

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

# Common Payment Systems

Version 2.0 | August 2018



# Payment System Types and How to Secure Them



## 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 a e-commerce merchant. Here are some common terms you may see or hear and what they mean.



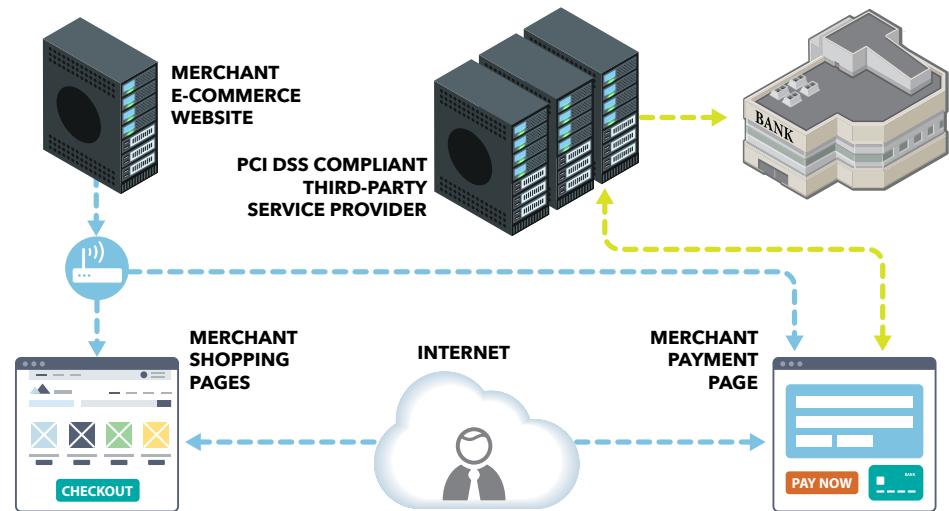
An **E-COMMERCE WEBSITE** houses and presents your business website and shopping pages to your customers. The website may be hosted and managed by you or by a third party hosting provider.



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.



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



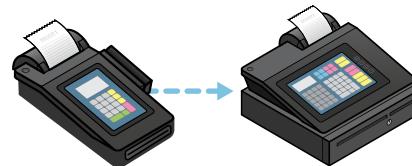
You accept payments with a standalone, dial-up payment terminal

**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**



LOWER

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

## TYPE 1 OVERVIEW

## TYPE 1 RISKS

## TYPE 1 THREATS

## TYPE 1 PROTECTIONS

**YES**

This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**

I'm not positive this is my payment system. Show me the overview again

### DIAL-UP PAYMENT TERMINAL

Dial-up payment terminal shows it is dialing for each transaction



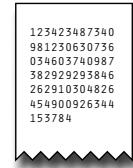
The payment terminal is connected to bank by a dial-up telephone line



PHONE LINE



Paper documents with card data



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



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

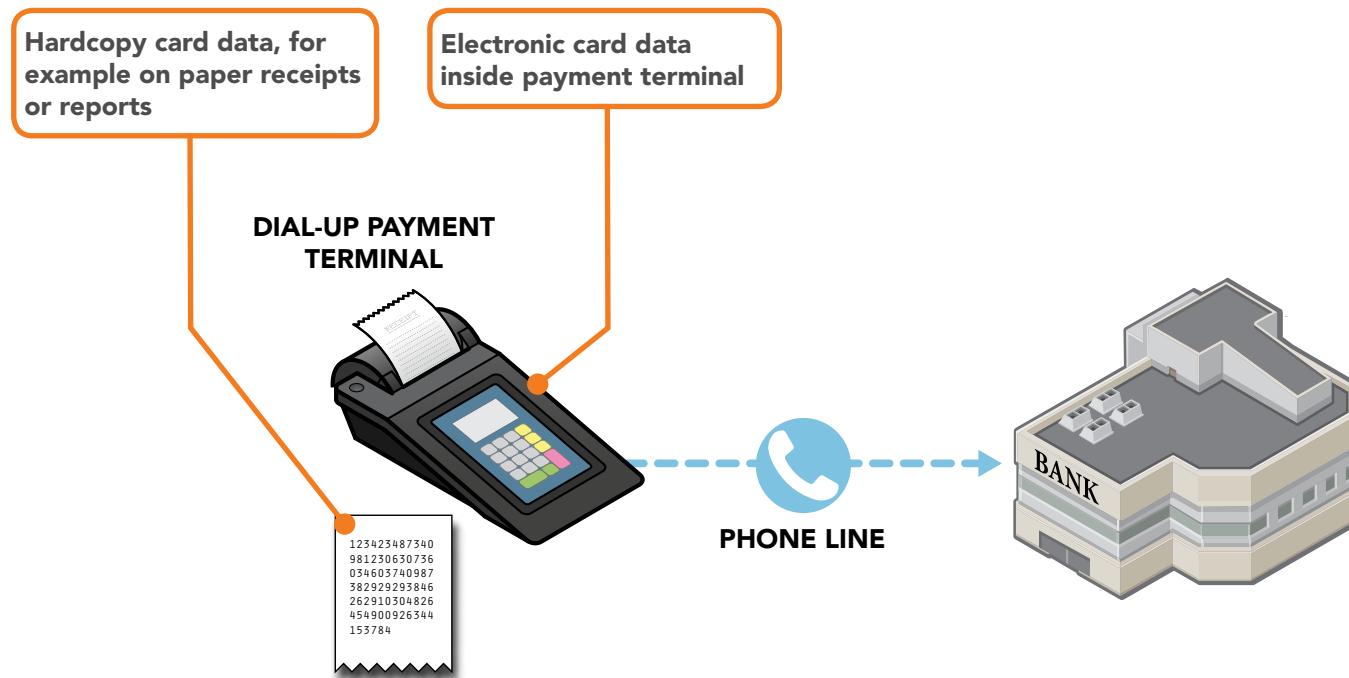
TYPE 1 OVERVIEW

TYPE 1 RISKS

TYPE 1 THREATS

TYPE 1 PROTECTIONS

## Where is your card data at risk?





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

TYPE 1 OVERVIEW

TYPE 1 RISKS

TYPE 1 THREATS

TYPE 1 PROTECTIONS

## 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.

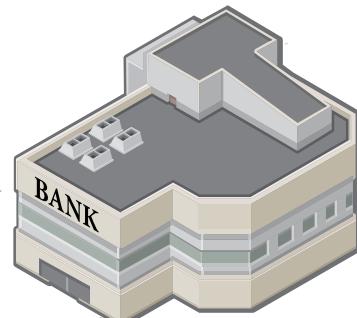
They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.

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

DIAL-UP PAYMENT TERMINAL



PHONE LINE





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

TYPE 1 OVERVIEW

TYPE 1 RISKS

TYPE 1 THREATS

TYPE 1 PROTECTIONS

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



Protect card data and only keep what you need



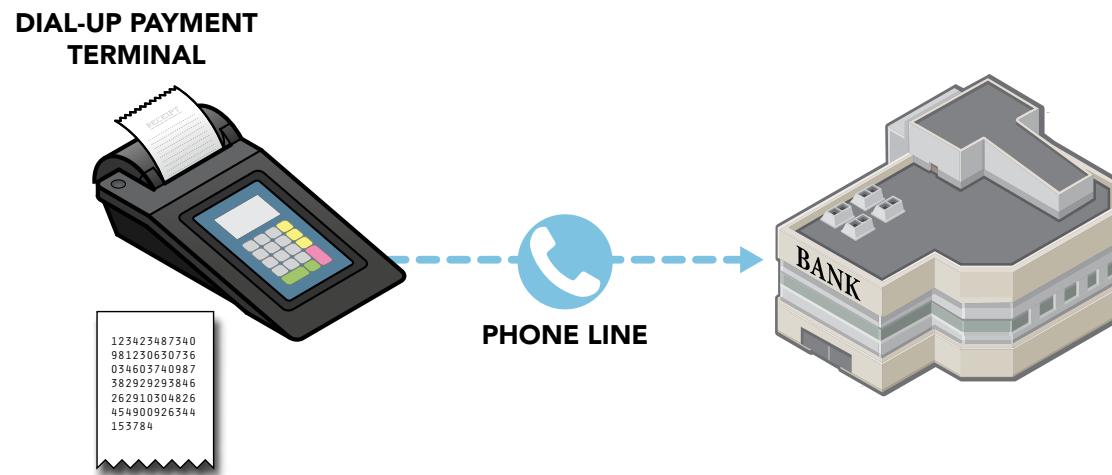
Inspect your payment terminals for damage or changes



Ask your vendor partners for help if you need it



Limit in-house access to your card data



\*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.



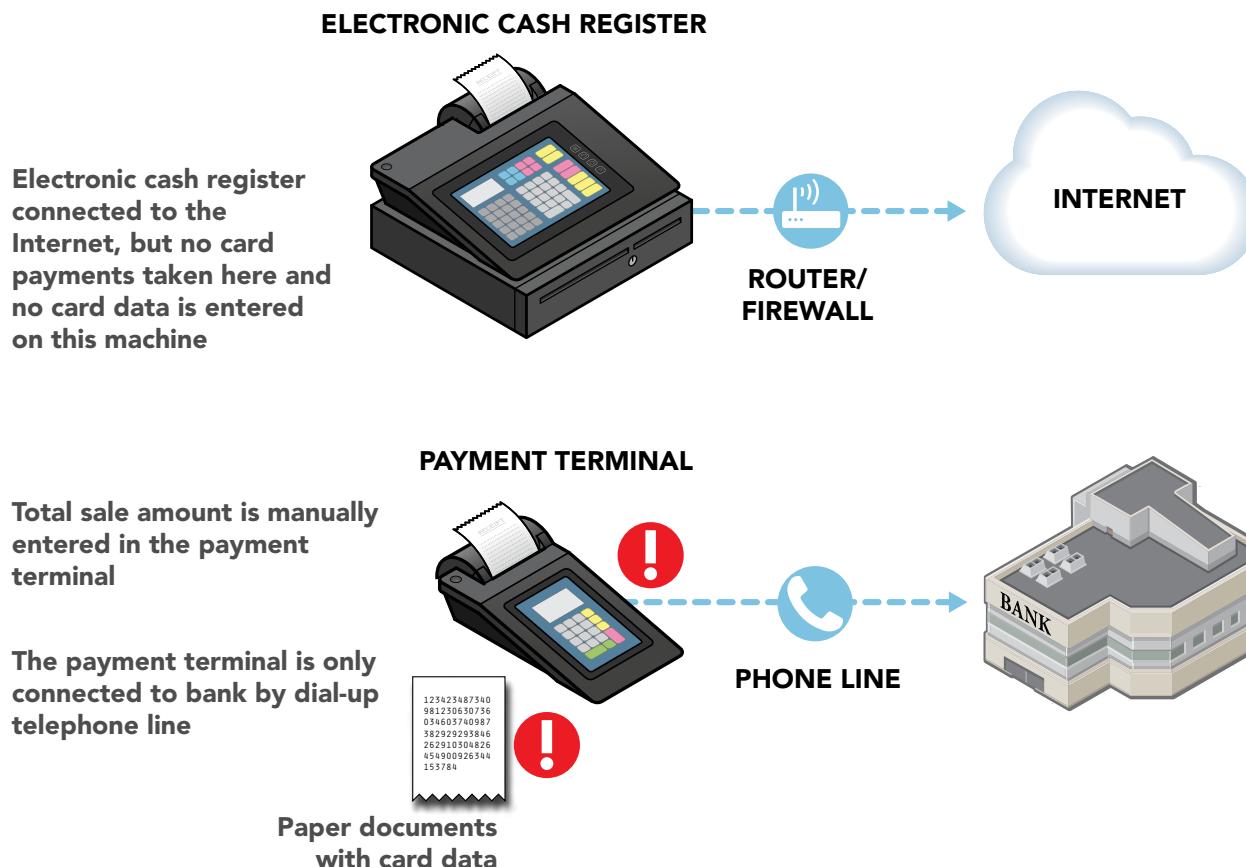
LOWER

## TYPE 2 OVERVIEW

## TYPE 2 RISKS

## TYPE 2 THREATS

## TYPE 2 PROTECTIONS



**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

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

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



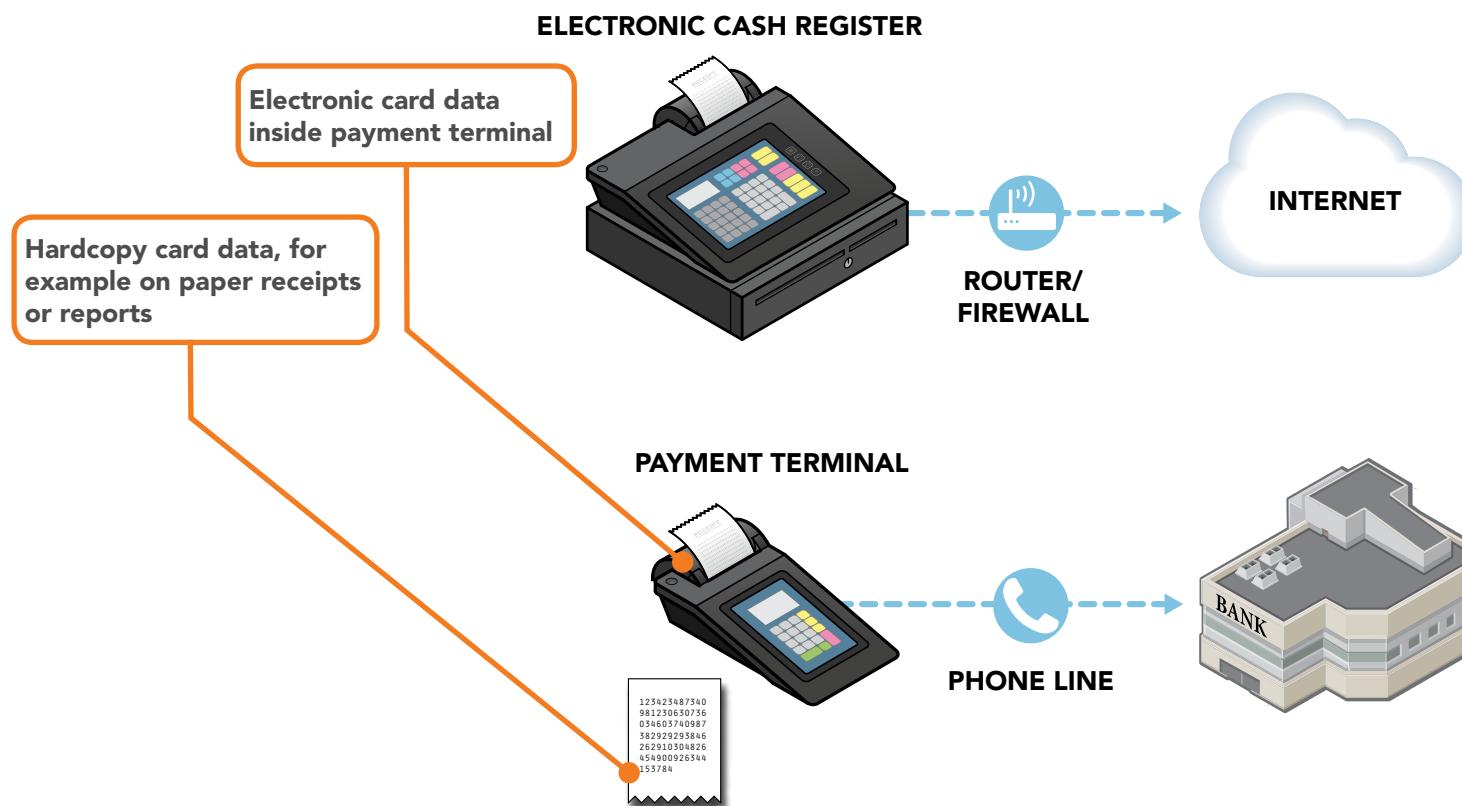
TYPE 2 OVERVIEW

TYPE 2 RISKS

TYPE 2 THREATS

TYPE 2 PROTECTIONS

## Where is your card data at risk?



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



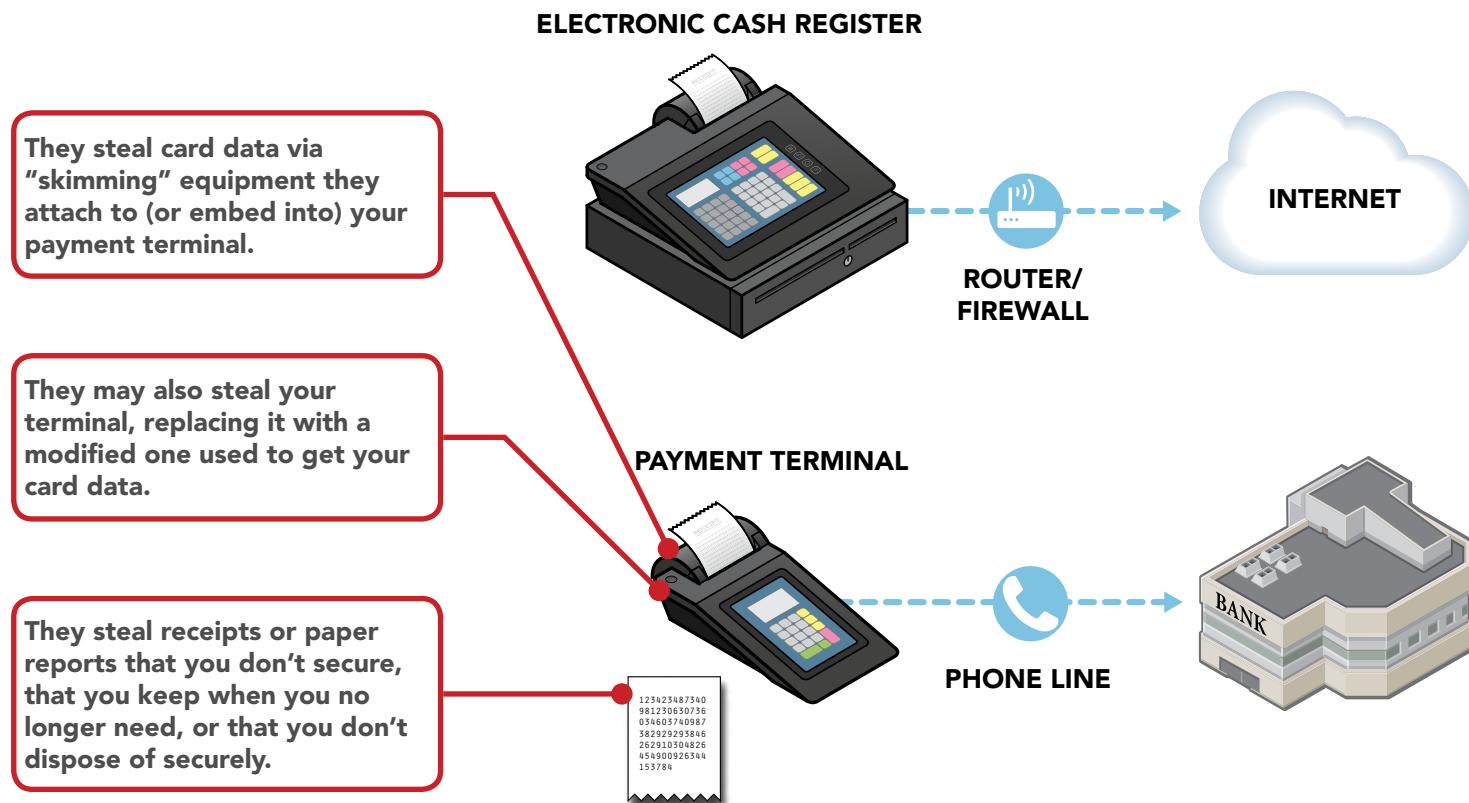
TYPE 2 OVERVIEW

TYPE 2 RISKS

TYPE 2 THREATS

TYPE 2 PROTECTIONS

## How do criminals get your card data?



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



TYPE 2 OVERVIEW

TYPE 2 RISKS

TYPE 2 THREATS

TYPE 2 PROTECTIONS

## 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

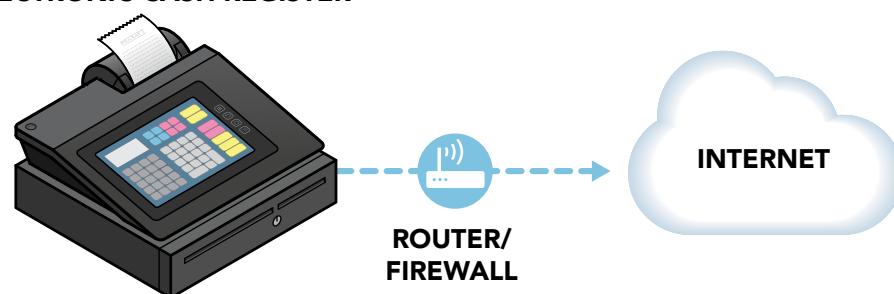


Ask your vendor partners for help if you need it

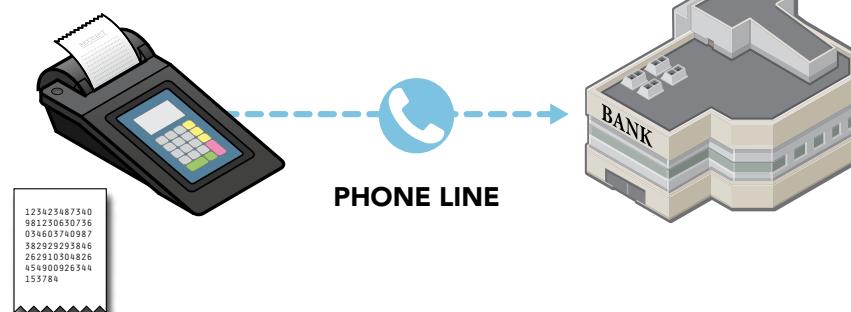


Protect in-house access to your card data

### ELECTRONIC CASH REGISTER



### PAYMENT TERMINAL



\*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](#).

# TYPE 3

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



## TYPE 3 OVERVIEW

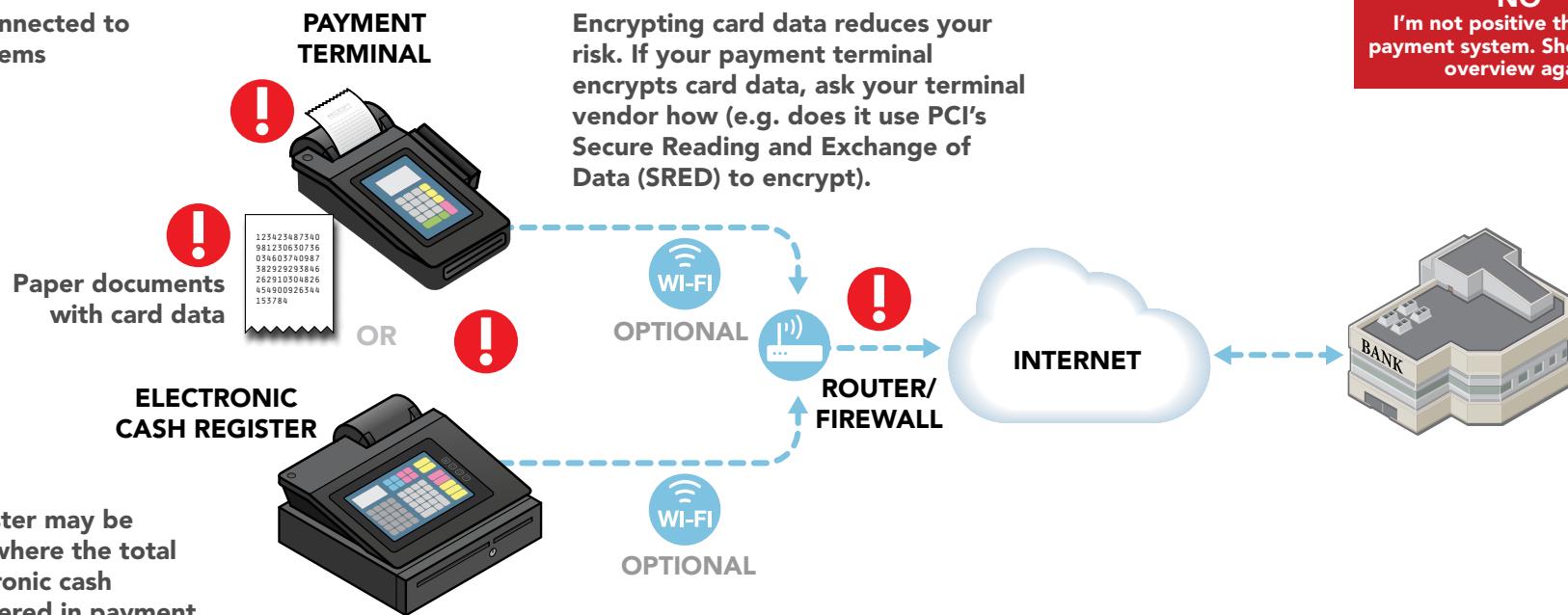
## TYPE 3 RISKS

## TYPE 3 THREATS

## TYPE 3 PROTECTIONS

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



**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

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.



