PAYMENT SYSTEM TYPES

To protect your business against payment data theft, you first have to understand how you take payments in your store or shop. What kind of equipment do you use, who are your bank and technology vendor partners, and how do these things all fit together?

Use these real-life visuals to identify what type of payment system you use, the kinds of risks associated with your system, and the security steps you can take to protect it.
How do you use this resource?

IDENTIFY WHICH VISUAL MOST CLOSELY REPRESENTS YOUR PAYMENT SYSTEM:

- This guide, intended to supplement the Guide to Safe Payment, shows several common payment system diagrams, starting with the most simple up to very complex.
- Each payment system diagram includes four views:
  1) Overview
  2) Risks - where card data is exposed
  3) Threats - how criminals can get card data
  4) Protections - recommended ways to protect card data.
- Flip through to find the one you recognize as yours.

UNDERSTAND YOUR RISKS AND THREATS:

- Once you find the payment system views that most closely matches yours, review the next two diagrams to see where card data is at risk for your business, and the ways your business is vulnerable to attack.

PROTECT CARD DATA AND YOUR BUSINESS WITH SECURITY BASICS:

- Lastly, review the fourth view for your payment system type that includes basic security recommendations to help you protect your business.
- This view includes links to the recommendations in the areas in the Guide to Safe Payments to help you in this process.
- See also Questions to Ask Your Vendors and the Glossary of Payment and Information Security Terms.

COMPLETE THE DATA SECURITY ESSENTIALS EVALUATION IF SO INSTRUCTED BY YOUR ACQUIRER/BRAND

Optionally, for merchant information only, you can elect to use this resource or PCI SSC’s Data Security Essentials Evaluation Tool to gain insight about security practices relevant to how you accept payments. To use this resource, simply:

- Start at Payment system types at-a-glance
- Find the payment system diagram that most closely matches how you accept payments
- From that diagram, click on the Blue Box to download the relevant Evaluation Form
- Provide your responses
- Review your results
- Print out or save the resulting PDF for future use

Note that these are preliminary results. You cannot submit the evaluation 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.
What do these terms mean?

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 that 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.
Understanding your E-commerce Payment System

When you sell products or services online, you are classified as an 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.

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.
Payment system types at-a-glance

How do you accept payments?
Review all payment diagrams that apply to how your business accepts payments

- You accept payments with a standalone, dial-up payment terminal
  - TYPES 1, 2

- You accept payments with a payment device connected only to a processor
  - TYPES 3, 4

- You accept payments with a payment terminal connected to an electronic cash register or till, and the electronic cash register/till is connected only to a processor
  - TYPE 5

- You accept payments with a payment terminal that is connected to other systems (e.g., servers) in your network
  - TYPES 6, 7, 8

- You accept payments via e-commerce
  - TYPES 9, 10, 11

- You accept payments via a PCI-listed SCR (Secure Card Reader) attached to a mobile device
  - TYPES 12, 13

- You accept payments via a virtual terminal
  - TYPE 14

- You accept payments via a PCI-listed P2PE Solution
  - TYPE 15

Data Security Essentials for Small Merchants: Common Payment Systems
Copyright 2018 PCI Security Standards Council, LLC. All Rights Reserved.
Dial-up payment terminal. Payments sent via phone line.

For this scenario, risks to card data are present at 1 above. Risks explained on next page.
Dial-up payment terminal. Payments sent via phone line.

Where is your card data at risk?

Type 1

1. Overview
2. Risks
3. Threats
4. Protections

Lower

**Hardcopy card data, for example on paper receipts or reports**

**Electronic card data inside payment terminal**

DIAL-UP PAYMENT TERMINAL

PHONE LINE

BANK
How do criminals get your card data?

- They steal receipts or paper reports that you don’t secure, that you keep when you no longer need, or that you don’t dispose of securely.

- They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.

- They may also steal your terminal, replacing it with a modified one used to get your card data.
How do you start to protect card data today?*

- Protect card data and only keep what you need
- Inspect your payment terminals for damage or changes
- Ask your vendor partners for help if you need it
- Limit in-house access to your card data

*Dial-up payment terminal. Payments sent via phone line.

