software from and who installed it for you? Who are your service providers?

KEEP A LIST. Now that you know who to call, keep company and contact names, phone numbers, website addresses, and other contact details where you can easily find them in an eme gency.

CONFIRM THE SECURITY OF YOUR SERVICE PROVIDERS. Is your service provider adhering to PCI DSS requirements? For e-commerce merchants, it is important that your payment service provider is PCI DSS compliant too! See Resources on *page 26* for lists of compliant service providers.

ASK QUESTIONS. Once you know who your outside providers are and what they do for you, talk to them to understand how they protect card data. Use *Questions to ask your Vendors* to help you know what to ask.

UNDERSTAND COMMON VENDORS. Review the sidebar to the right to understand common types of vendors or service providers you may work with.

COMMON VENDORS

Refer to the table in the Questions to ask your Vendors for more details about these common vendors:

- Payment terminal vendors
- Payment application vendors
- Payment system installers (called Integrators/ Resellers)
- Service providers that perform payment processing, or e-commerce hosting or processing
- Service providers that help you meet PCI DSS requirement(s) (for example, providing fi ewall or antivirus services)
- Providers of Software as a Service

Software can have flaws that are discovered after release, caused by mistakes made by programmers when they wrote the code. These flaws are also called security holes, bugs or vulnerabilities. Hackers exploit these mistakes to break into your computer and steal account data. Protect your systems by applying vendor-supplied "patches" to fix coding errors. Timely installation of security patches is crucial!

It is important that you know how your software is being regularly updated with patches and who is responsible (it could be you!). Also, some patches install automatically when they become available. If you're not sure how patches get added or who is responsible, make it a point to ask your vendor/ supplier.

ASK your vendor or service provider how it notifies you o new security patches, and make sure you receive and read these notices.

WHICH VENDORS SEND YOU PATCHES? You may get patches from vendors of your payment terminal, payment applications, other payment systems (tills, cash registers, PCs, etc.), operating systems (Android, Windows, iOS, etc.), application software (including your web browser), and business software.

MAKE SURE your vendors update your payment terminals, operating systems, etc. so they can support the latest security patches. Ask them.

E-COMMERCE MERCHANTS. Installing patches as soon as possible is very important for you too. Also look out for patches from your payment service provider. Ask your e-commerce hosting provider whether they patch your system (and how often). Make sure they update the operating system, e-commerce platform and/or web application so it can support the latest patches.

FOLLOW your vendor's/service provider's instructions and install those patches as soon as possible.

Protect in-house access to your data

Privilege abuse means a person using…

Someone else's information and details to gain access to systems or data that person is not authorized to have access to.

25% OF BREACHES INVOLVE INTERNAL ACTORS.

25%
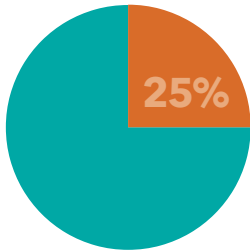
Verizon 2017

ACCESS CONTROL IS ALL IMPORTANT. Set up your system to grant access only based on a "business need-to-know." As the owner, you have access to everything. But most employees can do their job with access only to a subset of data, applications, and functions.

LIMIT ACCESS to payment systems and unencrypted card data to only those employees that need access, and only to the data, applications and functions they need to do their jobs.

KEEP A LOG. Track all "behind the counter" visitors in your establishment. Include name, reason for visit, and name of employee that authorized visitor's access. Keep the log for at least a year.

SECURELY DISPOSE OF DEVICES. Ask your payment system vendor or service provider how to securely remove card data before selling or disposing of payment devices (so data cannot be recovered).

SHARE THIS INFORMATION. Give this guide to your employees, business partners, and third-party service providers (such as e-commerce hosting providers) so they know what is expected.

MAKE USER IDS UNIQUE for each person with access to your payment system whenever possible. This will help you keep track of who logs in and when, and any changes they make.

Consider giving employees access to take payments but not to process refunds, or to take new bookings/orders but not to access payment card data related to existing booking/orders. Some employees should have no access at all.