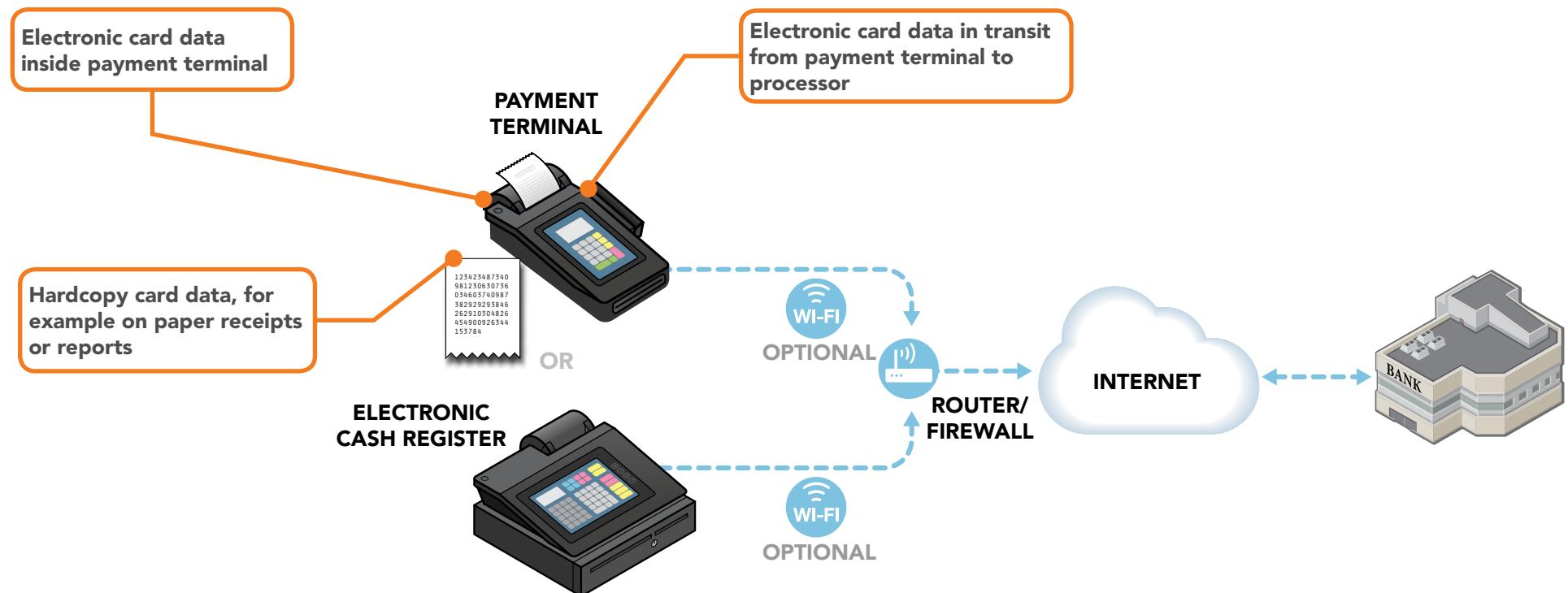
TYPE 3 OVERVIEW

TYPE 3 RISKS

TYPE 3 THREATS

TYPE 3 PROTECTIONS

## Where is your card data at risk?



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



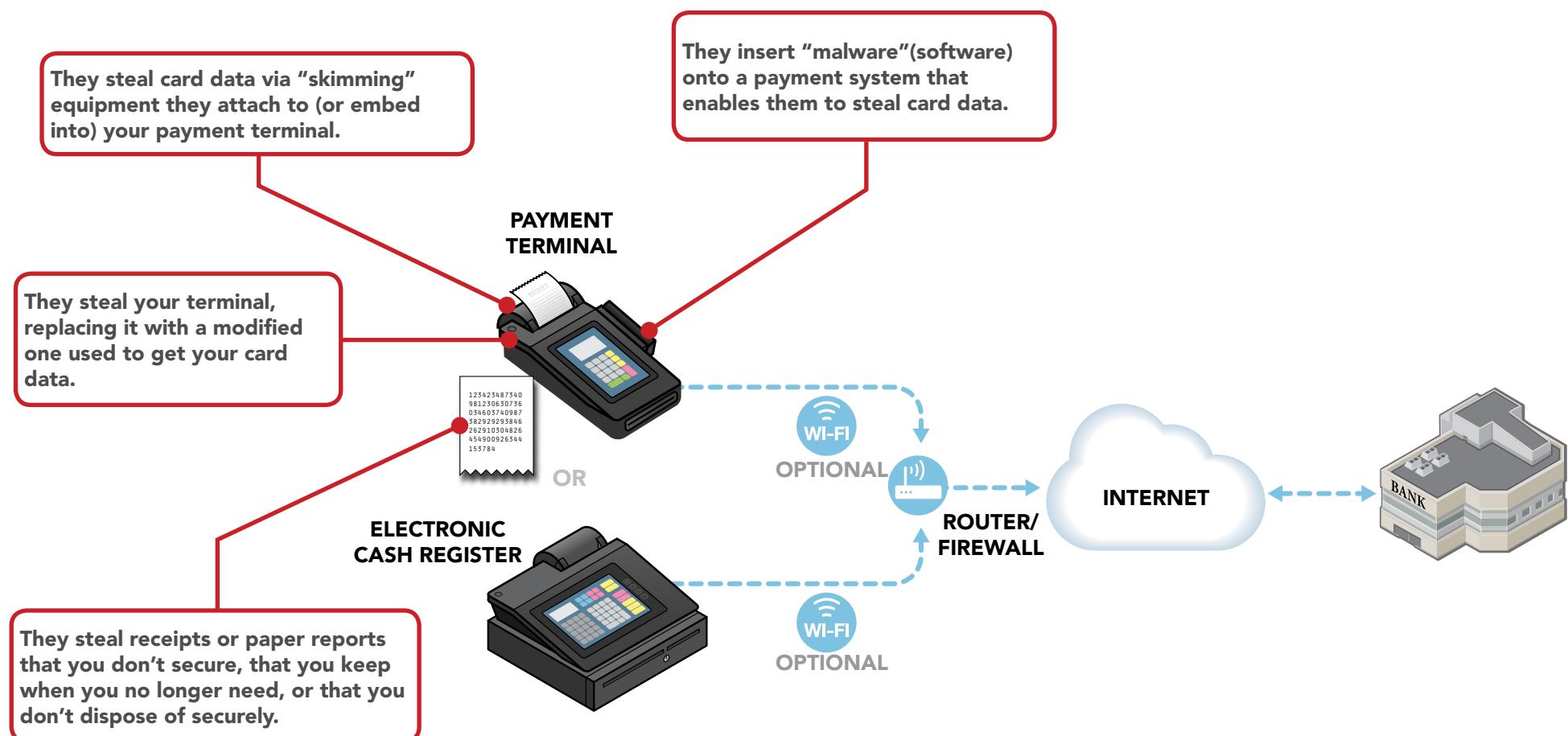
TYPE 3 OVERVIEW

TYPE 3 RISKS

TYPE 3 THREATS

TYPE 3 PROTECTIONS

## How do criminals get your card data?



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



TYPE 3 OVERVIEW

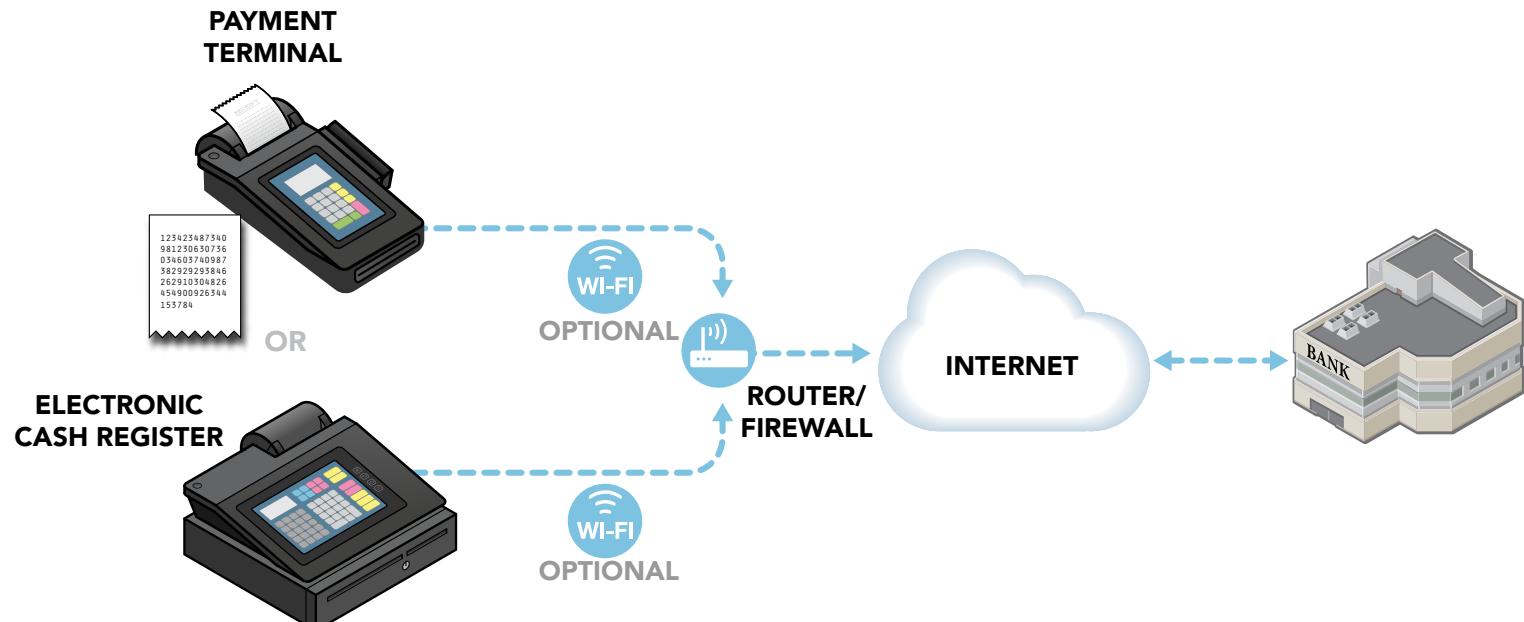
TYPE 3 RISKS

TYPE 3 THREATS

TYPE 3 PROTECTIONS

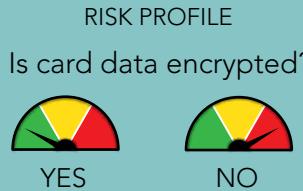
## How do you start to protect card data today?\*

- |   |   |   |   |
|---|---|---|---|
|  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       |  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](#).

# Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.



## TYPE 4 OVERVIEW

## TYPE 4 RISKS

## TYPE 4 THREATS

## TYPE 4 PROTECTIONS

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

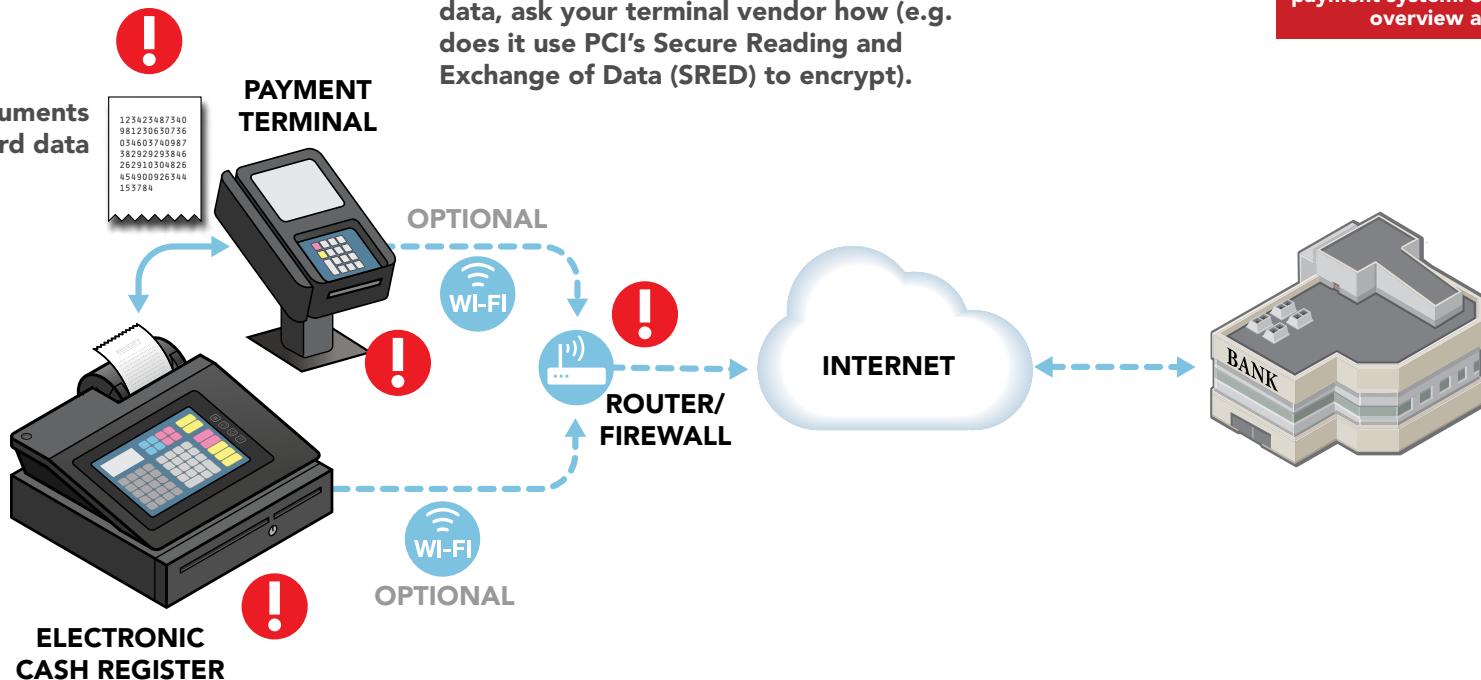
Paper documents with card data

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).

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



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

# Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.

TYPE 4 OVERVIEW

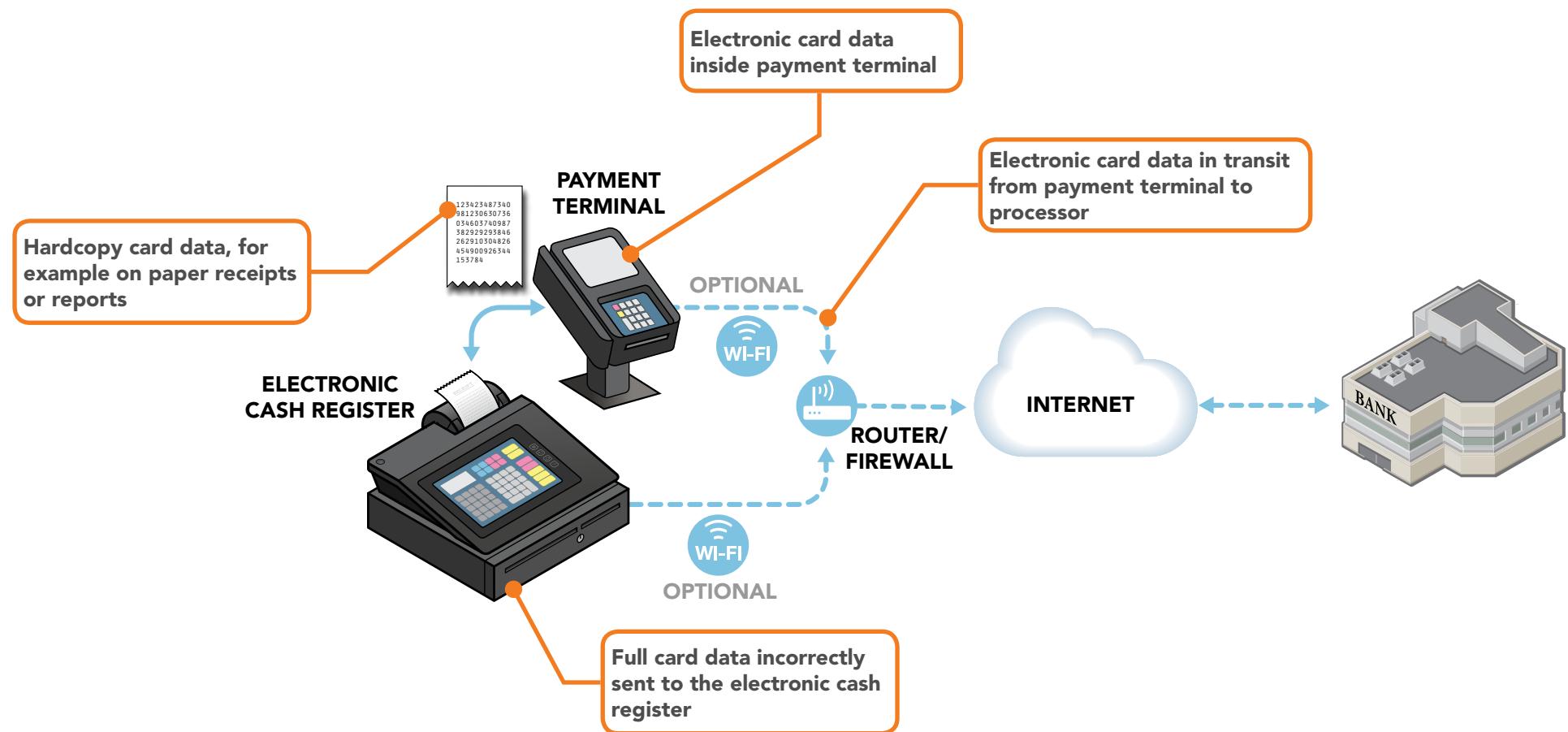
TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 PROTECTIONS



## Where is your card data at risk?



# Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.



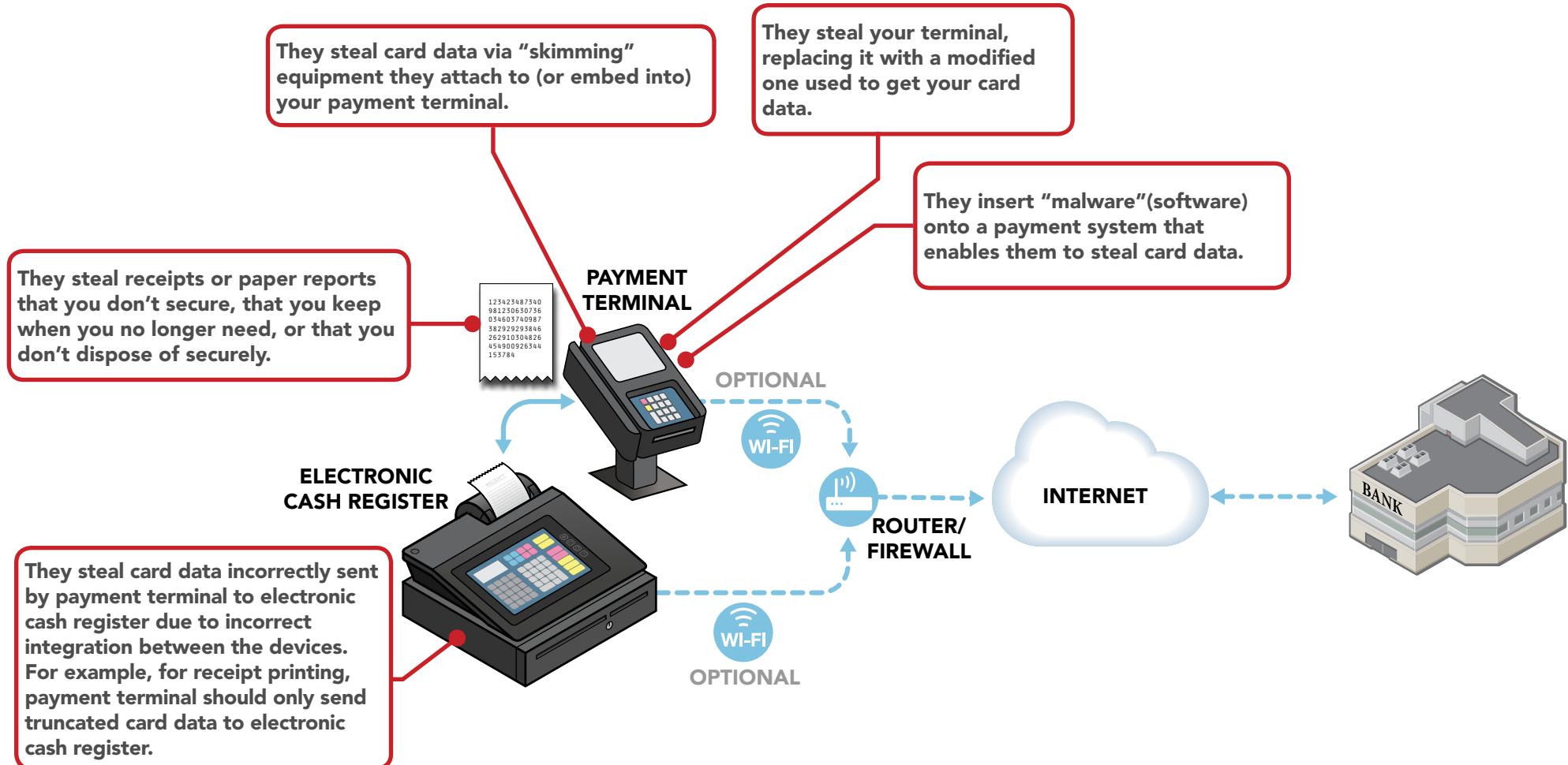
TYPE 4 OVERVIEW

TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 PROTECTIONS

## How do criminals get your card data?



# Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.