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.

Electronic cash register connected to the Internet, but no card payments taken here and no card data is entered on this machine.

Total sale amount is manually entered in the payment terminal.

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

Paper documents with card data

For this scenario, risks to card data are present at ⚠ above. Risks explained on next page.
Where is your card data at risk?

**Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.**

**PAYMENT TERMINAL**

**ELECTRONIC CASH REGISTER**

**Hardcopy card data, for example on paper receipts or reports**

Electronic card data inside payment terminal

INTERNET

ROUTER/FIREWALL

PHONE LINE

BANK
Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.

How do criminals get your card data?

- They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.
- They may also steal your terminal, replacing it with a modified one used to get your card data.
- They steal receipts or paper reports that you don’t secure, that you keep when you no longer need, or that you don’t dispose of securely.
Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.

How do you start to protect card data today?*

- Protect your card data and only keep what you need
- Inspect your payment terminals for damage or changes
- Ask your vendor partners for help if you need it
- Protect in-house access to your card data

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

Encrypting card data reduces your risk. If your payment terminal encrypts card data, ask your terminal vendor how (e.g. does it use PCI’s Secure Reading and Exchange of Data (SRED) to encrypt).

No other equipment connected to merchant payment systems

Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

Electronic cash register may be present. For example, where the total sale amount from electronic cash register is manually entered in payment terminal; no card payments are accepted on electronic cash register.

For this scenario, risks to card data are present at ⚠ above. Risks explained on next page.
Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

Where is your card data at risk?

Electronic card data inside payment terminal

Electronic card data in transit from payment terminal to processor

Hardcopy card data, for example on paper receipts or reports

Is card data encrypted?  

RISK PROFILE

Types of Threats

Types of Risks

Types of Protections

Yes  

No
How do criminals get your card data?

They steal card data via “skimming” equipment they attach to (or embed into) your payment terminal.

They steal your terminal, replacing it with a modified one used to get your card data.

They insert “malware” (software) onto a payment system that enables them to steal card data.

They steal receipts or paper reports that you don’t secure, that you keep when you no longer need, or that you don’t dispose of securely.
Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

**How do you start to protect card data today?**

- Use strong passwords
- Ask your vendor partners for help if you need it
- Use secure payment systems
- Protect card data and only keep what you need
- Protect in-house access to your card data
- Protect your business from the Internet
- Inspect your payment terminals for damage or changes
- Limit remote access for your vendor partners - don’t give hackers easy access
- Use anti-virus software
- Install patches from your payment terminal vendor
- Get regular vulnerability scanning
- Make your card data useless to criminals

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.*
Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

No other equipment connected to merchant payment systems, unless you have a separate PIN-entry device.

Payment terminal accepts card payments based on total sale amount received from electronic cash register. No card payments accepted on electronic cash register. No card data shared between electronic cash register and payment terminal.

Encrypting card data reduces your risk. If your payment terminal encrypts card data, ask your terminal vendor how (e.g. does it use PCI’s Secure Reading and Exchange of Data (SRED) to encrypt).

For this scenario, risks to card data are present at 1 above. Risks explained on next page.
Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.

Where is your card data at risk?

- Electronic card data in transit from payment terminal to processor
- Electronic card data inside payment terminal
- Hardcopy card data, for example on paper receipts or reports
- Full card data incorrectly sent to the electronic cash register
Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.

How do criminals get your card data?

- They steal card data via “skimming” equipment they attach to (or embed into) your payment terminal.
- They steal receipts or paper reports that you don’t secure, that you keep when you no longer need, or that you don’t dispose of securely.
- They steal card data incorrectly sent by payment terminal to electronic cash register due to incorrect integration between the devices. For example, for receipt printing, payment terminal should only send truncated card data to electronic cash register.
- They steal your terminal, replacing it with a modified one used to get your card data.
- They insert “malware”(software) onto a payment system that enables them to steal card data.
Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.