Don't give hackers easy access to your systems

HACKERS = THREATS

One of the easiest ways for hackers to get into your system is through people you trust. You need to know how your vendors are accessing your system to make sure it's not opening up any holes for hackers.

Multi-factor authentication uses a username and password plus at least one other factor (like a smart card, dongle*, or one-time passcode).

*a handy device that connects to a computer to allow access to wireless, software features, etc.

FIND OUT. Ask your payment system vendor or service provider if they use remote access to support or access your business systems.

ASK HOW TO LIMIT USE OF REMOTE ACCESS. Many remote access programs are always on, or always available by default, meaning the vendor can access your systems remotely all the time (this also means that hackers can access your systems too since many vendors use commonly-known passwords for remote access). Reduce your risk – ask your vendor how to disable remote access when not needed, and how to enable it when your vendor or service provider specifically requests it.

DISABLE IT WHEN DONE. To protect your business, it's important that you take a part in managing how and when your vendors can access your systems.

USE STRONG AUTHENTICATION. If you must allow remote access, require multi-factor authentication and strong cryptography.

ENSURE SERVICE PROVIDERS USE UNIQUE CREDENTIALS. Each one must use remote access credentials that are unique to your business and that are not the same ones used for other customers.

ASK FOR HELP. Ask your vendor or service provider for help disabling remote access, or (if your vendor or service provider needs remote access) for help setting up multi-factor authentication. See Questions to ask your Vendors to help you know exactly what to ask them.

If your vendor supports or troubleshoots your payment system from their office (and not from your location) they are using the Internet and remote access software to do this.

Examples of products your vendor may install on your terminal and use to support you remotely include VNC & LogMeIn.

Hackers write viruses and other malicious code to exploit software features and coding mistakes, so they can break into your systems and steal card data. Using up-to-date anti-virus (also called anti-malware) software helps to protect your systems.

INSTALL ANTI-VIRUS SOFTWARE TO PROTECT YOUR PAYMENT SYSTEM. It is easy to install and can be obtained from your local office supply shop or I   retailer.

SET THE SOFTWARE TO "AUTOMATIC UPDATE" so you always get the most recent protection available.

GET ADVICE. Ask your IT retailer about products they recommend for anti-virus/anti-malware protection.

RUN AUTOMATIC SCANS. Schedule regular full system scans, since your systems may have been infected by new malware that was released before your anti-virus software was able to detect it.

E-COMMERCE MERCHANTS. Installing anti-virus software is very important for you too. Ask your service provider(s) whether they have installed anti-virus software on your system (and how often it is updated). Make sure they keep the anti-virus software up-to-date and regularly scan your system for malware.

New vulnerabilities, security holes, and bugs are being discovered daily. It's vital to have your Internet-facing systems tested regularly to identify these new risks and address them as soon as possible. Your Internet-facing systems (like many payment systems) are the most vulnerable because they can be easily exploited by criminals, allowing them to sneak into your systems.

GET ADVICE. Ask your merchant bank if they have partnerships with any PCI Approved Scanning Vendors (ASVs). Ask your vendors and service providers too.

TALK TO A PCI ASV. These vendors can help you with tools that automatically identify vulnerabilities and misconfigu ations in your Internet-facing payment systems, e-commerce website, and/or networks and provide you with a report if, for example, you need to apply a patch. The PCI Council's list (referenced to the left) can help you find a scanning vendo .

SELECT A SCANNER. Contact several PCI ASVs to find one with a program suitable for your small business.

ADDRESS VULNERABILITIES. Ask your ASV, payment system vendor or service provider, or merchant bank for help correcting issues found by scanning.

The PCI Council's Approved Scanning Vendors (ASVs) perform external vulnerability scanning and reporting. See PCI's *List of PCI-Approved Scanning Vendors*

Use secure payment terminals and solutions

A sure way to better protect your business is to use secure payment solutions and trained professionals to help you. Here's how to choose safe products and make sure they are set up securely.

For PCI payment terminals and secure card readers that encrypt card data, see *page 24*.

USE SECURE PAYMENT TERMINALS AND PIN ENTRY DEVICES. The PCI Council approves payment terminals that protect PIN data. Make sure your payment terminal or device is on the List of PCI Approved PTS Devices for equipment that provides the best security, and supports "EMV chip."