TYPE 4 OVERVIEW

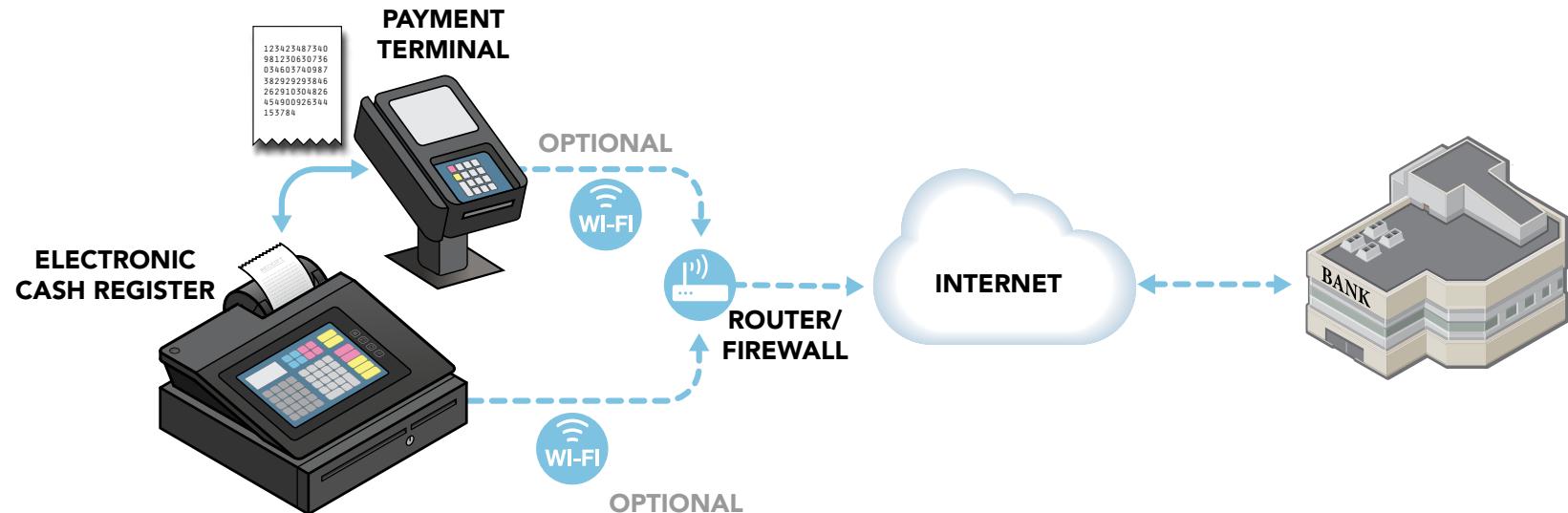
TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 PROTECTIONS

## 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       |  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](#).

# Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.



## TYPE 5 OVERVIEW

## TYPE 5 RISKS

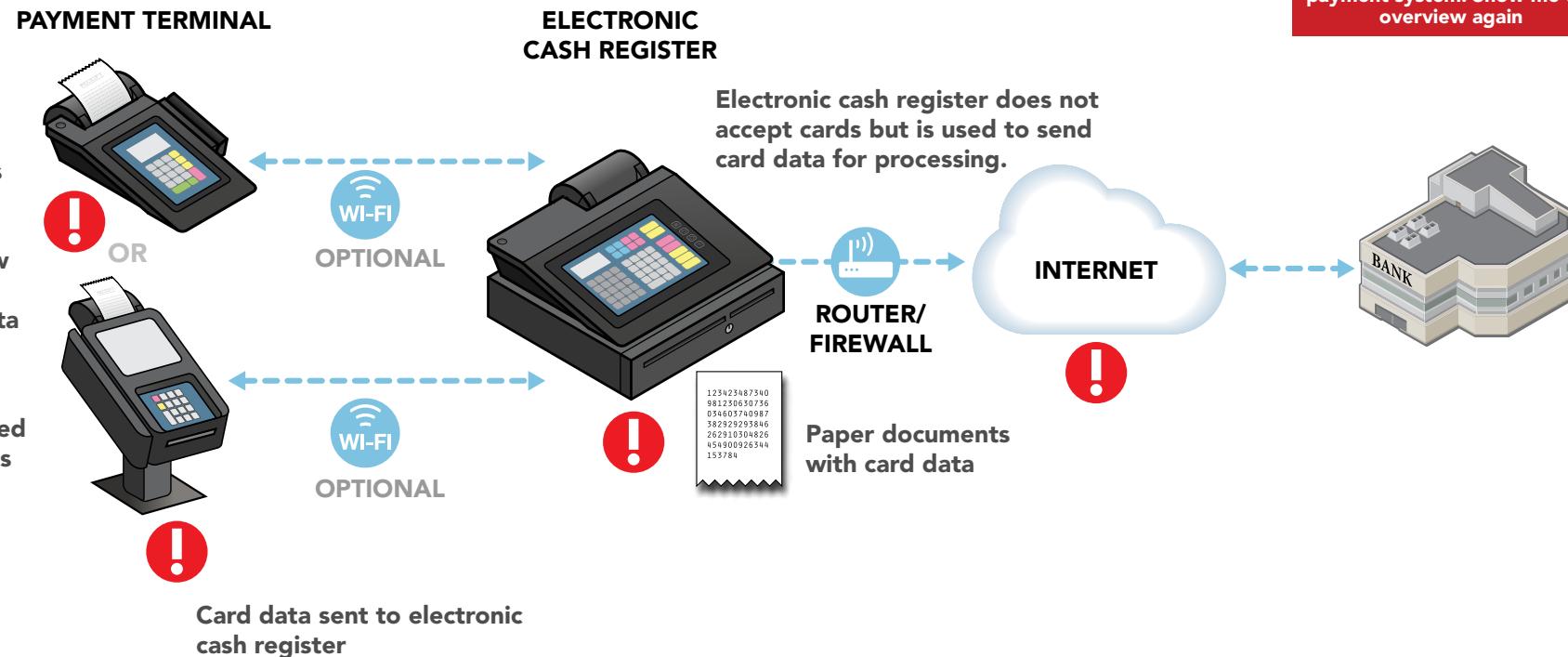
## TYPE 5 THREATS

## TYPE 5 PROTECTIONS

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

**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again



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

# Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.



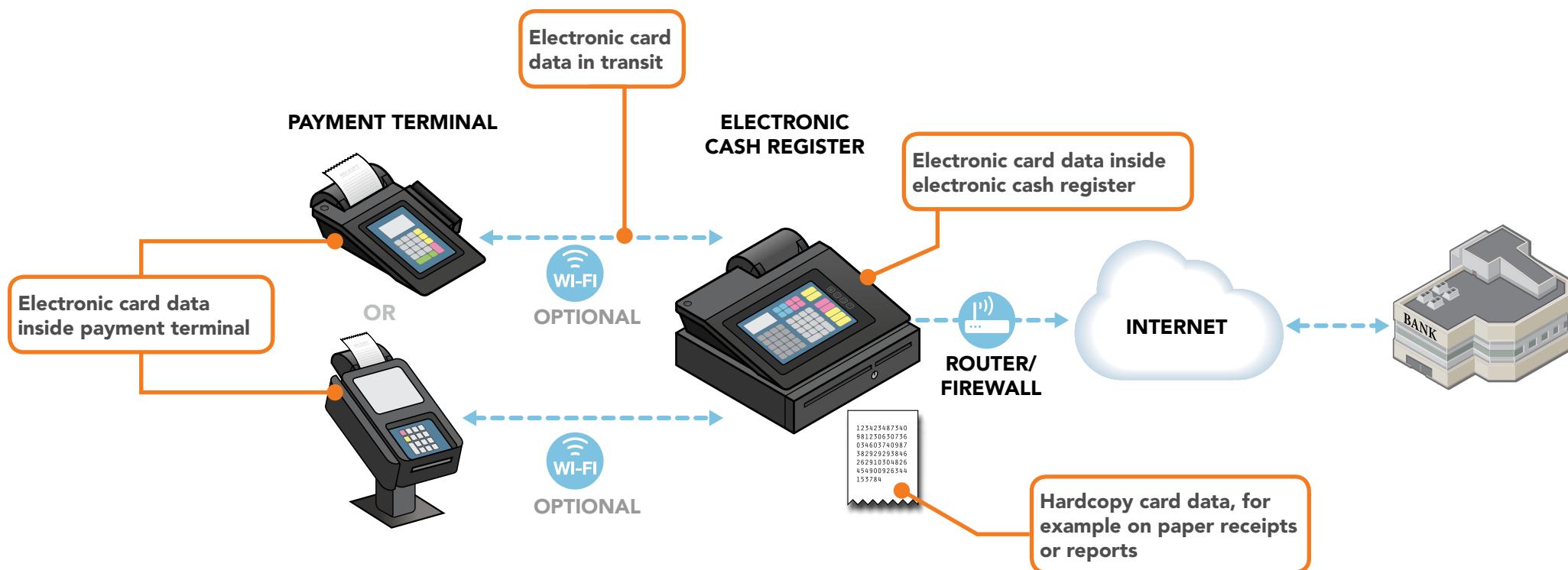
TYPE 5 OVERVIEW

TYPE 5 RISKS

TYPE 5 THREATS

TYPE 5 PROTECTIONS

## Where is your card data at risk?



# Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.



TYPE 5 OVERVIEW

TYPE 5 RISKS

TYPE 5 THREATS

TYPE 5 PROTECTIONS

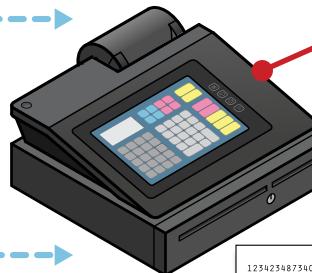
## How do criminals get your card data?

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

PAYMENT TERMINAL



ELECTRONIC CASH REGISTER

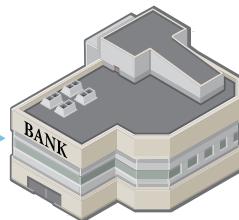


WI-FI  
OPTIONAL

WI-FI  
OPTIONAL

They steal card data via access to your electronic cash register, for example by installing malware (software) that enables this.

INTERNET

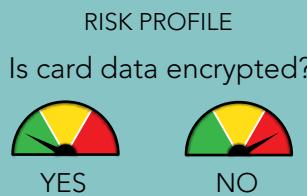


ROUTER/FIREWALL

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.

# Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.



## TYPE 5 OVERVIEW

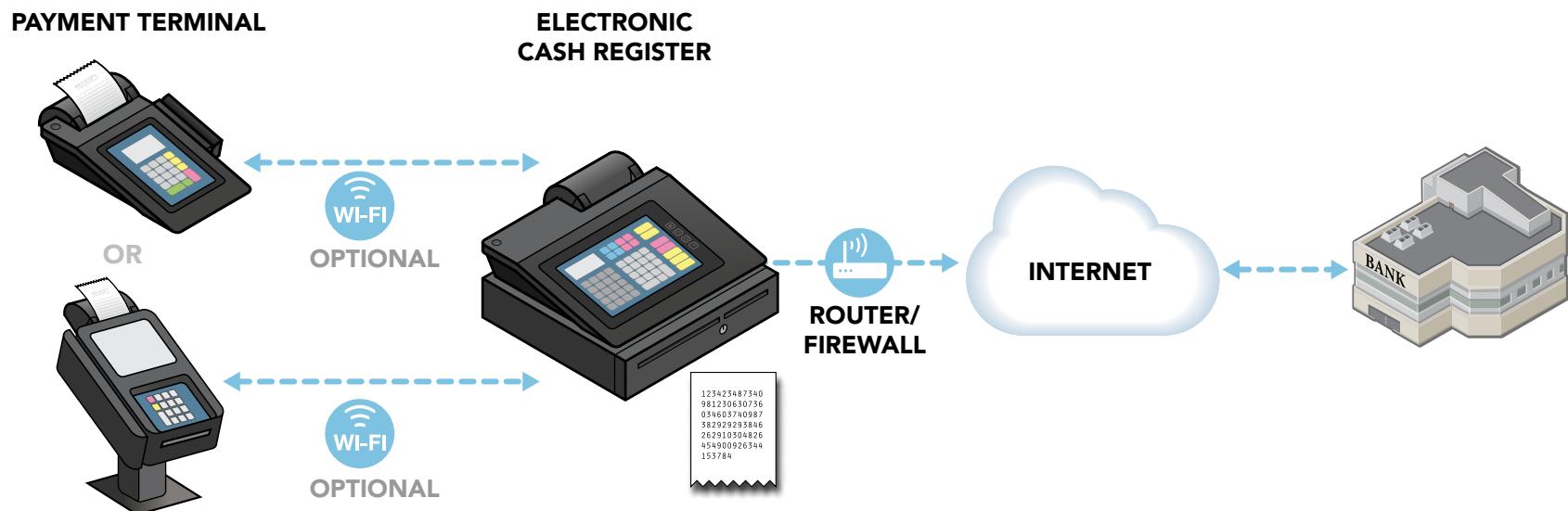
## TYPE 5 RISKS

## TYPE 5 THREATS

## TYPE 5 PROTECTIONS

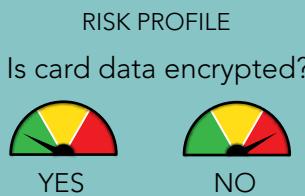
## How do you start to protect card data today?\*

- |   |   |   |   |
|---|---|---|---|
|  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       |  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.



## TYPE 6 OVERVIEW

## TYPE 6 RISKS

## TYPE 6 THREATS

## TYPE 6 PROTECTIONS

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

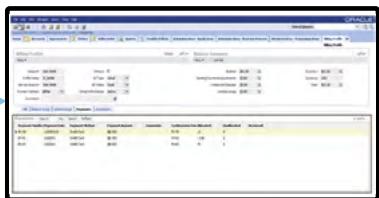
## INTEGRATED PAYMENT TERMINAL



Payment terminal shares card data with payment middleware

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).

## PAYMENT MIDDLEWARE

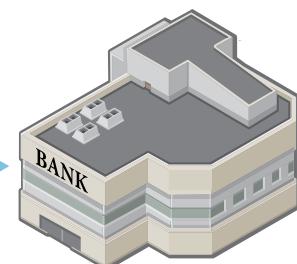


Software used as part of payment transaction

## ROUTER/ FIREWALL



## INTERNET



**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

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.



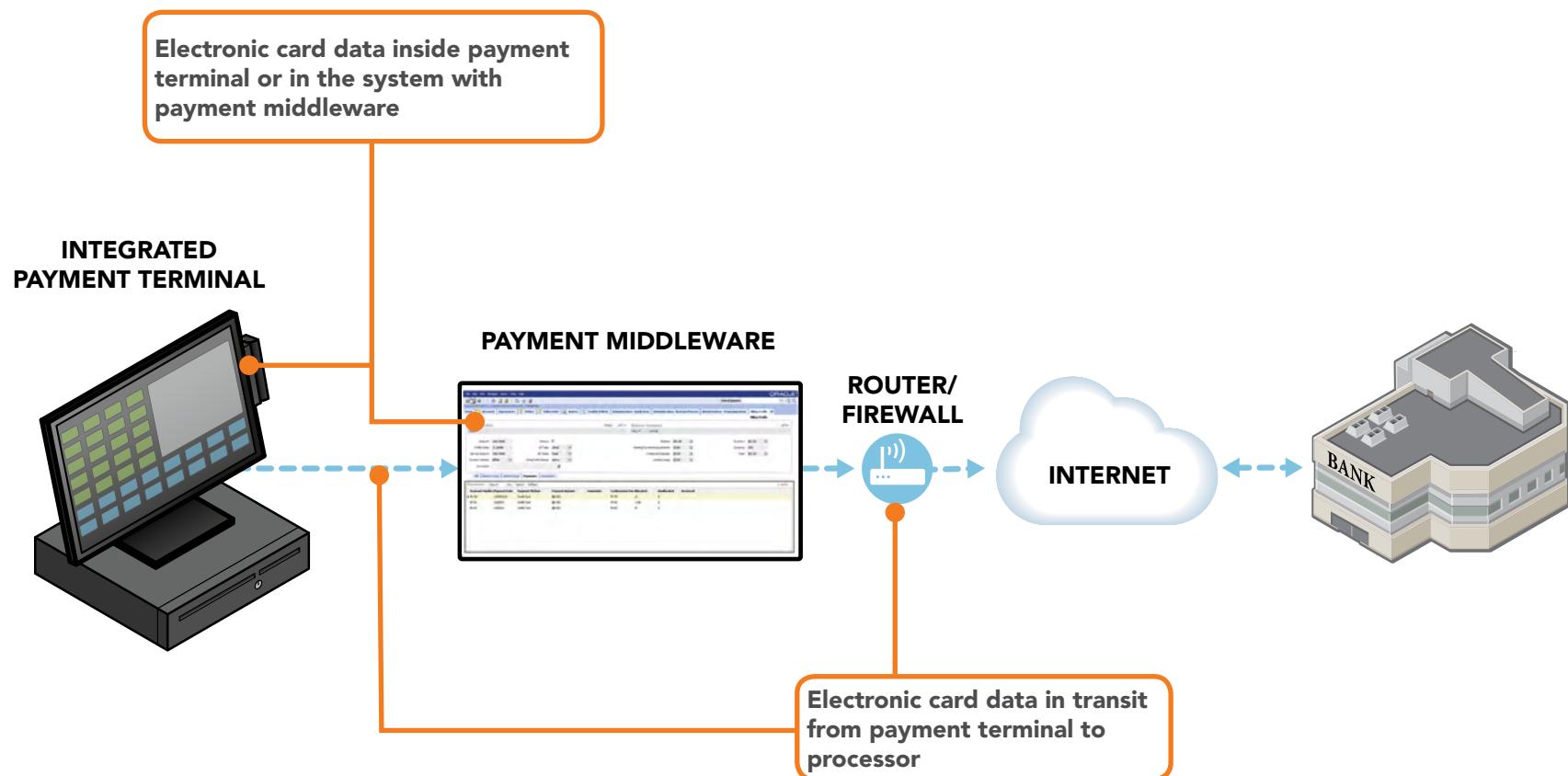
TYPE 6 OVERVIEW

TYPE 6 RISKS

TYPE 6 THREATS

TYPE 6 PROTECTIONS

## Where is your card data at risk?



# Integrated payment terminal and payment middleware share card data. Payments sent via Internet.



TYPE 6 OVERVIEW

TYPE 6 RISKS

TYPE 6 THREATS

TYPE 6 PROTECTIONS

## How do criminals get your card data?

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

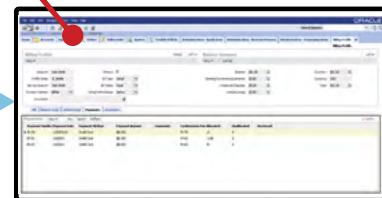
They insert "malware"(software) onto a payment system that enables them to steal card data.

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

INTEGRATED PAYMENT TERMINAL



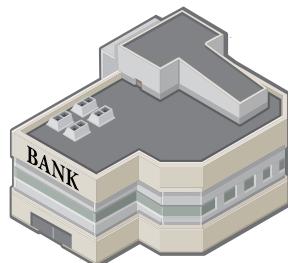
PAYMENT MIDDLEWARE



ROUTER/ FIREWALL



INTERNET



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.



TYPE 6 OVERVIEW

TYPE 6 RISKS

TYPE 6 THREATS

TYPE 6 PROTECTIONS

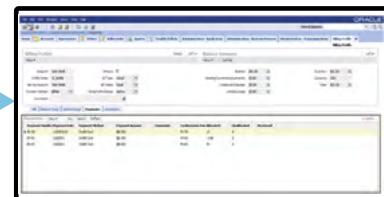
## How do you start to protect card data today?\*

- |  |  |  |   |  |   |  |   |
|--|--|--|---|--|---|--|---|
|  | 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       |  | Use anti-virus software   |  | Make your card data useless to criminals          |

**INTEGRATED PAYMENT TERMINAL**



**PAYMENT MIDDLEWARE**



**ROUTER/FIREWALL**



**INTERNET**



**BANK**

\*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.



## TYPE 7 OVERVIEW

## TYPE 7 RISKS

## TYPE 7 THREATS

## TYPE 7 PROTECTIONS

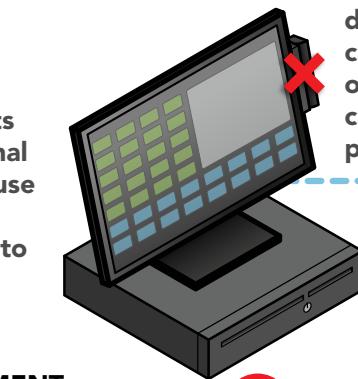
If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to [Type 15](#).

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).

## INTEGRATED PAYMENT TERMINAL



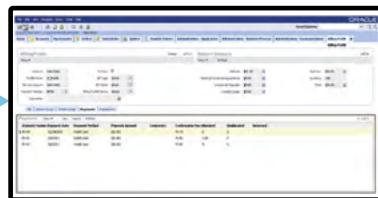
Integrated payment terminal with disabled card reader or with no card reader present

## WIRELESS PAYMENT TERMINAL



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

## PAYMENT MIDDLEWARE

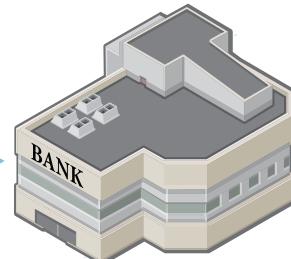


Software used as part of payment transaction

## ROUTER/ FIREWALL



## INTERNET



## YES

This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

## NO

I'm not positive this is my payment system. Show me the overview again

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

# Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.



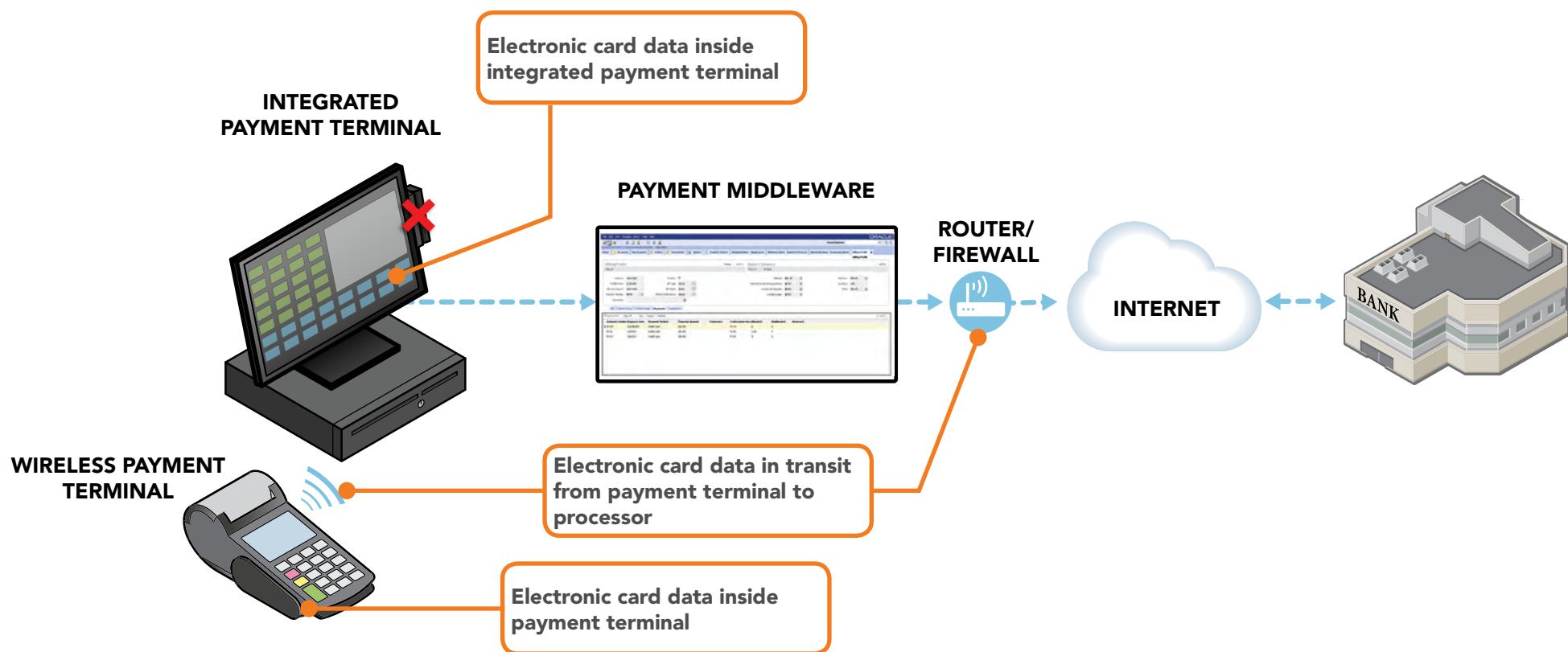
TYPE 7 OVERVIEW

TYPE 7 RISKS

TYPE 7 THREATS

TYPE 7 PROTECTIONS

## Where is your card data at risk?



# Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.



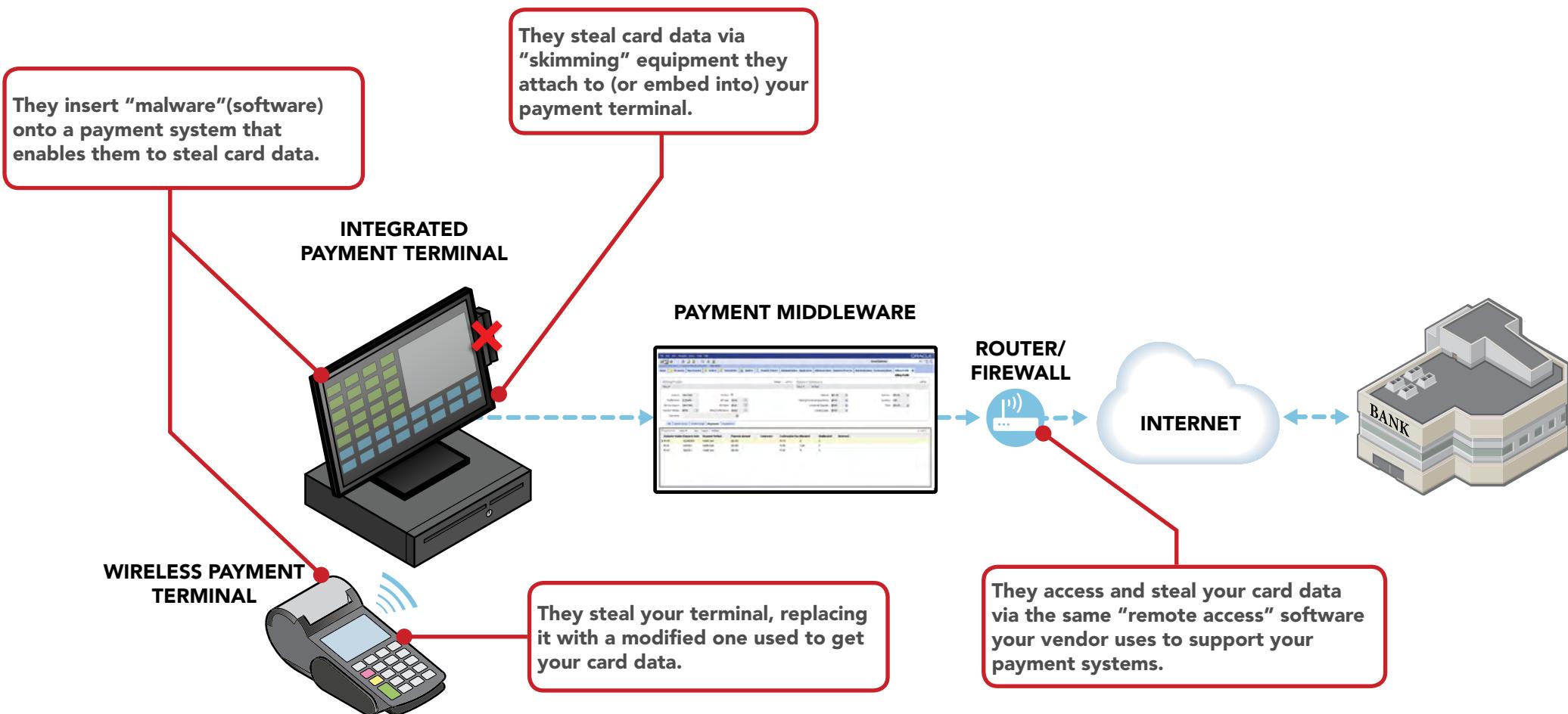
TYPE 7 OVERVIEW

TYPE 7 RISKS

TYPE 7 THREATS

TYPE 7 PROTECTIONS

## How do criminals get your card data?



# Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware. Payments sent via Internet.



TYPE 7 OVERVIEW

TYPE 7 RISKS

TYPE 7 THREATS

TYPE 7 PROTECTIONS

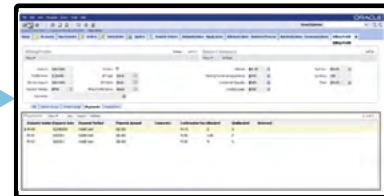
## How do you start to protect card data today?\*

- |   |   |   |   |
|---|---|---|---|
|  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       |  Use anti-virus software   |  Make your card data useless to criminals          |

### INTEGRATED PAYMENT TERMINAL



### PAYMENT MIDDLEWARE



### ROUTER/FIREWALL



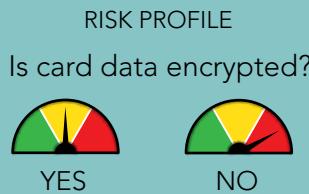
INTERNET



\*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](#).

TYPE  
8

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



## TYPE 8 OVERVIEW

## TYPE 8 RISKS

## TYPE 8 THREATS

## TYPE 8 PROTECTIONS

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).

## ELECTRONIC CASH REGISTER

Card data can be entered on electronic cash register or payment terminal

## PAYMENT TERMINAL

## GENERAL USE COMPUTERS



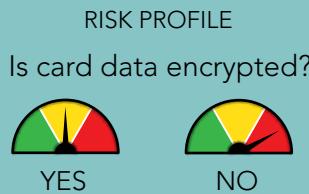
There are many risk points here due to the additional equipment in the same network as the payment terminal and also connected to the Internet. Each device and system has to be configured and managed securely to minimize risk.

**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

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.



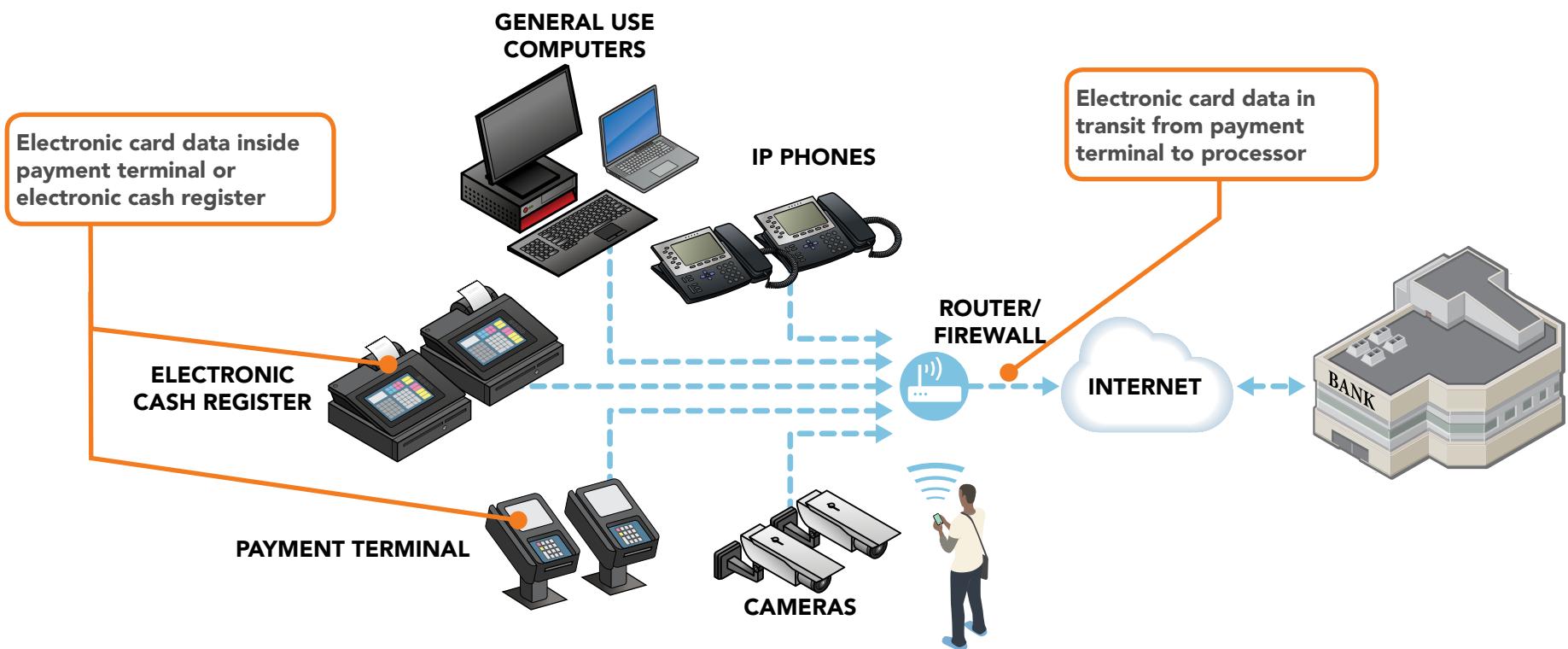
TYPE 8 OVERVIEW

TYPE 8 RISKS

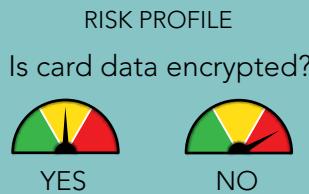
TYPE 8 THREATS

TYPE 8 PROTECTIONS

## Where is your card data at risk?



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



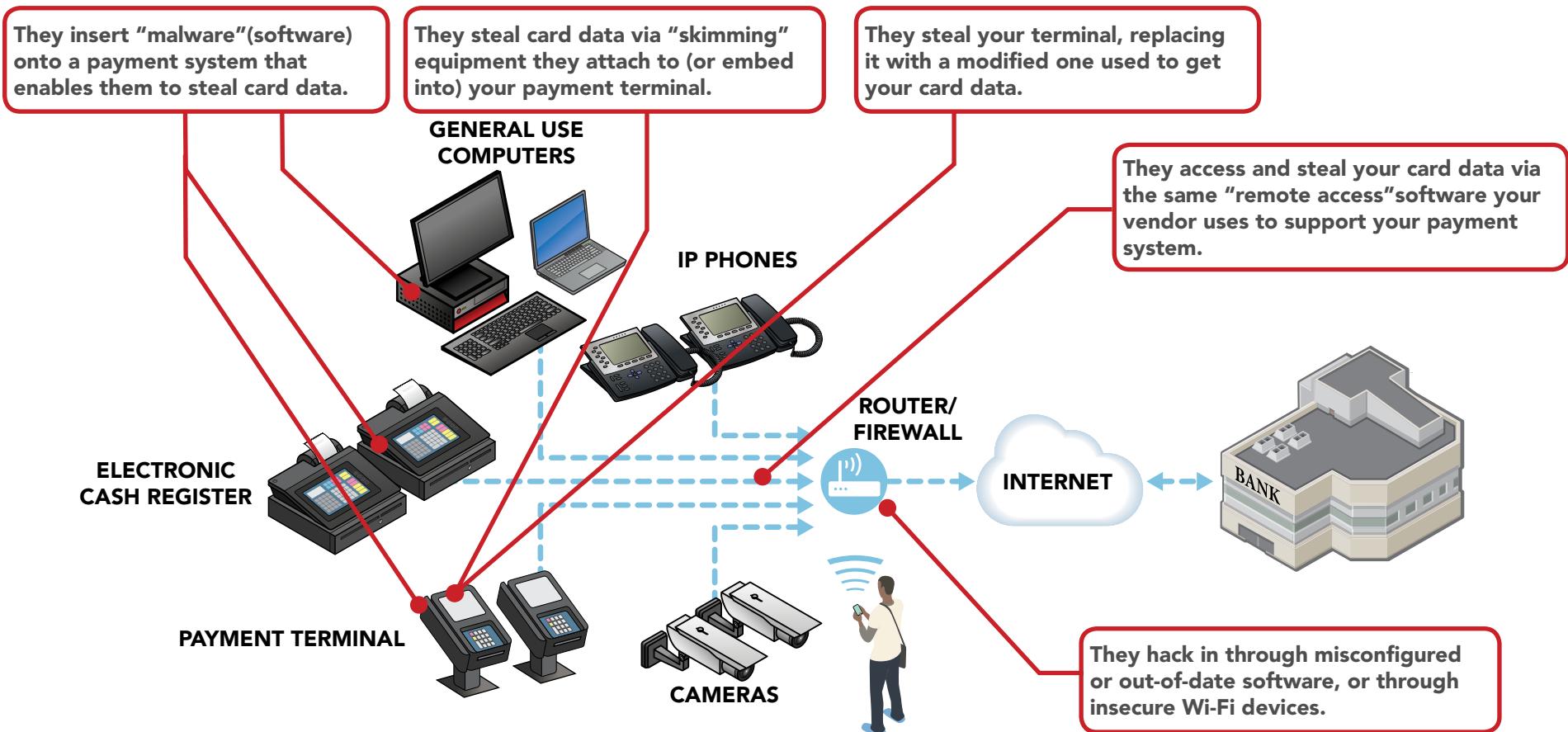
TYPE 8 OVERVIEW

TYPE 8 RISKS

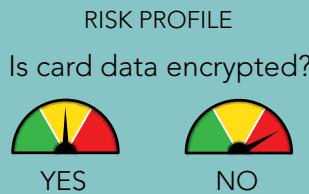
TYPE 8 THREATS

TYPE 8 PROTECTIONS

## How do criminals get your card data?



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



TYPE 8 OVERVIEW

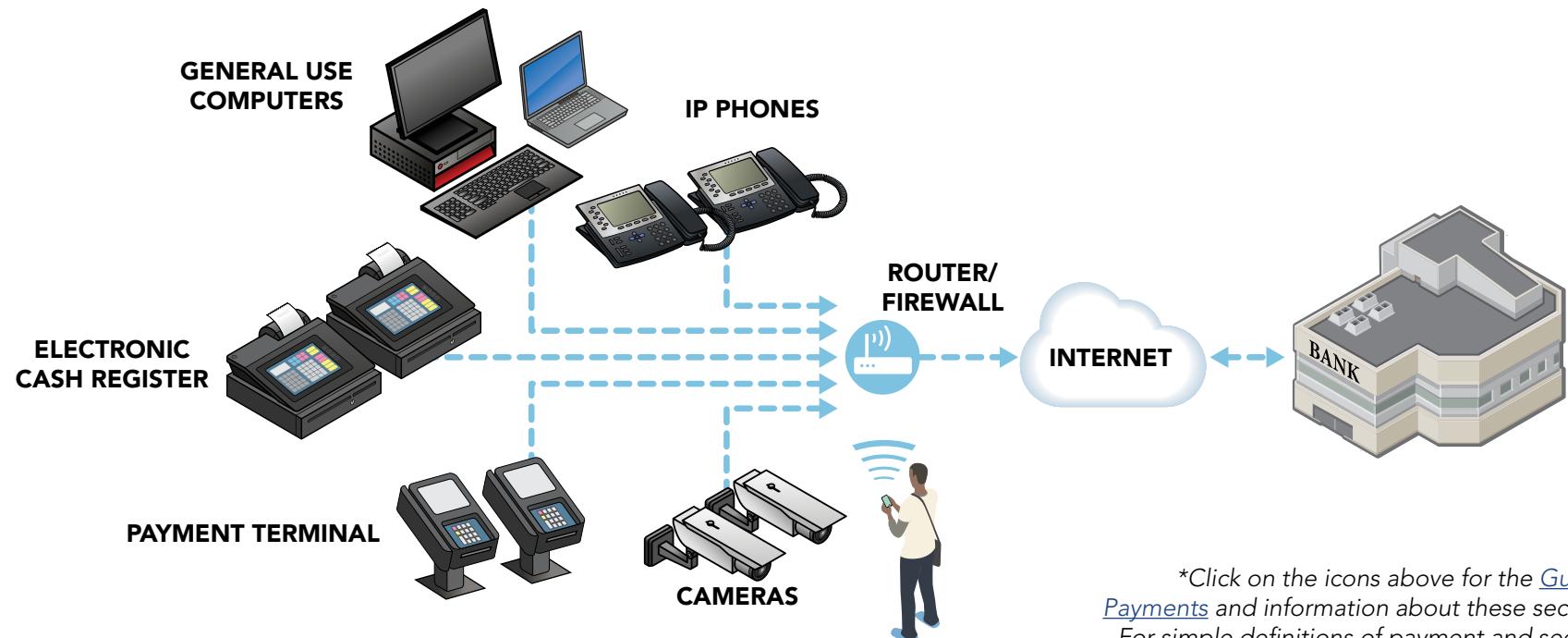
TYPE 8 RISKS

TYPE 8 THREATS

TYPE 8 PROTECTIONS

## 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       |  | 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](#).



# E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.

## TYPE 9 OVERVIEW

## TYPE 9 RISKS

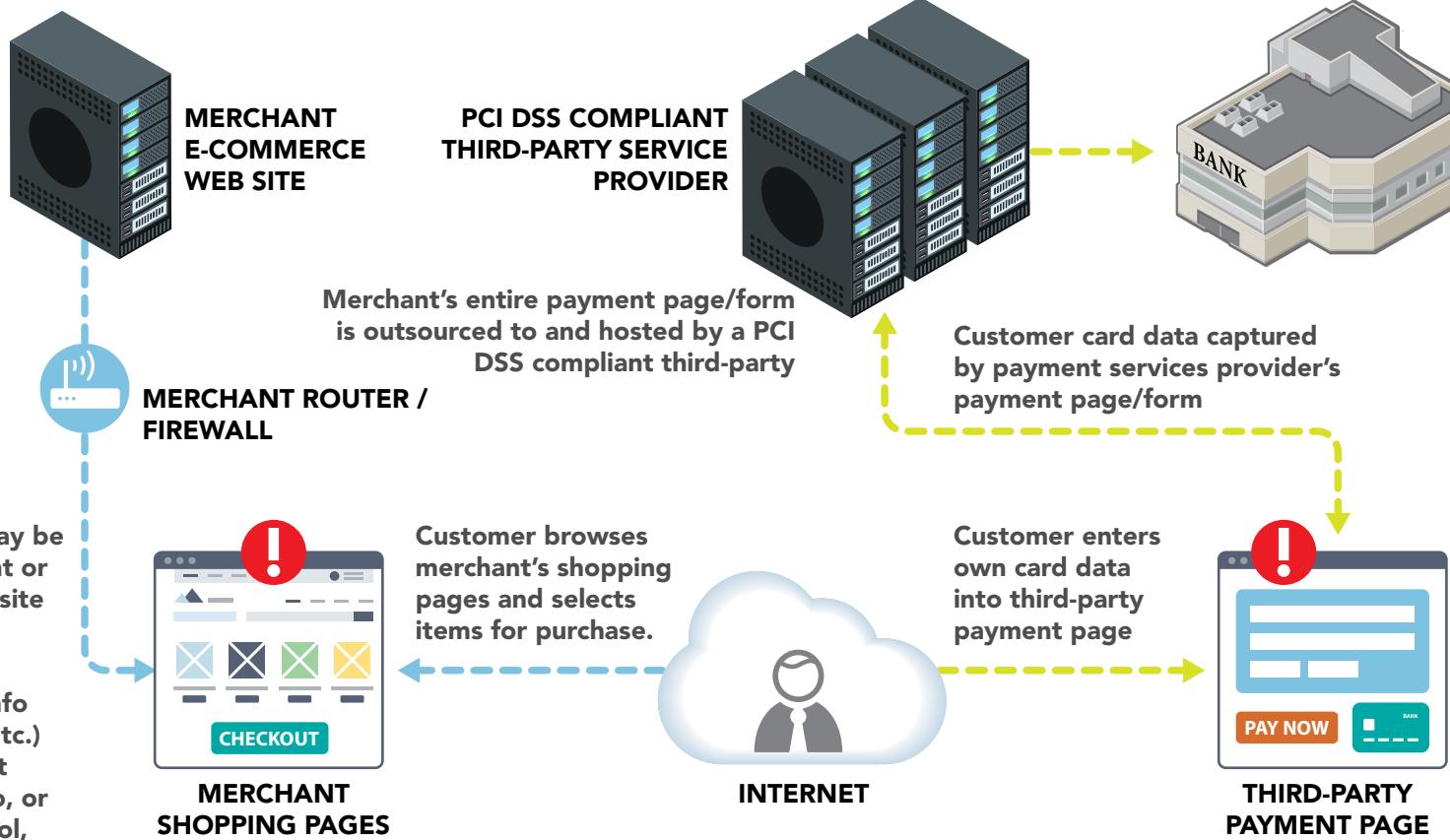
## TYPE 9 THREATS

## TYPE 9 PROTECTIONS

**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)

**Merchant website** may be hosted and managed by the merchant or by a third party hosting provider on the merchant's behalf. Either way, the merchant has no access to the payment page.



**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

**KEY**

- Merchant responsibility
- Third-party service provider responsibility



# E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.

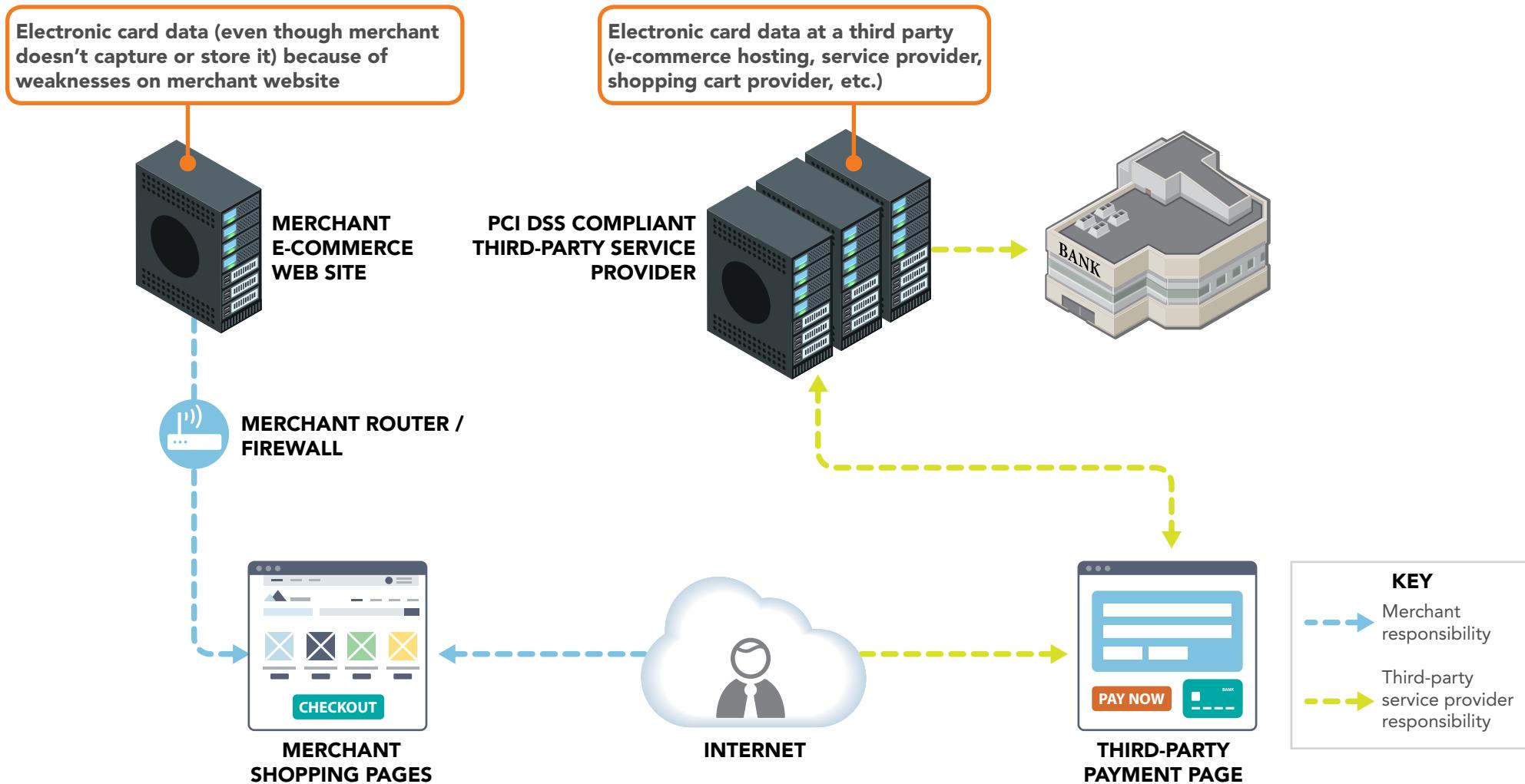
TYPE 9 OVERVIEW

TYPE 9 RISKS

TYPE 9 THREATS

TYPE 9 PROTECTIONS

## Where is your card data at risk?



# E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.



TYPE 9 OVERVIEW

TYPE 9 RISKS

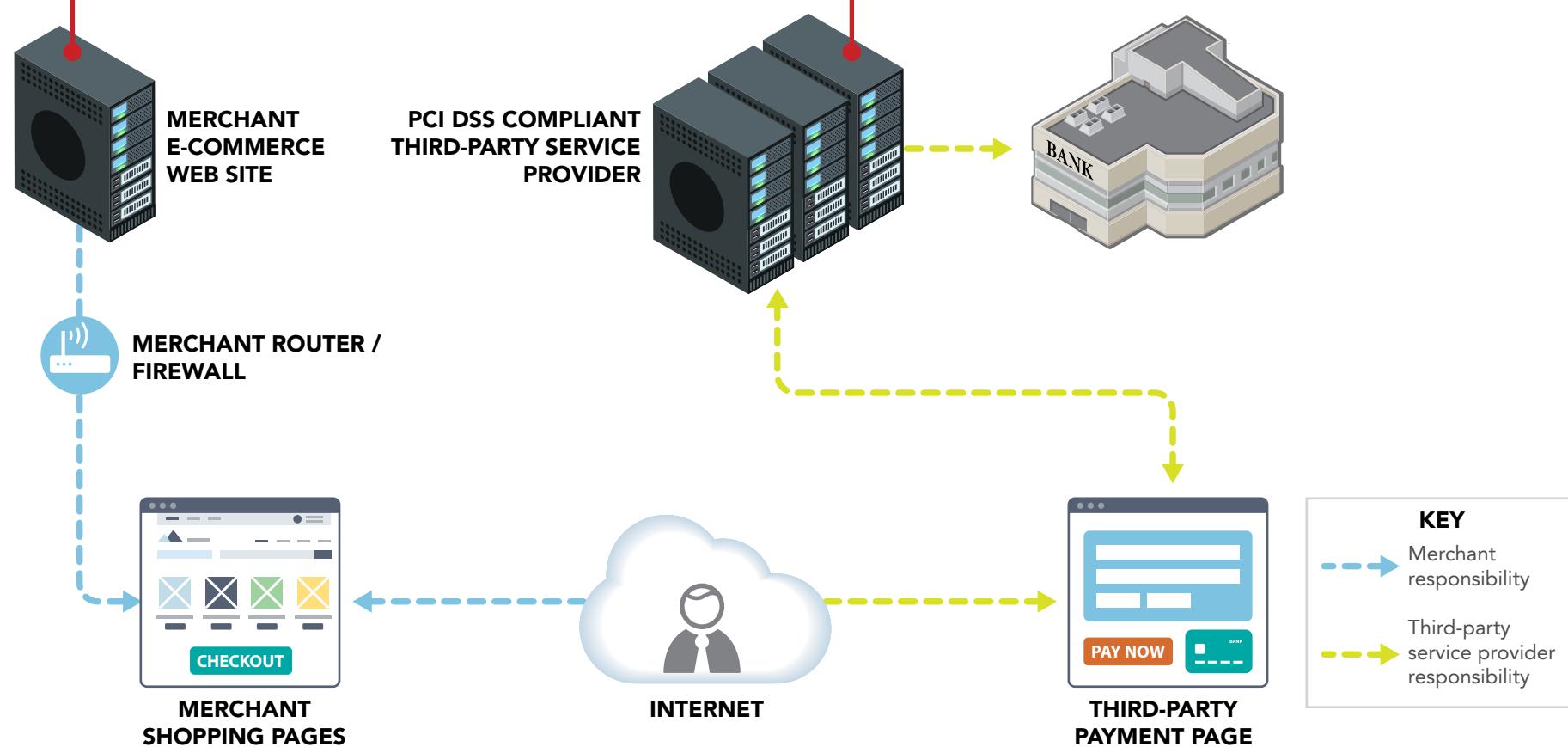
TYPE 9 THREATS

TYPE 9 PROTECTIONS

## 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.).





# E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.

TYPE 9 OVERVIEW

TYPE 9 RISKS

TYPE 9 THREATS

TYPE 9 PROTECTIONS

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



Use strong passwords



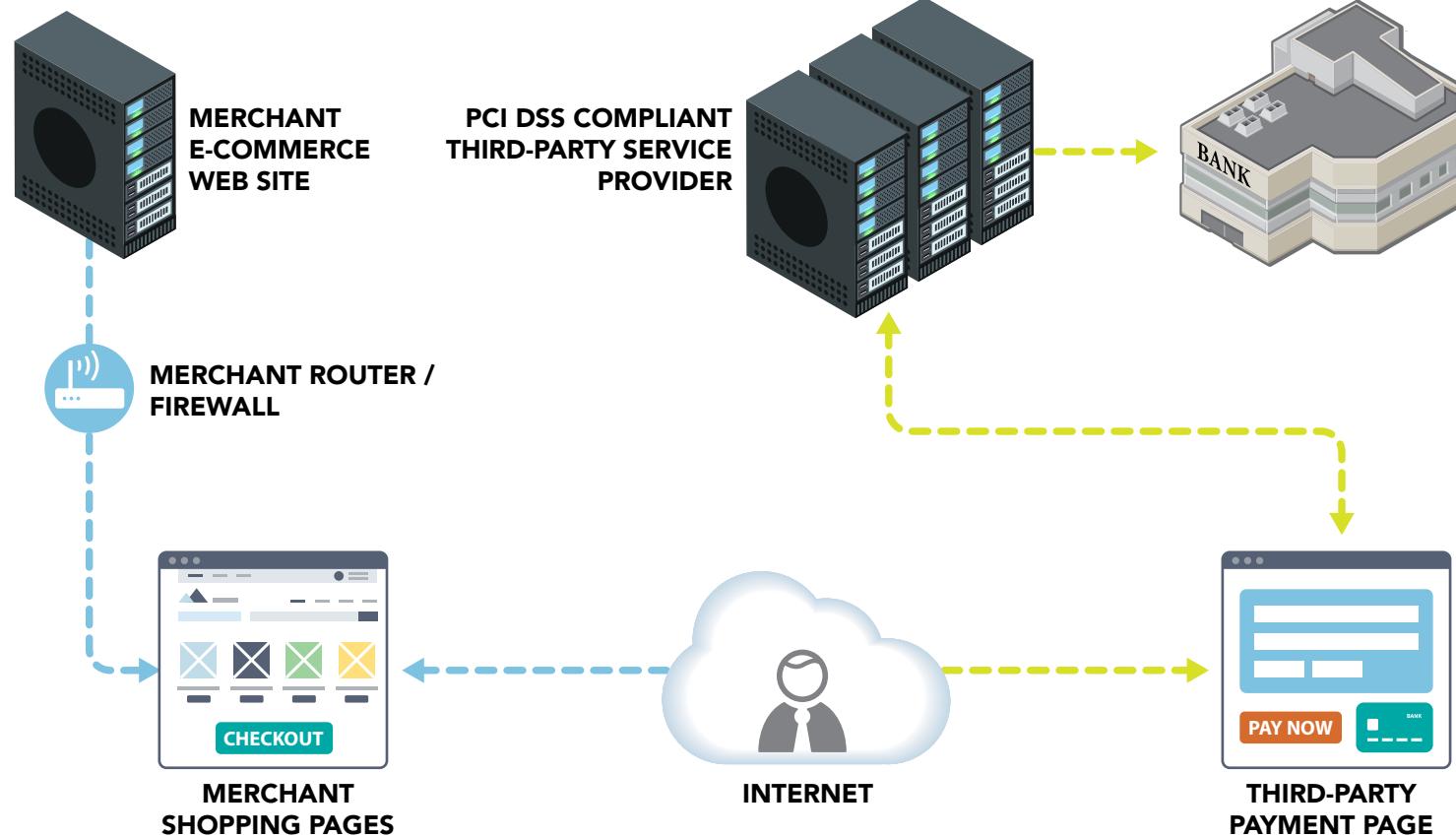
Protect card data and only keep what you need



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.

## TYPE 10 OVERVIEW

## TYPE 10 RISKS

## TYPE 10 THREATS

## TYPE 10 PROTECTIONS

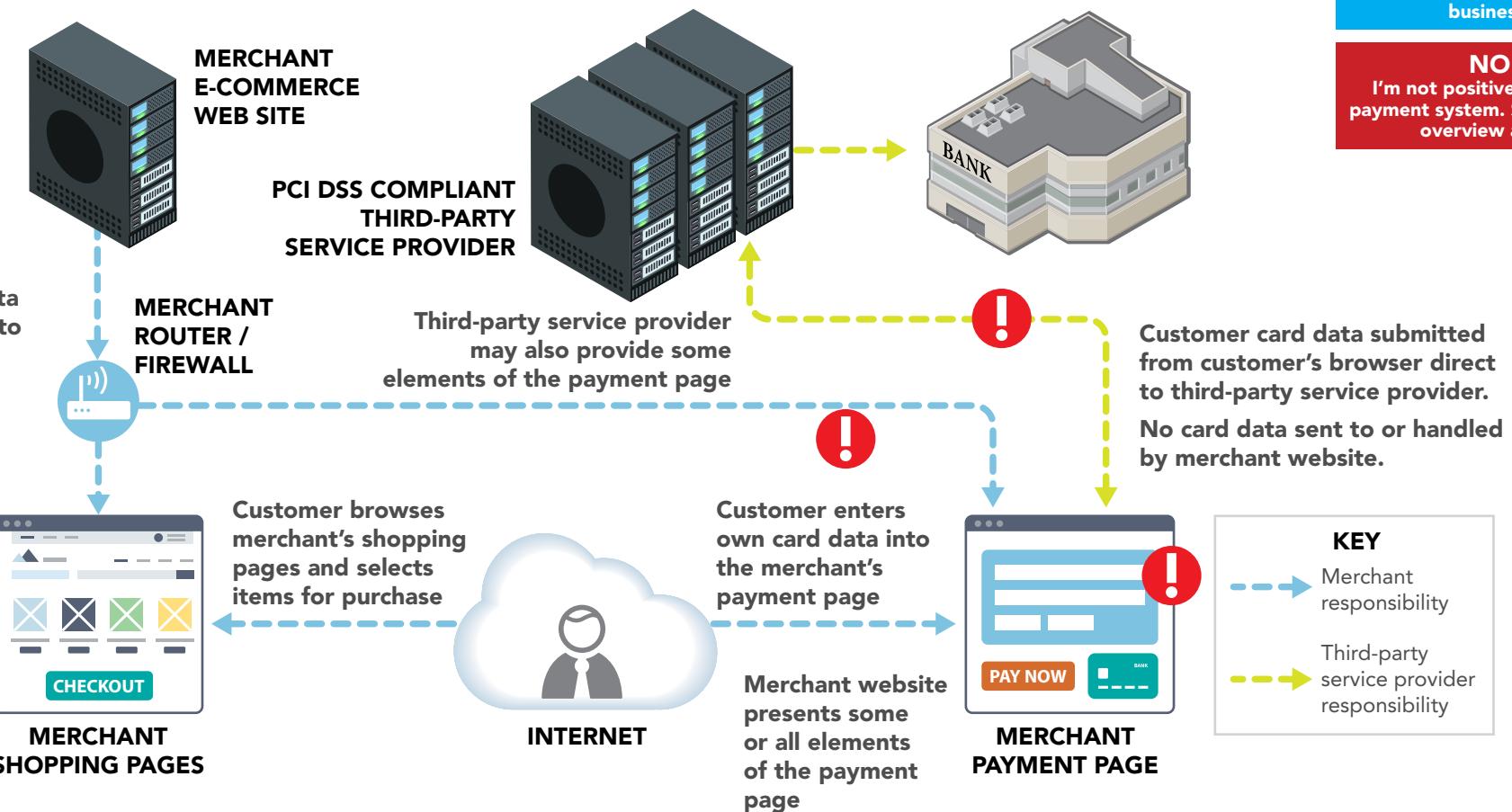
EITHER: Merchant website creates the entire payment page and uses the Direct Post Method to send card data (as shown).

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.

Merchant website may be hosted and managed by the merchant or by a third party hosting provider on the merchant's behalf.

Merchant website controls how card data is collected and sent to the third party.



**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

For this scenario, risks to card data are present at ! 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.**

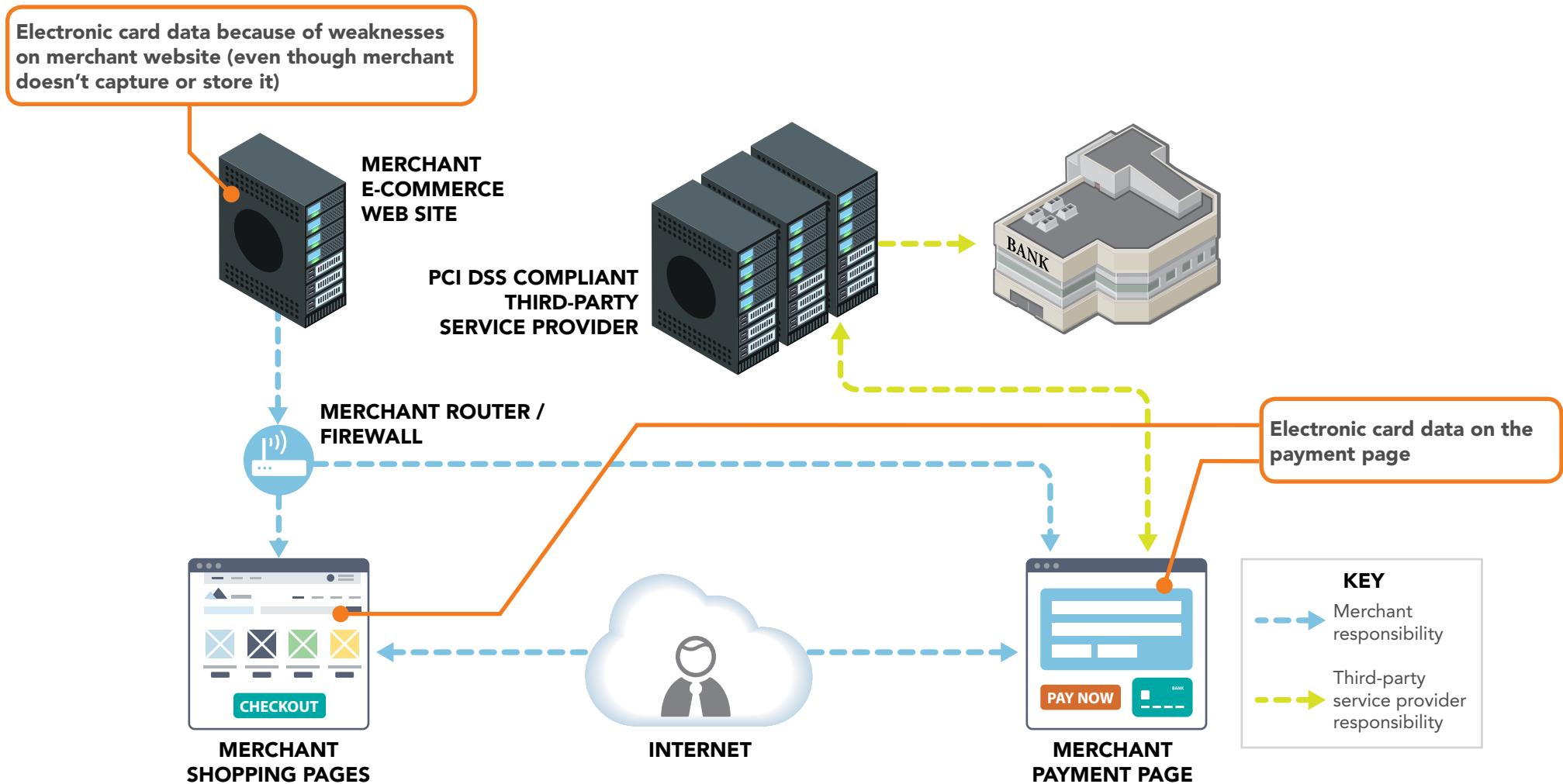
TYPE 10 OVERVIEW

TYPE 10 RISKS

TYPE 10 THREATS

TYPE 10 PROTECTIONS

## Where is your card data at risk?





# 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.

TYPE 10 OVERVIEW

TYPE 10 RISKS

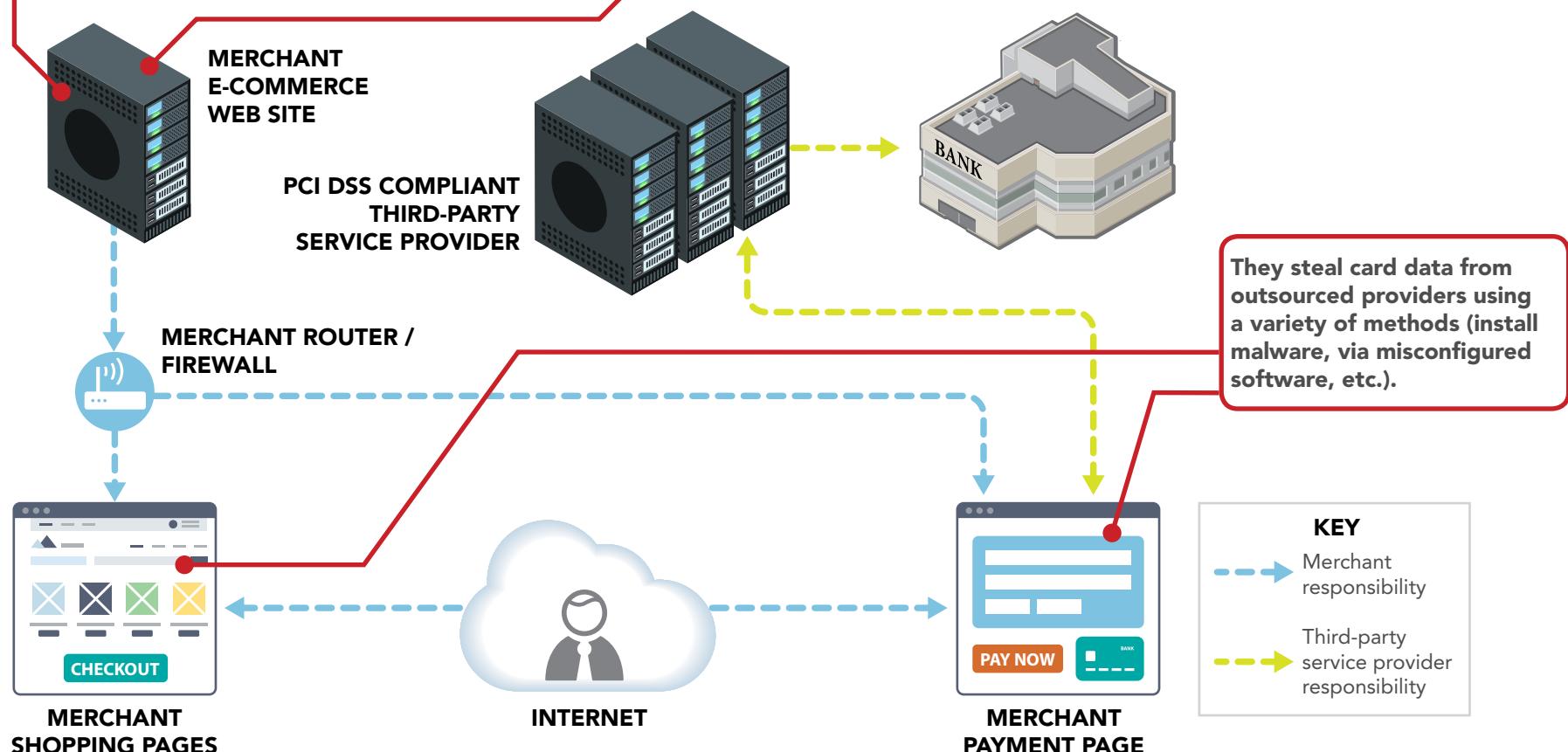
TYPE 10 THREATS

TYPE 10 PROTECTIONS

## 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





# 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.

TYPE 10 OVERVIEW

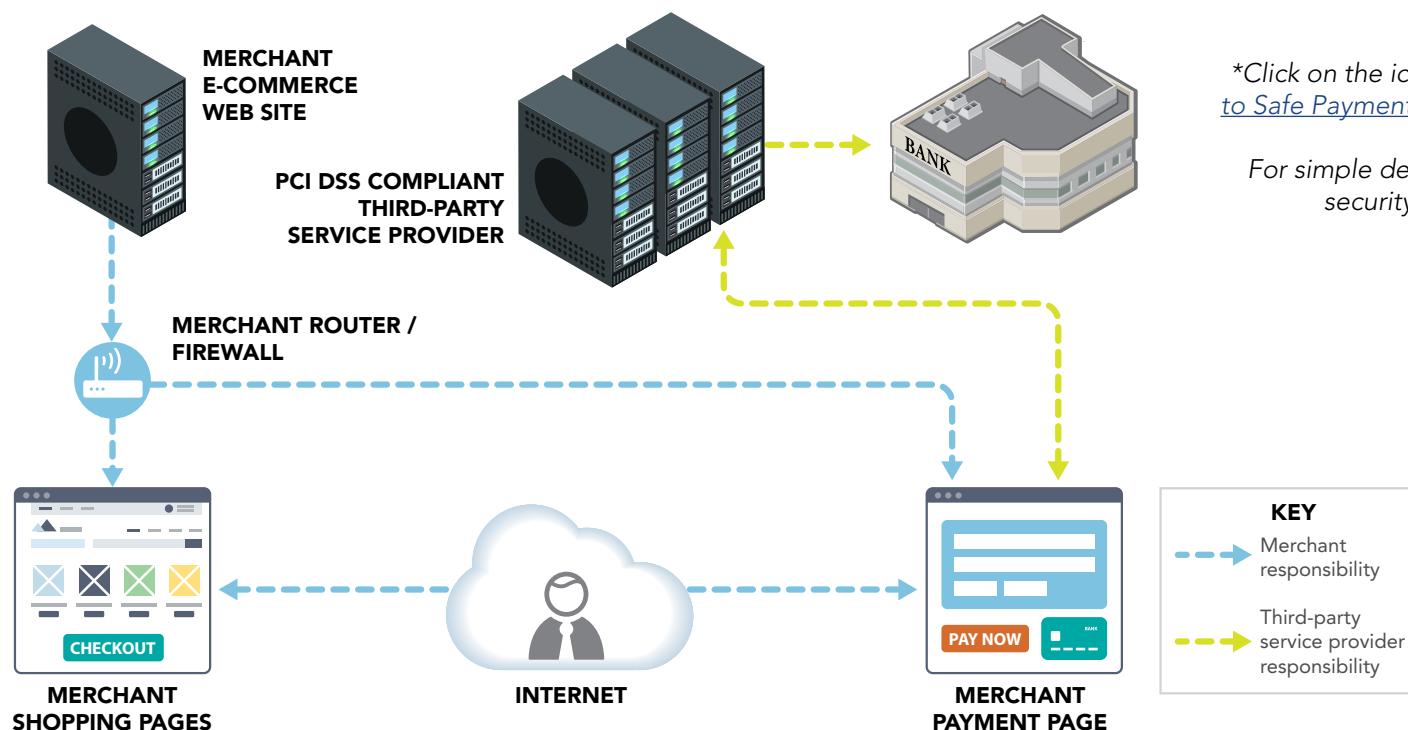
TYPE 10 RISKS

TYPE 10 THREATS

TYPE 10 PROTECTIONS

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

- |  |   |  |   |  |   |  |  |
|--|---|--|---|--|---|--|--|
|  | Use strong passwords                      |  | Protect card data and only keep what you need                                 |  | 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 |  | Use anti-virus software                           |  | Get regular vulnerability scanning               |
|  | Use secure payment systems                |  | Protect your business from the Internet                                       |  | 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.