How do you start to protect card data today?*

- Use strong passwords
- Ask your vendor partners for help if you need it
- Use secure payment systems
- Protect card data and only keep what you need
- Protect in-house access to your card data
- Protect your business from the Internet
- Inspect your payment terminals for damage or changes
- Limit remote access for your vendor partners - don’t give hackers easy access
- Use anti-virus software
- Install patches from your payment terminal vendor
- Get regular vulnerability scanning
- Make your card data useless to criminals

*Click on the icons above for the Guide to Safe Payments and information about these security basics.

For simple definitions of payment and security terms, see our Glossary.
Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

Encrypting card data reduces your risk. If your payment terminal encrypts card data, ask your terminal vendor how (e.g. does it use PCI’s Secure Reading and Exchange of Data (SRED) to encrypt).

No other equipment connected to merchant payment systems

Electronic cash register does not accept cards but is used to send card data for processing.

Card data sent to electronic cash register

For this scenario, risks to card data are present at 🔴 above. Risks explained on next page.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.
Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

Where is your card data at risk?

- Electronic card data in transit
- Electronic card data inside electronic cash register
- Hardcopy card data, for example on paper receipts or reports

Is card data encrypted?

- [ ] NO
- [x] YES
How do criminals get your card data?

- They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.
- They steal card data via access to your electronic cash register, for example by installing malware (software) that enables this.
- They steal receipts or paper reports that you don’t secure, that you keep when you no longer need, or that you don’t dispose of securely.
- They may also steal your terminal, replacing it with a modified one used to get your card data.
Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

How do you start to protect card data today?*

- Use strong passwords
- Ask your vendor partners for help if you need it
- Use secure payment systems
- Protect card data and only keep what you need
- Protect in-house access to your card data
- Protect your business from the Internet
- Inspect your payment terminals for damage or changes
- Limit remote access for your vendor partners - don’t give hackers easy access
- Install patches from your payment terminal vendor
- Get regular vulnerability scanning
- Use anti-virus software
- Make your card data useless to criminals

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
Integrated payment terminal and payment middleware share card data. Payments sent via Internet.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

Payment terminal and electronic cash register combined
Card is swiped by a staff member; diagram is not applicable for chip cards
No separate PIN entry device
No other equipment connected to merchant payment system

Encrypting card data reduces your risk. If your payment terminal encrypts card data, ask your terminal vendor how (e.g. does it use PCI’s Secure Reading and Exchange of Data (SRED) to encrypt).

For this scenario, risks to card data are present at ! above. Risks explained on next page.
Integrated payment terminal and payment middleware share card data. Payments sent via Internet.

Where is your card data at risk?

- Electronic card data inside payment terminal or in the system with payment middleware
- Electronic card data in transit from payment terminal to processor
Integrated payment terminal and payment middleware share card data. Payments sent via Internet.

How do criminals get your card data?

They steal card data via “skimming” equipment they attach to (or embed into) your payment terminal.

They insert “malware” (software) onto a payment system that enables them to steal card data.

They access and steal your customer’s card data via the same “remote access” software your vendor uses to support your payment systems.

They steal your terminal, replacing it with a modified one used to get your card data.
Integrated payment terminal and payment middleware share card data. Payments sent via Internet.

How do you start to protect card data today?*

- Use strong passwords
- Protect card data and only keep what you need
- Inspect your payment terminals for damage or changes
- Install patches from your payment terminal vendor
- Protect in-house access to your card data
- Limit remote access for your vendor partners - don’t give hackers easy access
- Get regular vulnerability scanning
- Use secure payment systems
- Protect your business from the Internet
- Limit remote access for your vendor partners - don’t give hackers easy access
- Make your card data useless to criminals
- Use anti-virus software
- Get regular vulnerability scanning

*Click on the icons above for the Guide to Safe Payments and information about these security basics.

For simple definitions of payment and security terms, see our Glossary.
Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

Card data shared with terminal and middleware

No other equipment connected to merchant payment systems

Encrypting card data reduces your risk. If your payment terminal encrypts card data, ask your terminal vendor how (e.g. does it use PCI’s Secure Reading and Exchange of Data (SRED) to encrypt).

Payments are only taken via wireless payment terminal, in customer’s presence

For this scenario, risks to card data are present at 1 above. Risks explained on next page.
Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.

Where is your card data at risk?

- Electronic card data inside integrated payment terminal
- Electronic card data inside payment terminal
- Electronic card data in transit from payment terminal to processor

Is card data encrypted?

- Yes
- No
Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.

How do criminals get your card data?

- They insert "malware" (software) onto a payment system that enables them to steal card data.
- They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.
- They steal your terminal, replacing it with a modified one used to get your card data.
- They access and steal your card data via the same "remote access" software your vendor uses to support your payment systems.
- They insert "malware" (software) onto a payment system that enables them to steal card data.

RISK PROFILE

Is card data encrypted?

YES  NO
Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.

How do you start to protect card data today?*

- Use strong passwords
- Protect card data and only keep what you need
- Inspect your payment terminals for damage or changes
- Install patches from your payment terminal vendor
- Ask your vendor partners for help if you need it
- Protect in-house access to your card data
- Limit remote access for your vendor partners - don’t give hackers easy access
- Get regular vulnerability scanning
- Use secure payment systems
- Protect your business from the Internet
- Limit remote access for your vendor partners - don’t give hackers easy access
- Make your card data useless to criminals
- Use anti-virus software

*Click on the icons above for the Guide to Safe Payments and information about these security basics.

For simple definitions of payment and security terms, see our Glossary.
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

There are many risk points here due to the additional equipment in the same network as the payment terminal and also connected to the Internet. Each device and system has to be configured and managed securely to minimize risk.

For this scenario, risks to card data are present at above. Risks explained on next page.
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

Where is your card data at risk?

Electronic card data inside payment terminal or electronic cash register

Electronic card data in transit from payment terminal to processor

Is card data encrypted?

RISK PROFILE

TYPE 8 OVERVIEW

TYPE 8 RISKS

TYPE 8 THREATS

TYPE 8 PROTECTIONS
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

How do criminals get your card data?

- They insert "malware" (software) onto a payment system that enables them to steal card data.
- They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.
- They steal your terminal, replacing it with a modified one used to get your card data.
- They access and steal your card data via the same "remote access" software your vendor uses to support your payment system.
- They hack in through misconfigured or out-of-date software, or through insecure Wi-Fi devices.

Is card data encrypted? [NO]
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

How do you start to protect card data today?*

- Use strong passwords
- Ask your vendor partners for help if you need it
- Use secure payment systems
- Protect card data and only keep what you need
- Protect in-house access to your card data
- Protect your business from the Internet
- Inspect your payment terminals for damage or changes
- Limit remote access for your vendor partners - don’t give hackers easy access
- Use anti-virus software
- Install patches from your payment terminal vendor
- Get regular vulnerability scanning
- Make your card data useless to criminals

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.

EITHER: Merchant website implements URL redirection to send the customer browser to the third-party service provider's payment page. (as shown)

OR: Merchant website implements an Inline Frame (IFrame) to display the third-party service provider's payment form embedded within the merchant's web page. (not shown)

For this scenario, risks to card data are present at ! above. Risks explained on next page.
E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.

Where is your card data at risk?

Electronic card data (even though merchant doesn’t capture or store it) because of weaknesses on merchant website

Electronic card data at a third party (e-commerce hosting, service provider, shopping cart provider, etc.)

**KEY**
- Merchant responsibility
- Third-party service provider responsibility
How do criminals get your card data?

They steal card data by compromising your website due to vulnerabilities or poor security practices, and changing how your customer is sent to your third-party service provider (for example, by adding a false payment page).

They steal card data from service providers using a variety of methods (install malware, via misconfigured software, etc.).
How do you start to protect card data today?*

- Use strong passwords
- Protect card data and only keep what you need
- Ask your vendor partners for help if you need it
- Protect in-house access to your card data

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
E-commerce merchant fully or partially presents the payment page to customers. Payments sent from customer browser direct to PCI DSS compliant third-party service provider.

Either: Merchant website creates the entire payment page and uses the Direct Post Method to send card data (as shown).

Or: Merchant website creates the entire payment page and requests the customer browser to create the payment from JavaScript code executed from the third-party service provider (not shown).

In both cases, card data is sent direct from the customer browser to the third-party service provider.

For this scenario, risks to card data are present at ![image](image-url) above. Risks explained on next page.
E-commerce merchant fully or partially presents the payment page to customers. Payments sent from customer browser direct to PCI DSS compliant third-party service provider.

Where is your card data at risk?

Electronic card data because of weaknesses on merchant website (even though merchant doesn’t capture or store it)

KEY
- Merchant responsibility
- Third-party service provider responsibility
E-commerce merchant fully or partially presents the payment page to customers. Payments sent from customer browser direct to PCI DSS compliant third-party service provider.

**How do criminals get your card data?**

They steal card data by compromising your website due to vulnerabilities or poor security practices, and changing your payment page to transparently take copies of your customers’ card data as sales go through.

They steal data by compromising your web application to change your checkout process or payment pages.

They steal card data from outsourced providers using a variety of methods (install malware, via misconfigured software, etc.).

**KEY**
- Merchant responsibility
- Third-party service provider responsibility

**Diagram Elements**
- Merchant
- E-commerce web site
- PCI DSS compliant third-party service provider
- Merchant router/firewall
- Merchant shopping pages
- Internet
- Merchant payment page
- Bank
How do you start to protect card data today?*

- Use strong passwords
- Protect in-house access to your card data
- Use secure payment systems
- Protect card data and only keep what you need
- Limit remote access for your vendor partners - don’t give hackers easy access
- Protect your business from the Internet
- Install patches from your payment terminal vendor
- Use anti-virus software
- Ask your vendor partners for help if you need it
- Get regular vulnerability scanning
- Make your card data useless to criminals

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
E-commerce merchant accepts card data using payment page presented to customers from own website. Payments sent via the merchant website.

For this scenario, risks to card data are present at ! above. Risks explained on next page.
E-commerce merchant accepts card data using payment page presented to customers from own website. Payments sent via the merchant website.

Where is your card data at risk?

- Electronic card data because of weaknesses in your website server or infrastructure.
- Electronic card data because of weaknesses in your web applications.
- Electronic card data at a third party (e-commerce hosting, payment gateway, shopping cart provider, etc.)

**Diagram Notes:**
- **MERCHANT E-COMMERCE WEB SITE**
- **MERCHANT ROUTER / FIREWALL**
- **INTERNET**
- **MERCHANT SHOPPING PAGES**
- **CHECKOUT**
- **MERCHANT PAYMENT PAGE**
- **PAY NOW**

**KEY:** Merchant responsibility
How do criminals get your card data?

They steal card data by compromising your website due to vulnerabilities or poor security practices. For example, SQL injection is a common technique used to steal data from websites.

They steal data by compromising your web application to change your checkout process or payment pages.

They steal card data from outsourced providers using a variety of methods (install malware, via misconfigured software, etc.).

*KEY*
- Merchant responsibility
**How do you start to protect card data today?**

- Use strong passwords
- Protect in-house access to your card data
- Use secure payment systems
- Protect card data and only keep what you need
- Limit remote access for your vendor partners - don’t give hackers easy access
- Protect your business from the Internet
- Install patches from your payment terminal vendor
- Use anti-virus software
- Make your card data useless to criminals
- Ask your vendor partners for help if you need it
- Get regular vulnerability scanning

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

Mobile payment terminal only connects to the Internet over the cellular network and does not use Wi-Fi.

For merchants when at non-fixed locations (flea market, trade show, etc.)

Secure card reader is listed on the PCI SSC website as an approved SCR. Ask your vendor or check here to confirm (select SCR under “device type”): PCI-listed PTS Devices.

Card data and PIN are encrypted in the secure card reader and PIN entry device before sending to phone/tablet; phone/tablet only has access to encrypted card data.

Merchant has no ability to manually enter card data.

Merchant verifies that mobile payment terminal has not been tampered with in any way, and that applications can only be downloaded from vendor application stores.

For this scenario, risks to card data are present at 1 above. Risks explained on next page.
Where is your card data at risk?

Electronic card data if entered directly into the mobile phone or tablet

Electronic PIN data if entered directly into the mobile phone or tablet

PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.
How do criminals get your card data?

- They hack into phone/tablet and insert “malware” (software) that enables them to bypass the secure card reader and steal card data or PIN data on mobile phones/tablets.
- They use applications in “app store” that enable them to bypass the secure card reader and steal card data or PIN data when you download that app onto your phone/tablet.
- They steal card data by swapping out the secure card reader for one they have modified to include a skimmer.
How do you start to protect card data today?*

- Inspect your secure card readers and PIN entry devices for damage or changes.
- Use a secure card reader and PIN entry device.
- Limit remote access for your vendor partners - don’t give hackers easy access.
- Install patches from your vendors.
- Make your card data useless to criminals.
- Ask your vendor partners for help if you need it.
- Protect card data and only keep what you need.
- Protect in-house access to your card data.

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.

If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

Connects to Internet over the cellular network and/or Wi-Fi.

For merchants when at non-fixed locations (flea market, trade show, etc.)

Secure card reader is listed on the PCI SSC website as an approved SCR. Ask your vendor or check here to confirm (select SCR under “device type”): PCI-listed PTS Devices.

Card data and PIN are encrypted in the secure card reader and PIN entry device before sending to phone/tablet; phone/tablet only has access to encrypted card data

Merchant has no ability to manually enter card data

Merchant verifies that mobile payment terminal has not been tampered with in any way, and that applications can only be downloaded from vendor application stores.

For this scenario, risks to card data are present at ⚠ above. Risks explained on next page.
PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.

Where is your card data at risk?

- Electronic card data if entered directly into the mobile phone or tablet
- Electronic PIN data if entered directly into the mobile phone or tablet

PIN ENTRY DEVICE

SECURE CARD READER (PAYMENT TERMINAL)

WIFI OR CELLULAR NETWORK

Electronic card data if entered directly into the mobile phone or tablet
How do criminals get your card data?

- They hack into phone/tablet and insert “malware”(software) that enables them to bypass the secure card reader and steal card data or PIN data on mobile phones/tablets.
- They use applications in “app store” that enable them to bypass the secure card reader and steal card or PIN data when you download that app onto your phone/tablet.
- They steal card data by swapping out the secure card reader for one they have modified to include a skimmer.
- They access merchant’s phone/tablet through insecure public Wi-Fi (no firewall and/or unknown security) to bypass the secure card reader and steal card or PIN data.
PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.

How do you start to protect card data today?*

- Protect in-house access to your card data
- Protect your business from the Internet
- Inspect your secure card readers and PIN entry devices for damage or changes
- Limit remote access for your vendor partners - don’t give hackers easy access
- Install patches from your payment terminal vendor
- Make your card data useless to criminals
- Ask your vendor partners for help if you need it
- Use a secure card reader and PIN entry device

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

A “virtual terminal” is a web page accessed by the merchant, for example, with a computer or a tablet.

Merchant manually enters card data via their web browser into the virtual terminal.

For merchants without a traditional payment terminal. They manually enter transactions one at a time and usually have low payment transaction volume (for example, those doing sales from home).

Note that there is greater risk if mobile payment acceptance is done over unprotected public Wi-Fi since criminals can steal your card data via that unsecured network.

For this scenario, risks to card data are present at ![above. Risks explained on next page.](image)

Virtual terminal from PCI DSS compliant payment processor.

For merchants with a traditional payment terminal, the risks are lower since the payment system is designed to securely handle card data. The diagram illustrates the flow of payments through the virtual terminal, with potential risks at various stages: merchant device, virtual terminal service, and network. The evaluation form is available for download to help merchants understand how they can better protect their business.
Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

Where is your card data at risk?

- Electronic card data on PC or mobile phones/tablets used to access virtual payment terminal website

**TYPE 14 OVERVIEW**

**TYPE 14 RISKS**

**TYPE 14 THREATS**

**TYPE 14 PROTECTIONS**

VIRTUAL TERMINAL FROM PCI DSS COMPLIANT PAYMENT PROCESSOR

MERCHAND PC

MERCHAND PHONE/TABLET

INTERNET

ROUTER/FIREWALL
How do criminals get your card data?

- They access your phone/tablet through insecure public Wi-Fi (no firewall and/or unknown security) to steal card or PIN data.
- They hack into PC or mobile phone/tablet and insert “malware” (software) that enables them to steal card data as it’s entered into virtual terminal.
Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

How do you start to protect card data today?*

- Use strong passwords
- Install patches from your payment terminal vendor
- Ask your vendor partners for help if you need it
- Limit remote access for your vendor partners - don’t give hackers easy access
- Use anti-virus software
- Get regular vulnerability scanning
- Use a firewall (or personal firewall software if using public Wi-Fi)

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

The solution is included on PCI’s List of P2PE Validated Solutions (hint: look in the solution provider’s P2PE Instruction Manual for the solution name).

Merchant implements P2PE according to the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

All storage, processing or transmission of card data for this channel is within the PCI-approved payment terminal.

For this scenario, risks to card data are present at above. Risks explained on next page.
Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

Where is your card data at risk?

Paper-based payment data (written down/received from mail order/telephone orders, paper receipts, forms, etc.) not properly protected and/or disposed of.

Electronic card data because someone comes into your shop and replaces your terminal.

Electronic card data if payment terminal is installed incorrectly because you did not follow instructions in the PIM.
Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

How do criminals get your card data?

- They steal card data recorded on paper (written down/received from mail order/telephone orders, paper receipts, forms, etc.)
- They steal your terminal, replacing it with a modified one that they use to get your card data.
- They steal card data via weaknesses present because you didn’t follow the P2PE Instruction Manual

**P2PE INSTRUCTION MANUAL (PIM) FROM P2PE SOLUTION PROVIDER**

**PAYMENT TERMINAL PROVIDED BY PCI-LISTED P2PE SOLUTION PROVIDER**

**PIN ENTRY DEVICE AND/OR SECURE CARD READERS PROVIDED BY PCI-LISTED P2PE SOLUTION PROVIDER**

**MERCHAND RESPONSIBILITY**

**Encrypted Account Data**

**Encrypted Account Data**

**MOBILE PHONE OR TABLET**

**P2PE SOLUTION PROVIDER LISTED ON PCI SSC’S WEBSITE**
Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

How do you start to protect card data today?*

- Protect card data and only keep what you need
- Inspect your payment terminals for damage or changes
- Ask your vendor partners for help if you need it
- Protect in-house access to your card data
- Make your card data useless to criminals

*Click on the icons above for the Guide to Safe Payments and information about these security basics. For simple definitions of payment and security terms, see our Glossary.
### Resources

#### Infographics and Videos

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infographic: It’s Time to Change Your Password</td>
<td><a href="https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf">https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf</a></td>
<td></td>
</tr>
<tr>
<td>Video: Learn Password Security in 2 Minutes</td>
<td><a href="https://www.youtube.com/watch?v=FsrOXgZKa7U">https://www.youtube.com/watch?v=FsrOXgZKa7U</a></td>
<td></td>
</tr>
<tr>
<td>Video: Passwords</td>
<td><a href="https://www.youtube.com/watch?v=dNVQkJ65KL8g">https://www.youtube.com/watch?v=dNVQkJ65KL8g</a></td>
<td></td>
</tr>
<tr>
<td>Video: Patching</td>
<td><a href="https://www.youtube.com/watch?v=0NGz1mGO3Jg">https://www.youtube.com/watch?v=0NGz1mGO3Jg</a></td>
<td></td>
</tr>
<tr>
<td>Video: Remote Access</td>
<td><a href="https://www.youtube.com/watch?v=MxqSNFqvAVc">https://www.youtube.com/watch?v=MxqSNFqvAVc</a></td>
<td></td>
</tr>
</tbody>
</table>

#### PCI Data Security Essentials for Small Merchants and Related Guidance

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>URL</th>
</tr>
</thead>
</table>