USE SECURE SOFTWARE. Make sure your payment software is on the List of PCI Validated Payment Applications.

USE QUALIFIED PROFESSIONALS. Make sure the person installing your payment system does it correctly and securely. Choose from the List of PCI QIRs to help you. Ask your merchant bank to help you make the selection.

USE SECURE E-COMMERCE PAYMENT SERVICE PROVIDERS. If you don't already, consider using a PCI DSS complaint service provider to help you securely process your e-commerce payment transactions, and/or to manage your e-commerce website.

LOOK FOR PCI DSS COMPLIANT SERVICE PROVIDERS. Make sure your payment service provider is compliant with PCI DSS. Check Mastercard's and Visa's lists to confirm th t they are listed:
MasterCard's List of Compliant Service Providers
Visa's Global Registry of Service Providers
Visa Europe's Registered Agents

REFER TO THIS LIST OF VENDOR QUESTIONS. Use Questions to ask your Vendors to help you know what to ask your vendors and service providers.

Your customers enter their personal identific tion numbers (PINs) for their payment cards into your payment terminal or PIN entry device. It is important to use secure devices to protect your customers' PIN data.

Protect your business from the Internet

The Internet is the main highway used by data thieves to attack and steal your customers' card data. For this reason, if your business is on the Internet, anything you use for card payments needs extra protection.

A firewall is equipment or software that sits between your payment system and the Internet. It acts as a barrier to keep traffic out of your network and systems that you don't want and didn't authorize. Firewalls are configured (in hardware, software, or both) with specific criteria to block or prevent unauthorized access to a network. Firewalls are often included in the router "box" provided by your Internet provider.

ISOLATE USAGE. Don't use the device or system you take payments with for anything else. For example, don't surf the web or check emails or social media from the same device or computer that you use for payment transactions. When necessary for business (for example, updating your business's social media page), use another computer and not your payment device for these updates.

PROTECT YOUR "VIRTUAL TERMINAL." If you enter customer payments via a virtual terminal (a web page you access with a computer or a tablet), minimize your risk - don't attach an external card reader to it.

PROTECT WI-FI. If your shop offers free Wi-Fi for your customers, make sure you use another network for your payment system (this is called "network segmentation"). Ask your network installer for help with safely configuring Wi-Fi.

USE A FIREWALL. A properly configured firewall acts as a buffer to keep hackers and malicious software from getting access to your payment systems, your e-commerce website, and/or your card data. Check with your payment terminal vendor or service provider to make sure you have one and ask them for help configuring it correctly.

USE PERSONAL FIREWALL SOFTWARE OR EQUIVALENT when payment systems are not protected by your business firewall (for example, when connected to public Wi-Fi).

For simple tips on configuring your firewall, see PCI Firewall Basics

For the best protection, make your data useless to criminals

Your data is vulnerable when it travels to your merchant bank, and when it's kept or stored on your computers and devices. The best way to keep it safe is to make it useless even if it's stolen by encrypting it whenever you store it or send it, and removing it altogether when it's not needed. While this can be more complex to put in place, in the long run, it can make security much easier to manage.

What is tokenization?
See page 14 for an explanation.

WORK WITH YOUR PAYMENT SYSTEMS VENDOR OR SERVICE PROVIDER. You should encrypt all card data you store or send. Make sure your payment system is using encryption and/or tokenization technology. If you are not sure, ask them.

USE PCI DEVICES THAT ENCRYPT CARD DATA. The PCI Council approves payment terminals that protect PIN data and payment terminals and "secure card readers" that additionally encrypt card data. See the List of PCI Approved PTS Devices.

USE SECURE PCI ENCRYPTION SOLUTIONS. Ask whether your payment terminal encryption is done via a Point-to-Point Encryption solution and is on the PCI Council's List of PCI P2PE Validated Solutions.

ARE YOU A MERCHANT NOW MOVING TO EMV CHIP TERMINALS? This is a great opportunity to make an investment in a terminal that supports EMV and also provides the added security of encryption and tokenization.