## TYPE 11 OVERVIEW

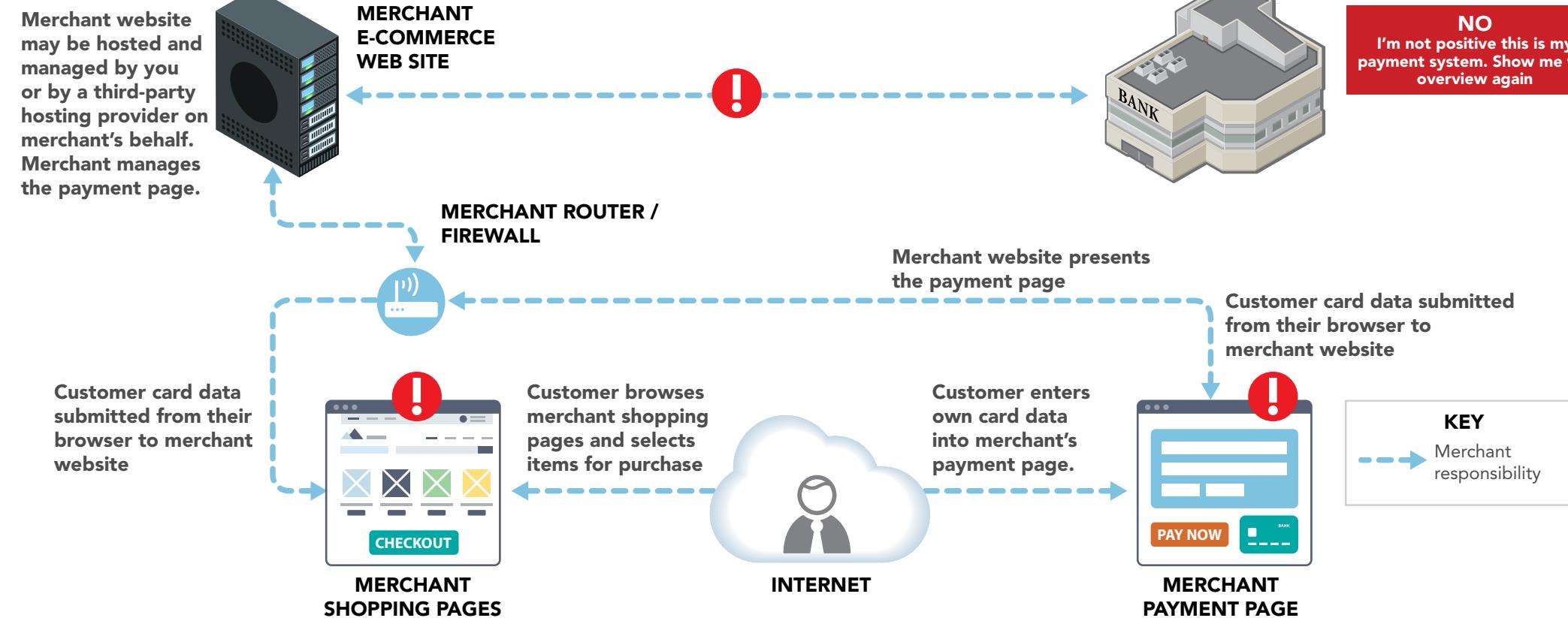
## TYPE 11 RISKS

## TYPE 11 THREATS

## TYPE 11 PROTECTIONS

**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again



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.

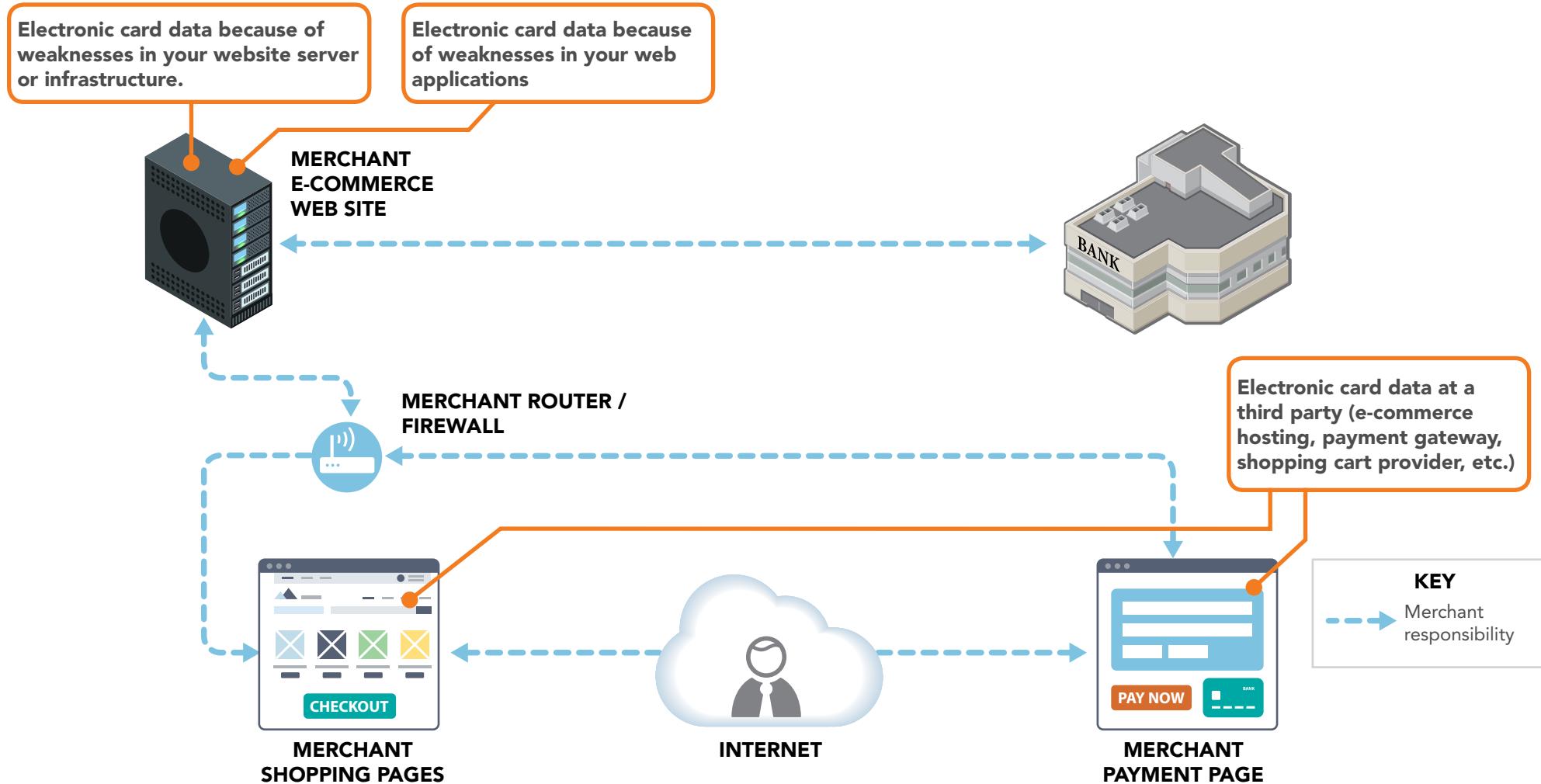
TYPE 11 OVERVIEW

TYPE 11 RISKS

TYPE 11 THREATS

TYPE 11 PROTECTIONS

## Where is your card data at risk?





# E-commerce merchant accepts card data using payment page presented to customers from own website. Payments sent via the merchant website.

TYPE 11 OVERVIEW

TYPE 11 RISKS

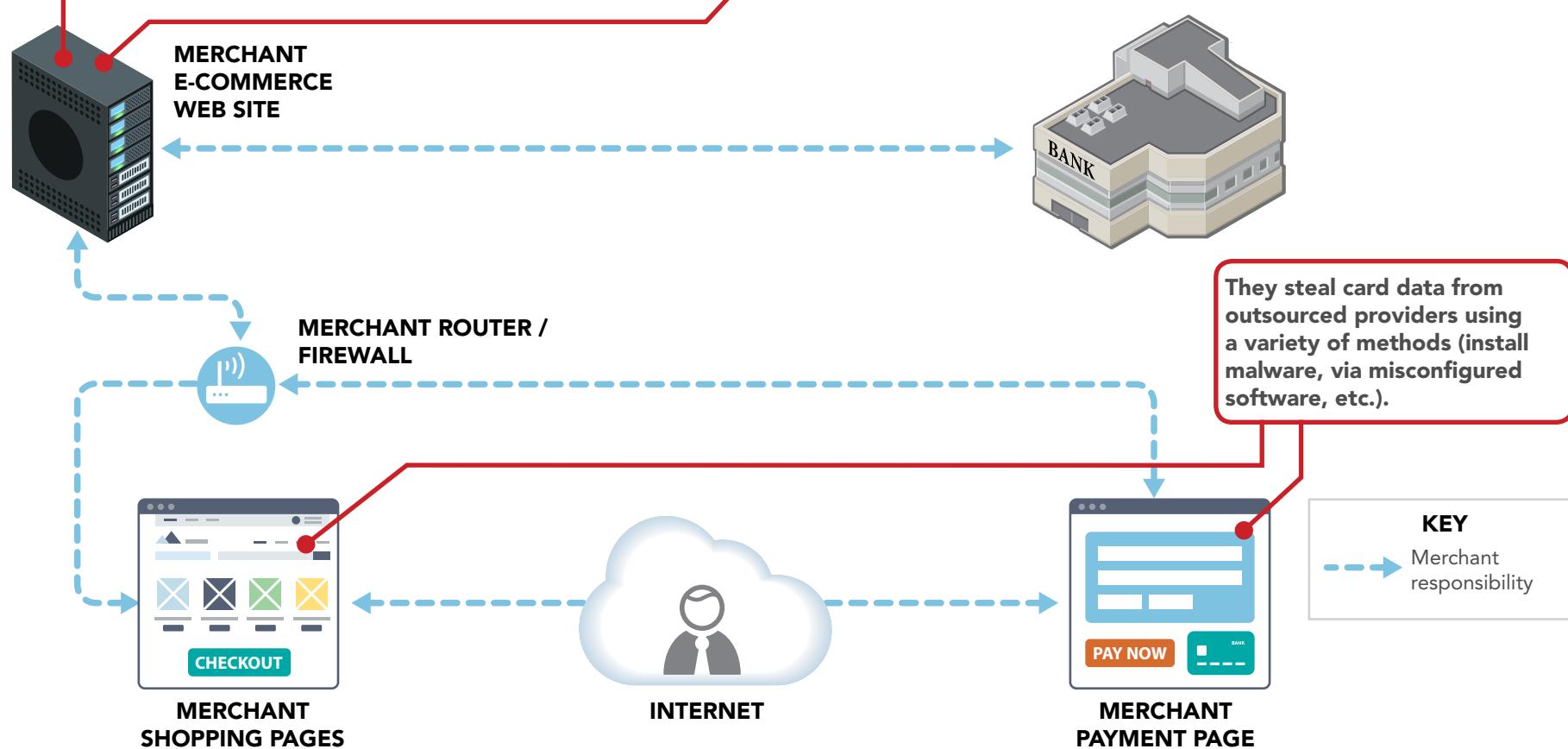
TYPE 11 THREATS

TYPE 11 PROTECTIONS

## 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.





# E-commerce merchant accepts card data using payment page presented to customers from own website. Payments sent via the merchant website.

TYPE 11 OVERVIEW

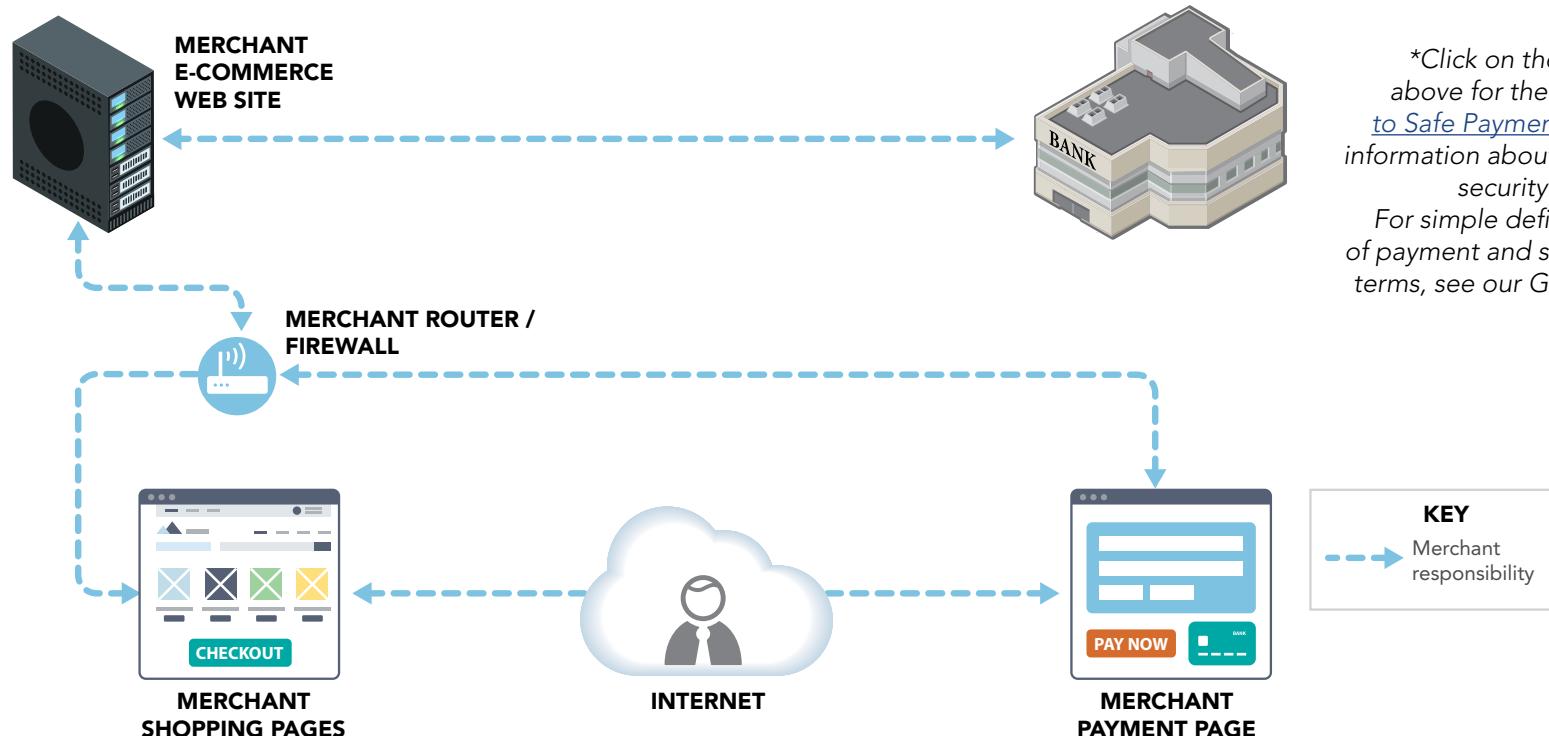
TYPE 11 RISKS

TYPE 11 THREATS

TYPE 11 PROTECTIONS

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

- |  |   |   |  |
|--|---|---|--|
|  Use strong passwords                      |  Protect card data and only keep what you need                                 |  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 |  Use anti-virus software                           |  Get regular vulnerability scanning               |
|  Use secure payment systems                |  Protect your business from the Internet                                       |  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](#).



# PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

## TYPE 12 OVERVIEW

## TYPE 12 RISKS

## TYPE 12 THREATS

## TYPE 12 PROTECTIONS

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

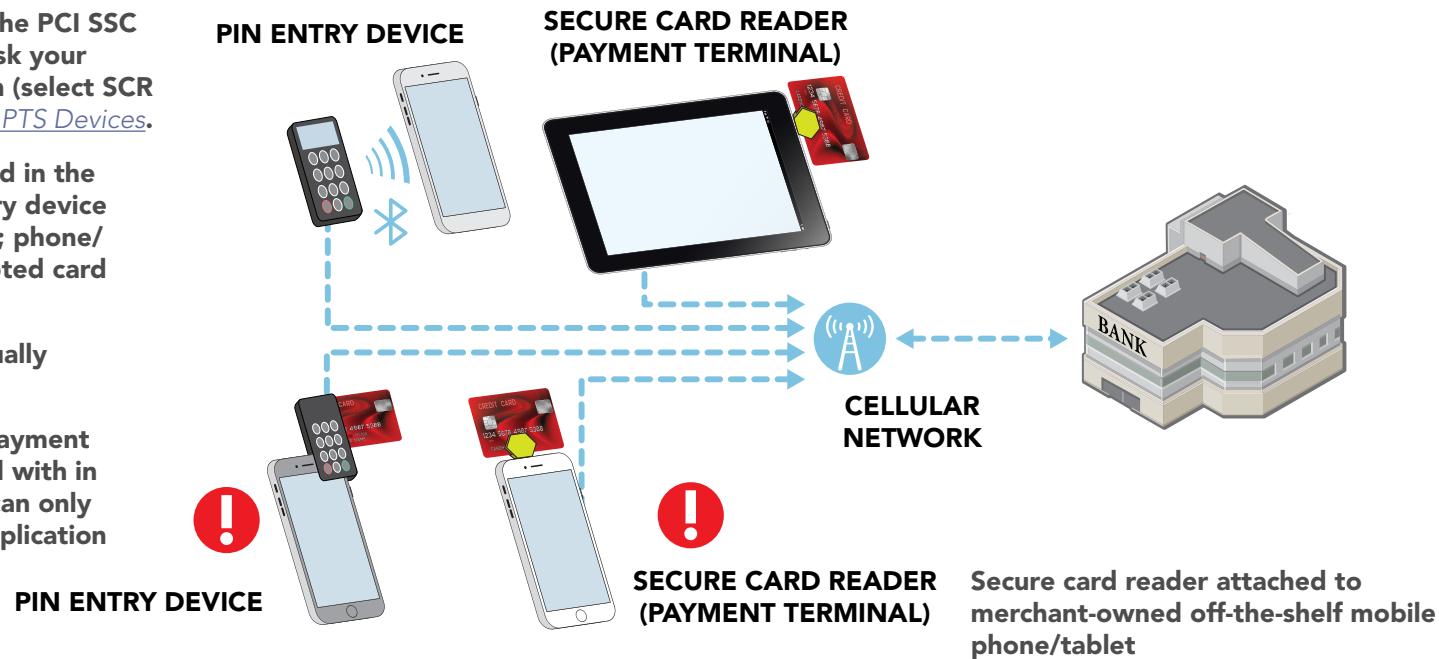
Merchant has no ability to manually enter card data.

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.

Different devices are used to read magnetic stripe card data, enter personal identification number (PIN), and read chip card data

**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again



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 only.

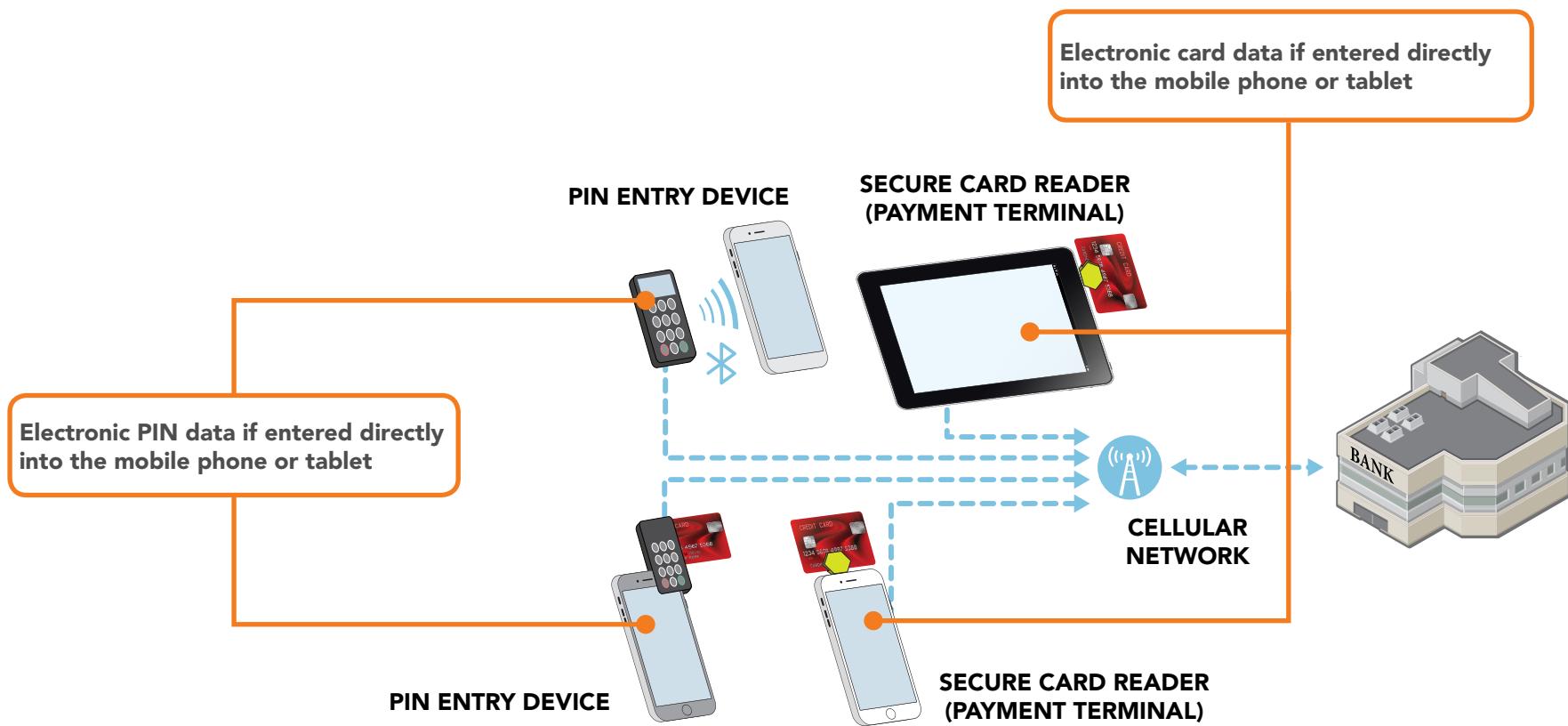
TYPE 12 OVERVIEW

TYPE 12 RISKS

TYPE 12 THREATS

TYPE 12 PROTECTIONS

## Where is your card data at risk?





# PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

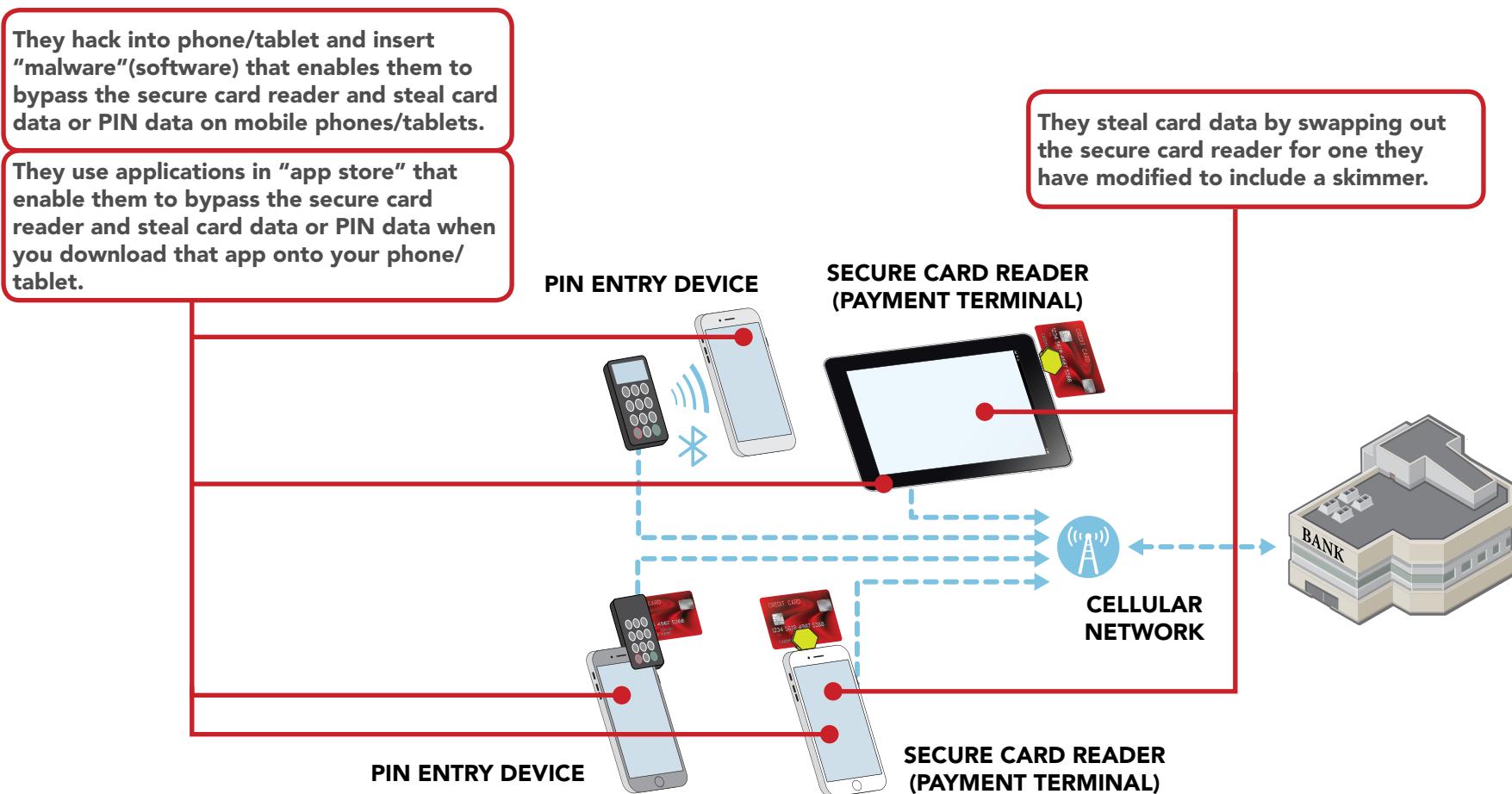
TYPE 12 OVERVIEW

TYPE 12 RISKS

TYPE 12 THREATS

TYPE 12 PROTECTIONS

## How do criminals get your card data?



# PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.



TYPE 12 OVERVIEW

TYPE 12 RISKS

TYPE 12 THREATS

TYPE 12 PROTECTIONS

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



Inspect your secure card readers and PIN entry devices for damage or changes



Install patches from your vendors



Use a secure card reader and PIN entry device



Make your card data useless to criminals



Limit remote access for your vendor partners - don't give hackers easy access



Ask your vendor partners for help if you need it



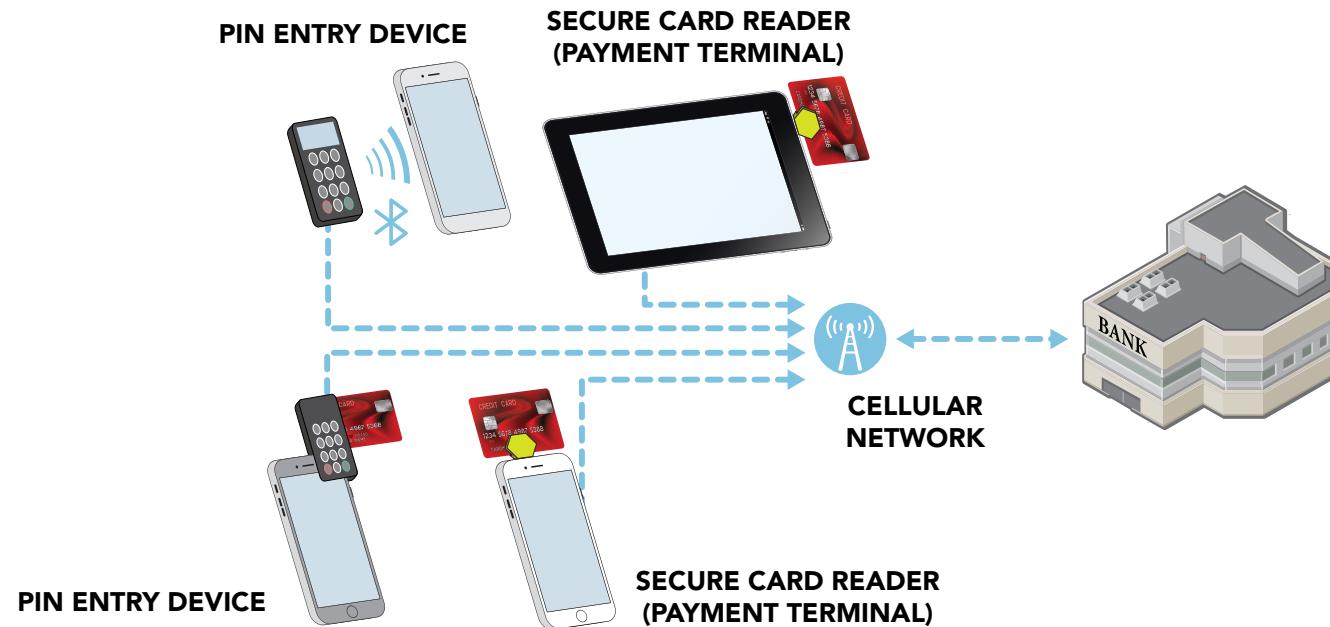
Protect card data and only keep what you need



Protect your business from the Internet



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.

## TYPE 13 OVERVIEW

## TYPE 13 RISKS

## TYPE 13 THREATS

## TYPE 13 PROTECTIONS

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.)

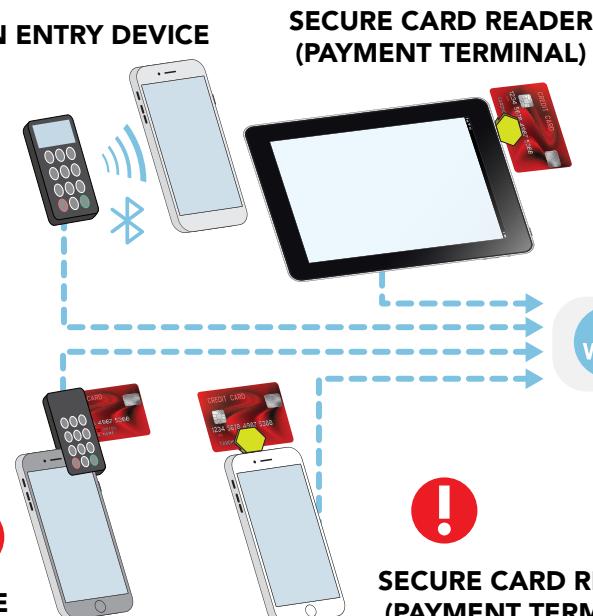
Secure card reader is listed on the PCI SSC website as an approved SCR. Ask your vendor or check here to confirm (select SCR under "device type"): [PCI-listed PTS Devices](#).

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

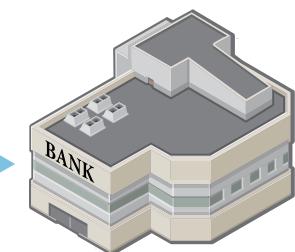
Merchant verifies that mobile payment terminal has not been tampered with in any way, and that applications can only be downloaded from vendor application stores.

### PIN ENTRY DEVICE



Different devices are used to read magnetic stripe card data, enter personal identification number (PIN), and read chip card data

### WIFI OR CELLULAR NETWORK



### SECURE CARD READER (PAYMENT TERMINAL)

Secure card reader attached to merchant-owned off-the-shelf mobile phone/tablet

**YES**  
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**  
I'm not positive this is my payment system. Show me the overview again

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.



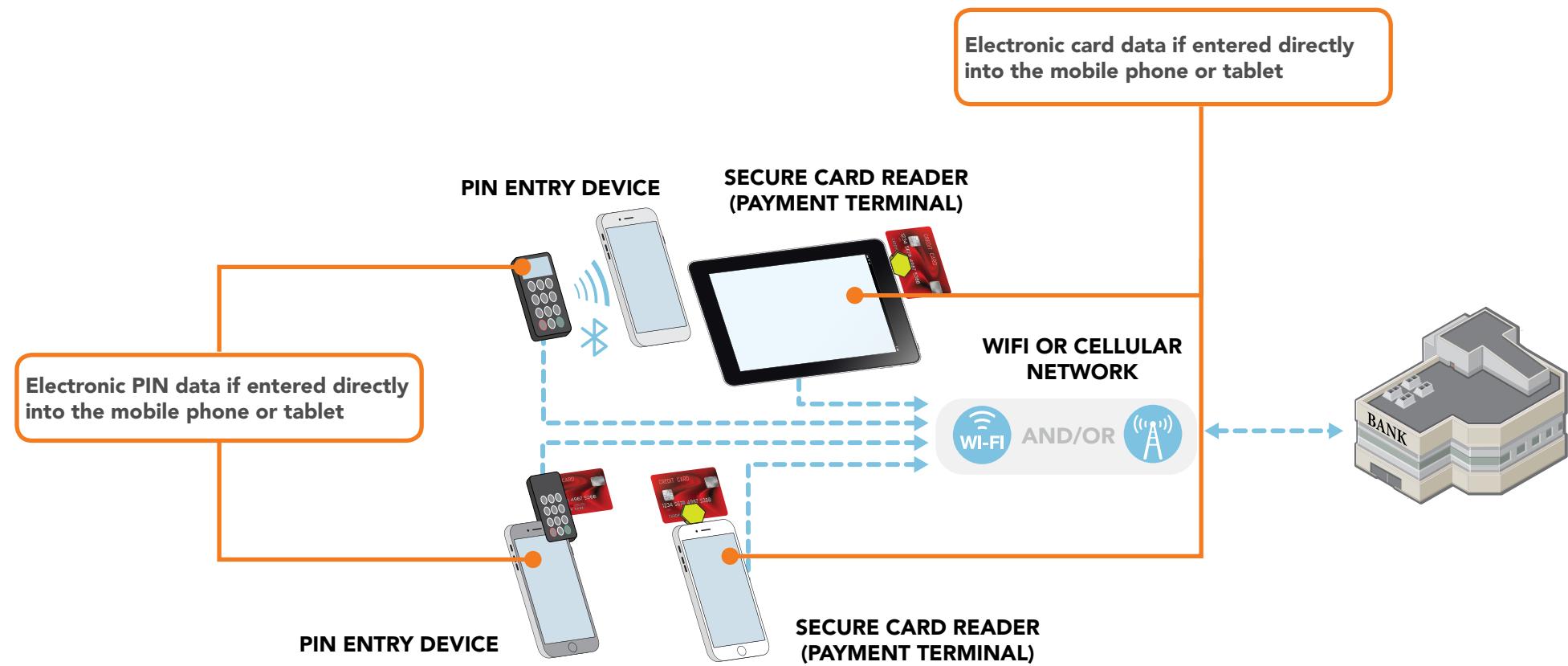
TYPE 13 OVERVIEW

TYPE 13 RISKS

TYPE 13 THREATS

TYPE 13 PROTECTIONS

## Where is your card data at risk?





# PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.

TYPE 13 OVERVIEW

TYPE 13 RISKS

TYPE 13 THREATS

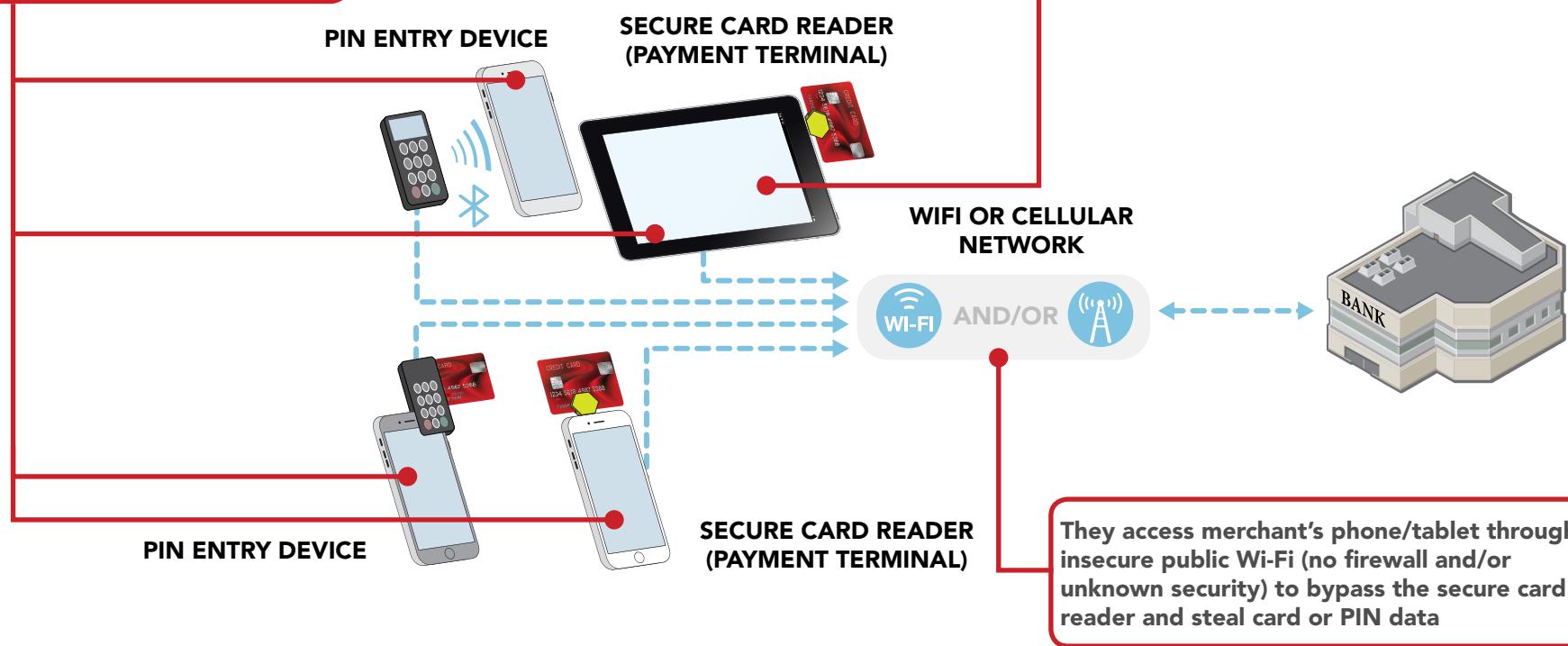
TYPE 13 PROTECTIONS

## 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.



# PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.



TYPE 13 OVERVIEW

TYPE 13 RISKS

TYPE 13 THREATS

TYPE 13 PROTECTIONS

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



Protect in-house access to your card data



Inspect your secure card readers and PIN entry devices for damage or changes



Protect your business from the Internet



Limit remote access for your vendor partners - don't give hackers easy access



Install patches from your payment terminal vendor



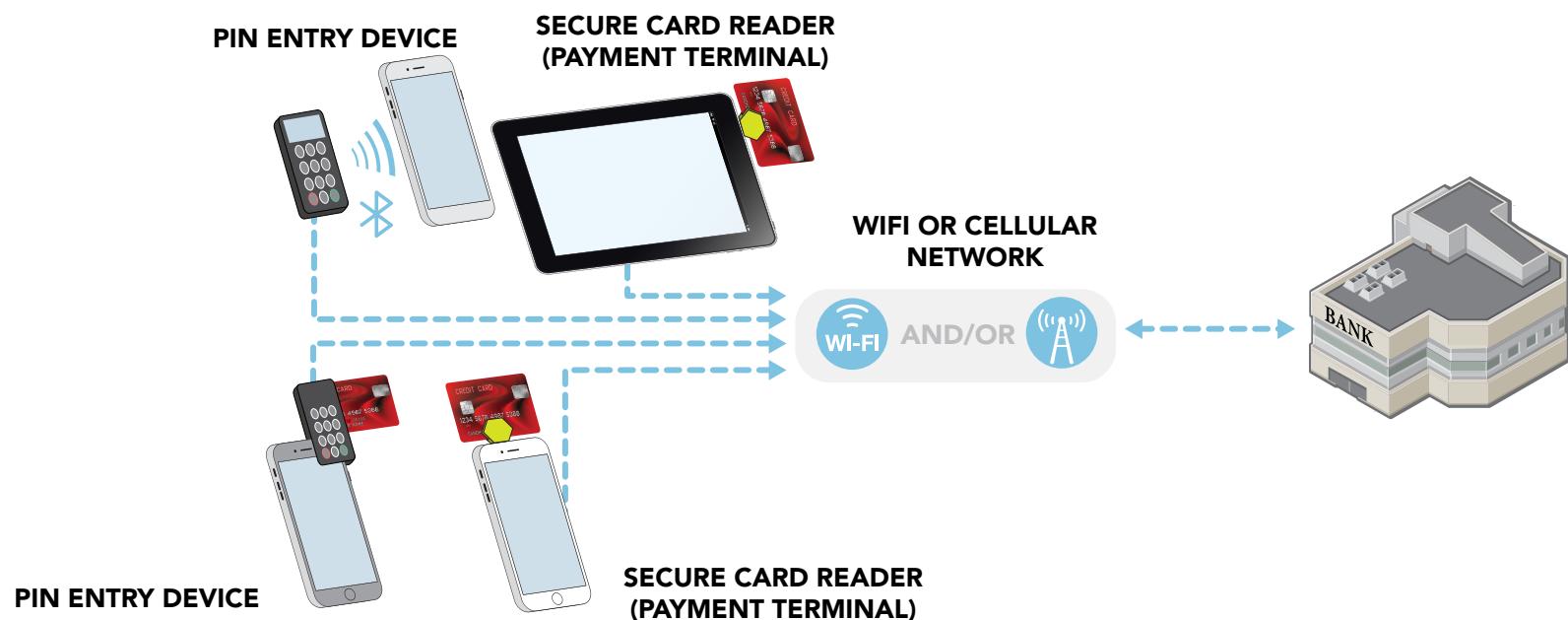
Make your card data useless to criminals



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.

## TYPE 14 OVERVIEW

## TYPE 14 RISKS

## TYPE 14 THREATS

## TYPE 14 PROTECTIONS

**YES**

This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**

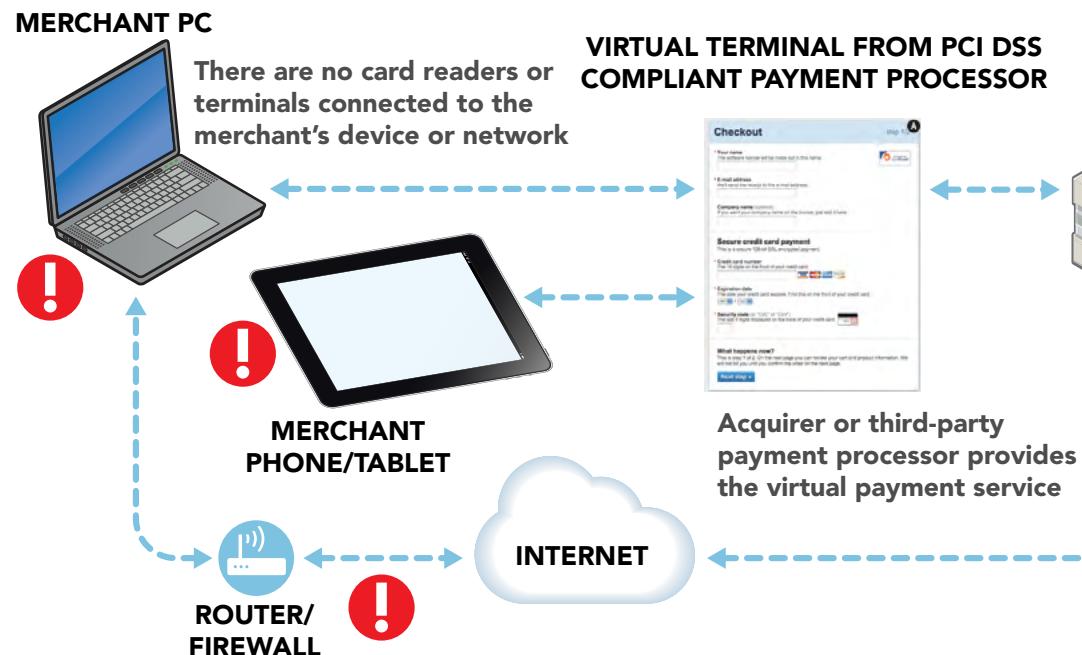
I'm not positive this is my payment system. Show me the overview again

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.



# Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

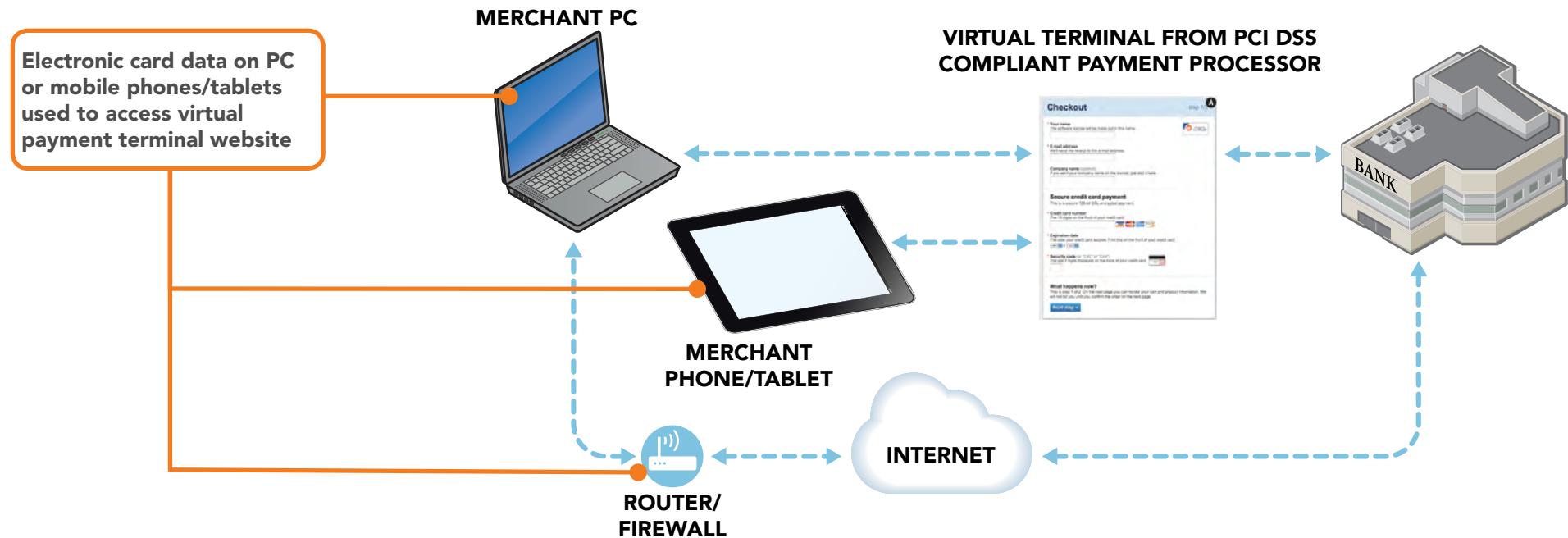
TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

## Where is your card data at risk?





# Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

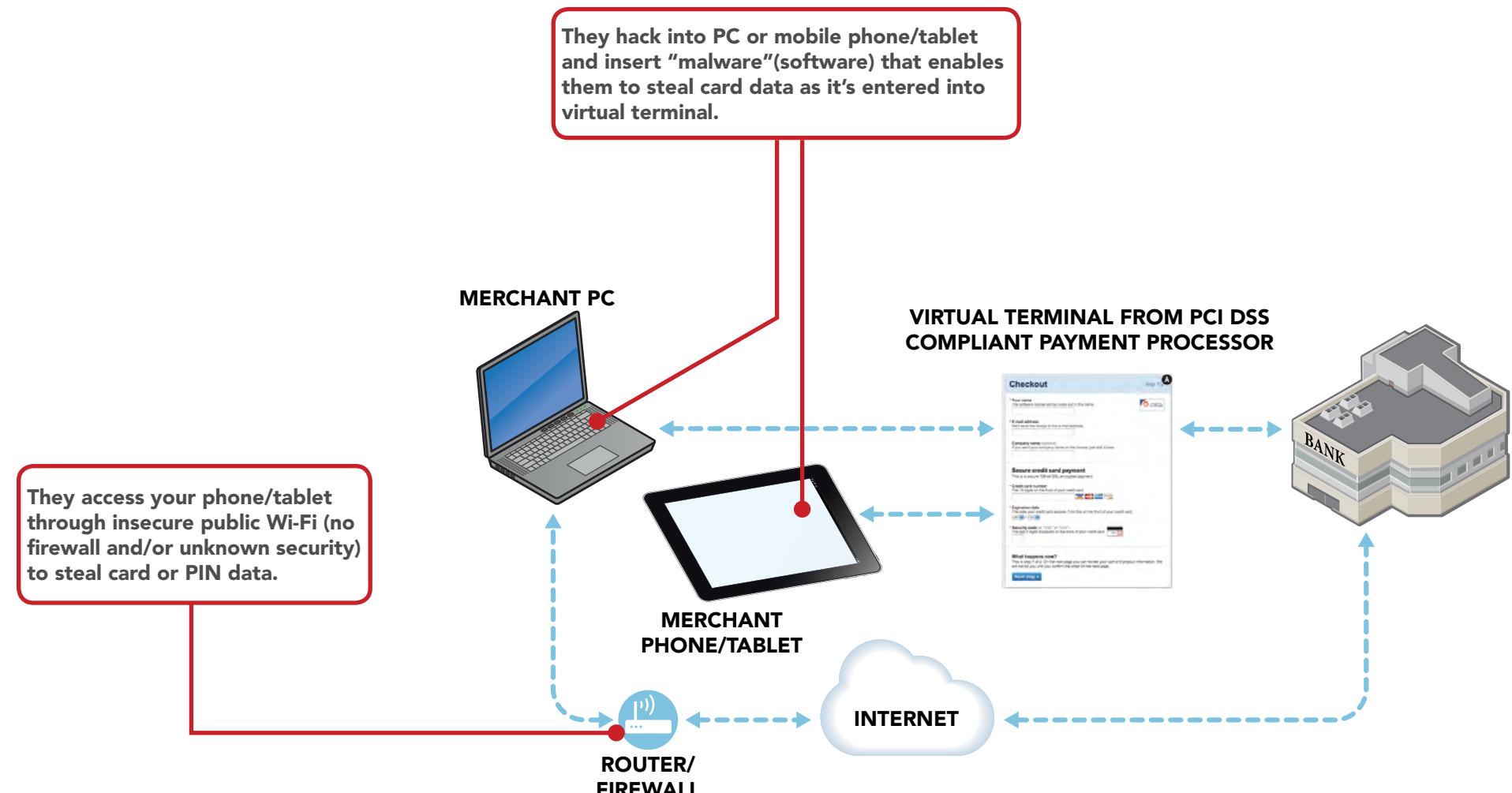
TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

## How do criminals get your card data?





# Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

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



Use strong passwords



Install patches from your payment terminal vendor



Use anti-virus software



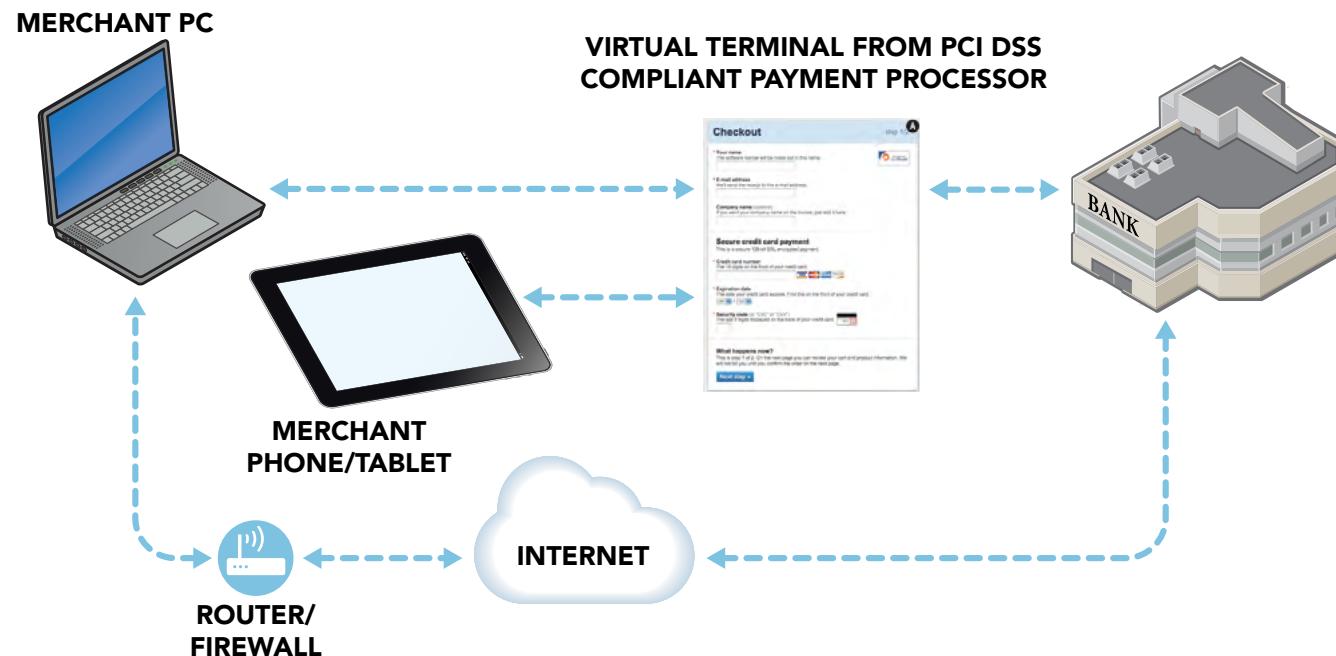
Get regular vulnerability scanning



Ask your vendor partners for help if you need it



Limit remote access for your vendor partners - don't give hackers easy access



\*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.

## TYPE 15 OVERVIEW

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.

## TYPE 15 RISKS

## TYPE 15 THREATS

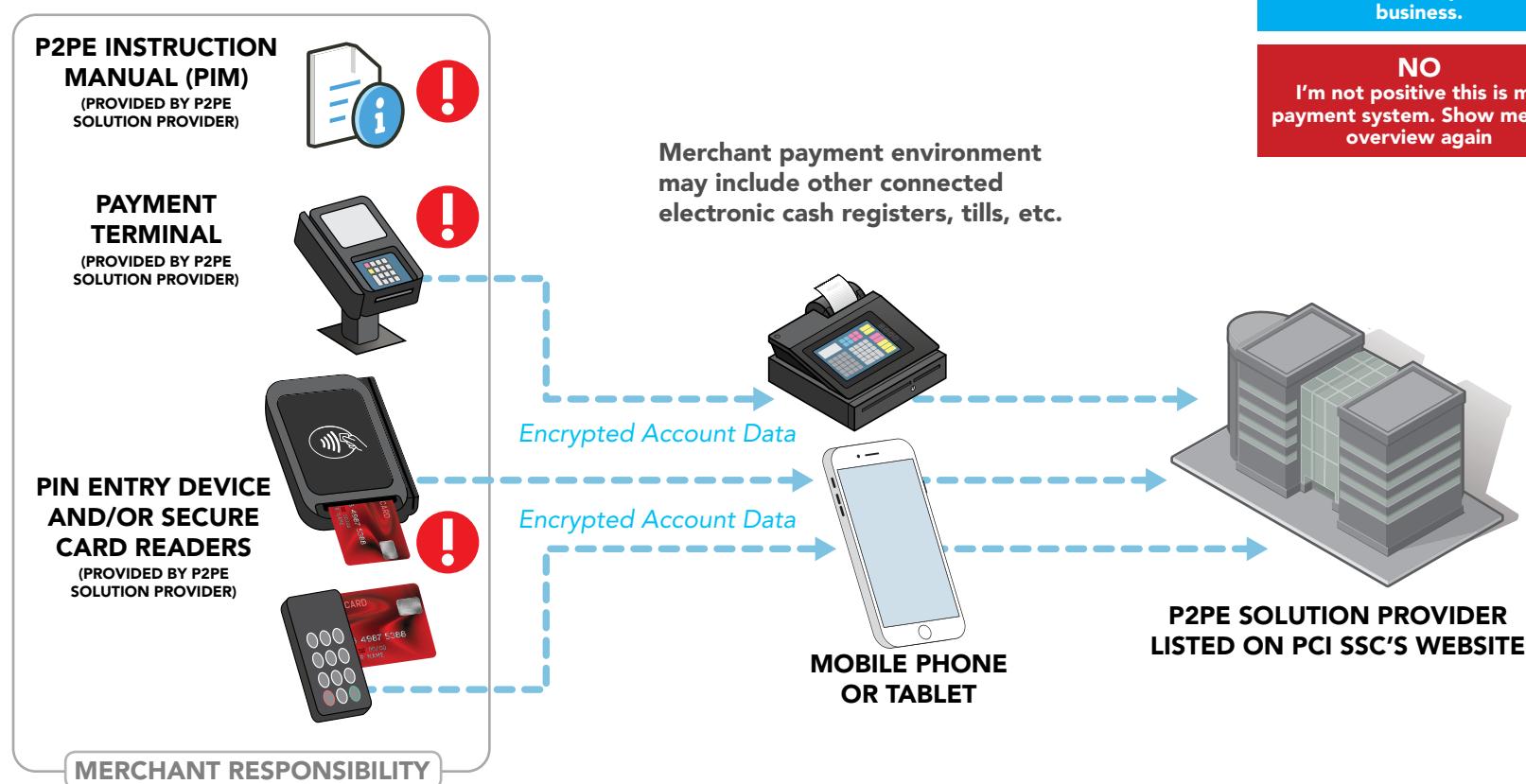
## TYPE 15 PROTECTIONS

**YES**

This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

**NO**

I'm not positive this is my payment system. Show me the overview again



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.

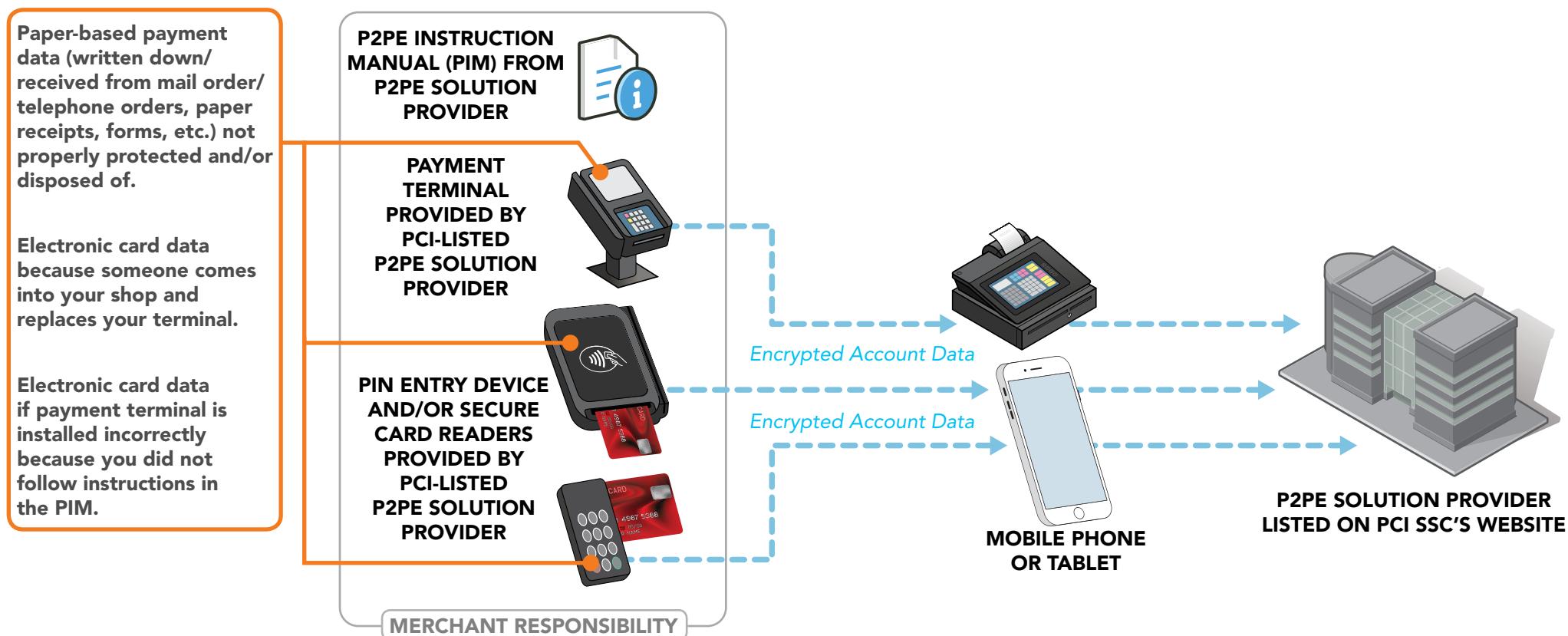
TYPE 15 OVERVIEW

TYPE 15 RISKS

TYPE 15 THREATS

TYPE 15 PROTECTIONS

## Where is your card data at risk?





# Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

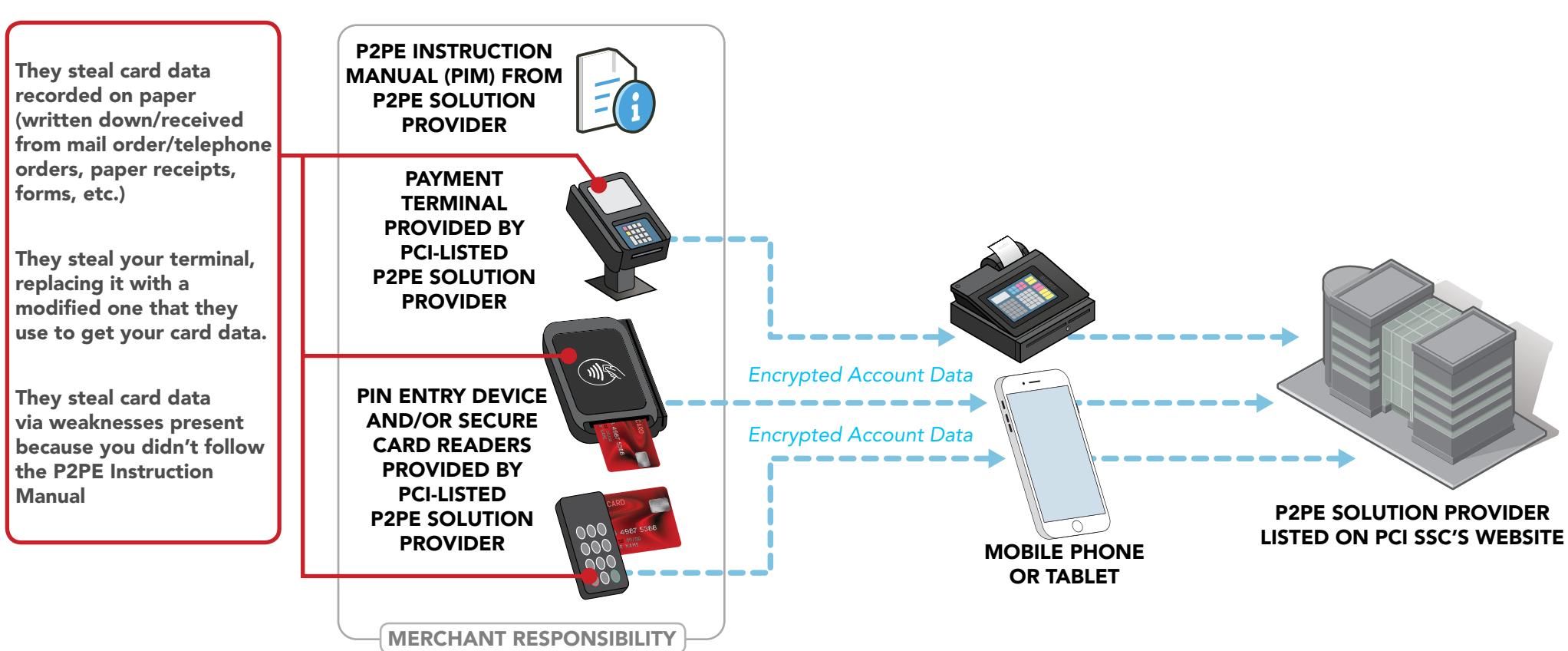
TYPE 15 OVERVIEW

TYPE 15 RISKS

TYPE 15 THREATS

TYPE 15 PROTECTIONS

## How do criminals get your card data?





# Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

TYPE 15 OVERVIEW

TYPE 15 RISKS

TYPE 15 THREATS

TYPE 15 PROTECTIONS

## 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



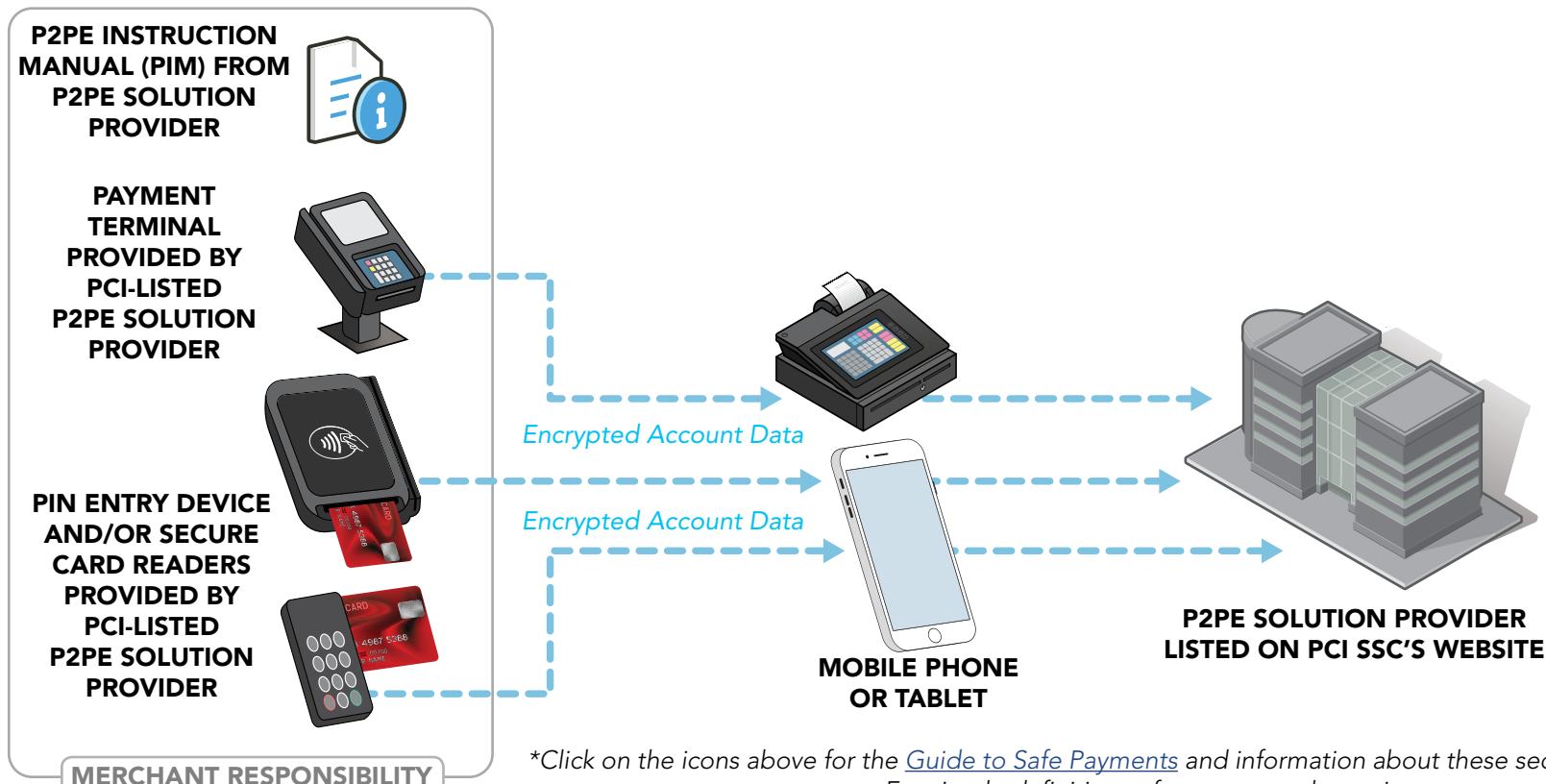
Ask your vendor partners for help if you need it



Protect in-house access to your card data



Make your card data useless to criminals



# Resources

## Infographics and Videos

Resource	Link	URL
Infographic: It's Time to Change Your Password	<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>	
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves	<a href="https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf">https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf</a>	
Video: Learn Password Security in 2 Minutes	<a href="https://www.youtube.com/watch?v=FsrOXgZKa7U">https://www.youtube.com/watch?v=FsrOXgZKa7U</a>	
Infographic: PCI Firewall Basics	<a href="https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf">https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf</a>	
Video: Passwords	<a href="https://www.youtube.com/watch?v=dNVQk65KL8g">https://www.youtube.com/watch?v=dNVQk65KL8g</a>	
Infographic: Passwords	<a href="https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf">https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf</a>	
Video: Patching	<a href="https://www.youtube.com/watch?v=0NGz1mGO3Jg">https://www.youtube.com/watch?v=0NGz1mGO3Jg</a>	
Infographic: Patching	<a href="https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Patching.pdf">https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Patching.pdf</a>	
Video: Remote Access	<a href="https://www.youtube.com/watch?v=MxgSNFgvAVc">https://www.youtube.com/watch?v=MxgSNFgvAVc</a>	
Infographic: Remote Access	<a href="https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Secure-Remote-Access.pdf">https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Secure-Remote-Access.pdf</a>	

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

Resource	Link	URL
Common Payment Systems	<a href="https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf">https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf</a>	
Small Merchant Questions for Vendors	<a href="https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf">https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf</a>	
Small Merchant Glossary	<a href="https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf">https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf</a>	
Evaluation Tool: Acquirer Overview	<a href="https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Acquirers.pdf">https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Acquirers.pdf</a>	
Evaluation Tool: Small Merchant Overview	<a href="https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf">https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf</a>	