UPGRADE YOUR SOLUTION. Reduce your risk – consider getting a new payment terminal that uses both encryption and tokenization technology to remove the value of card data for hackers.

ASK. See Questions to ask your Vendors for help with questions to ask your vendor or service provider.

PCI-approved secure card readers and payment terminals that encrypt card data do it using technology called "Secure Reading and Exchange of Data (SRED)" - ask your vendor if your payment terminal encrypts card data with SRED.

E-commerce websites must encrypt card data that is sent over the Internet, for example, using something called transport-layer security (TLS). Ask your service provider how they encrypt your card data.

WHERE TO GET HELP

Resources

PCI Council Listings

Resource	URL
List of Validated Payment Applications	*https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement*
List of Approved PTS Devices	*https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices*
List of Approved Scanning Vendors	*https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors*
List of Qualified Integrators / Resellers	*https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers*
List of P2PE Validated Solutions	*https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions*

Payment Brand Lists

Resource		URL
Lists of Compliant Service Providers	MasterCard's List of Compliant Service Providers	*https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html*
	Visa's Global Registry of Service Providers	*http://www.visa.com/splisting/*
	Visa Europe's Registered Merchant Agents	*https://www.visaeurope.com/receiving-payments/security/downloads-and-resources*

PCI DSS and Related Guidance

Resource	URL
More about PCI DSS	*https://www.pcisecuritystandards.org/pci_security/how*
PCI DSS Self-Assessment Questionnaires	*https://www.pcisecuritystandards.org/pci_security/completing_self_assessment*
Guide: Skimming Prevention: Overview of Best Practices for Merchants	*https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf*

Resources

Infographics and Videos

Resource	URL
Infographic: It's Time to Change Your Password	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Video: Passwords	https://www.youtube.com/watch?v=dNVQk65KL8g
Infographic: Passwords	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf
Video: Patching	https://www.youtube.com/watch?v=0NGz1mGO3Jg
Infographic: Patching	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Patching.pdf
Video: Remote Access	https://www.youtube.com/watch?v=MxgSNFgvAVc
Infographic: Remote Access	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Secure-Remote-Access.pdf

PCI Data Security Essentials for Small Merchants and Related Guidance

Resource	URL
Common Payment Systems	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Small Merchant Questions for Vendors	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Small Merchant Glossary	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf
Infographic: PCI Firewall Basics	https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf
Evaluation Tool: Acquirer Overview	https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Acquirers.pdf
Evaluation Tool: Small Merchant Overview	https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf

Sources and Helpful References

Dept for Culture Media and Sport – *Cyber Security Breaches Survey 2023*

Ponemon Institute – *State of Cybersecurity in Small & Medium-Sized Businesses (SMB)* (Sponsored by Keeper Security), *March 2023*

National Cyber Security Centre – *Cyber Security Small Business Guide, 2020*

Verizon Data Breach Investigations Report - 2023

About the PCI Security Standards Council

The PCI Security Standards Council is a global forum for the industry to come together to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. Read more about PCI SSC's Global Payment Security Engagement Initiative at www.pcisecuritystandards.org/pdfs/PCI_SSC_Partnering_for_Global_Payment_Security.pdf

The Council maintains, evolves, and promotes the Payment Card Industry Security Standards. It also provides critical tools needed for implementation of the standards such as assessment and scanning qualific tions, self-assessment questionnaires, training and education, and product certific tion programs.

The Council's founding members, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., have agreed to incorporate the PCI Data Security Standard (PCI DSS) as part of the technical requirements for each of their data security compliance programs. Each founding member also recognizes the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI Security tandards Council.

All five payment b ands, along with Strategic Members, share equally in the Council's governance, have equal input into the PCI Security Standards Council and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the Council as Strategic or Affili te members and Participating Organizations to review proposed additions or modific tions to the standards. Participating Organizations may include merchants, banks, processors, hardware and software developers, and point-of-sale vendors.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

PCI SSC PARTICIPATING PAYMENT BRANDS

PARTICIPATING ORGANIZATIONS
Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors