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

Common Payment Systems

Version 3.0 | April 2024

PCI Security Standards Council®

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.

PCI Security Standards Council®

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

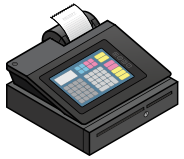
Note that these are preliminary results. *You cannot submit the evaluation from PCI SSC's website, nor does PCI SSC submit it on your behalf.* **You must contact your merchant bank and follow their completion and submission instructions.**

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; may also be known as POS System) 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.

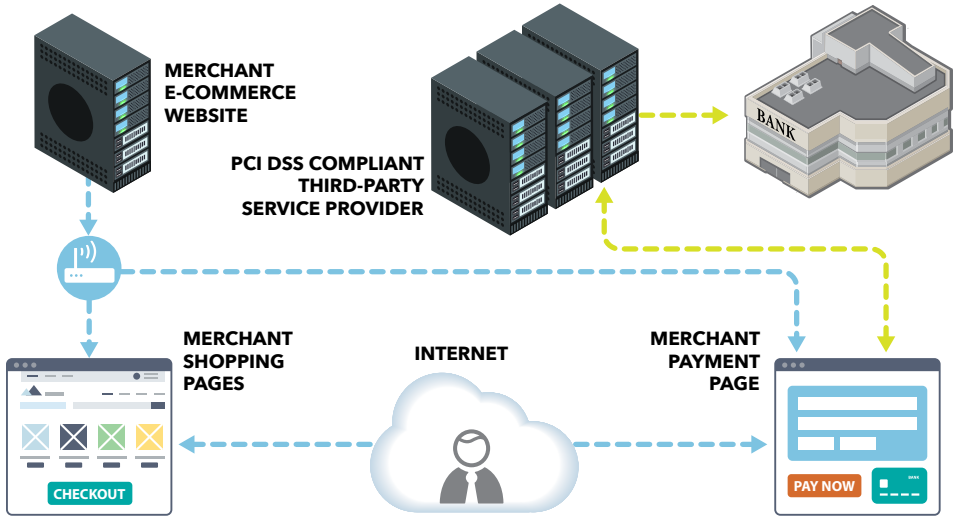
Understanding your E-commerce Payment System

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.



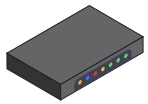
An **E-COMMERCE PAYMENT SYSTEM** encompasses the entire process for a customer to select products or services and for the e-commerce merchant to accept card payments, including a website with shopping pages and a payment page or form, other connected devices or systems (for example Wi-Fi or a PC used 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.

Understanding your Petroleum & Fuel System

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

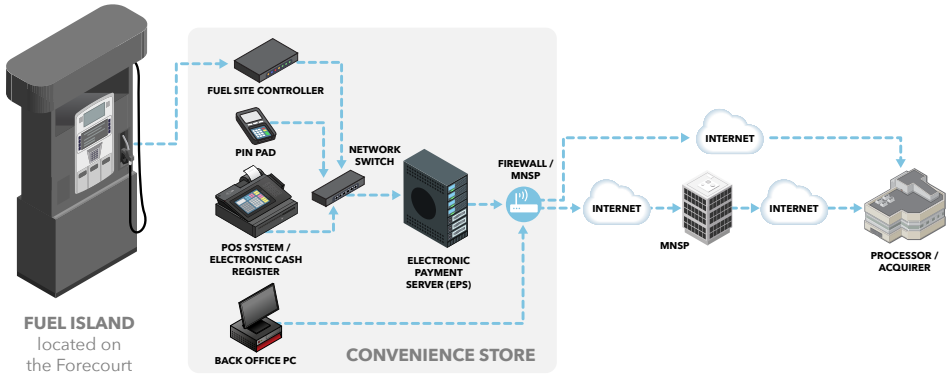
A **PETROLEUM SYSTEM** encompasses the entire process for a consumer to purchase petroleum, either outside at an unattended Fuel Island or inside at a POS Terminal.

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



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

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



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

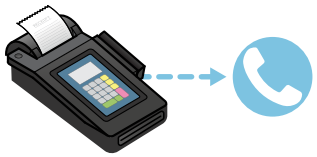
A **BACK OFFICE PC** is a dedicated personal computer used to manage nonconsumer business operations for a convenience and retail fuel site. The back office system supports daily operational activities such as inventory management, price book, product supply, fuel management, site-level accounting, and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

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

Payment system types at-a-glance

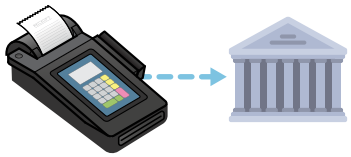
How do you accept payments?

Review all payment diagrams that apply to how your business accepts payments



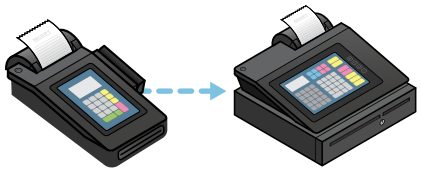
You accept payments with a standalone, dial-up payment terminal

TYPES 1, 2



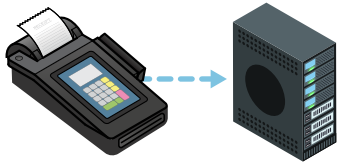
You accept payments with a payment device connected only to a processor

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

You accept payments via a petroleum system

TYPE 16

TYPE 1

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

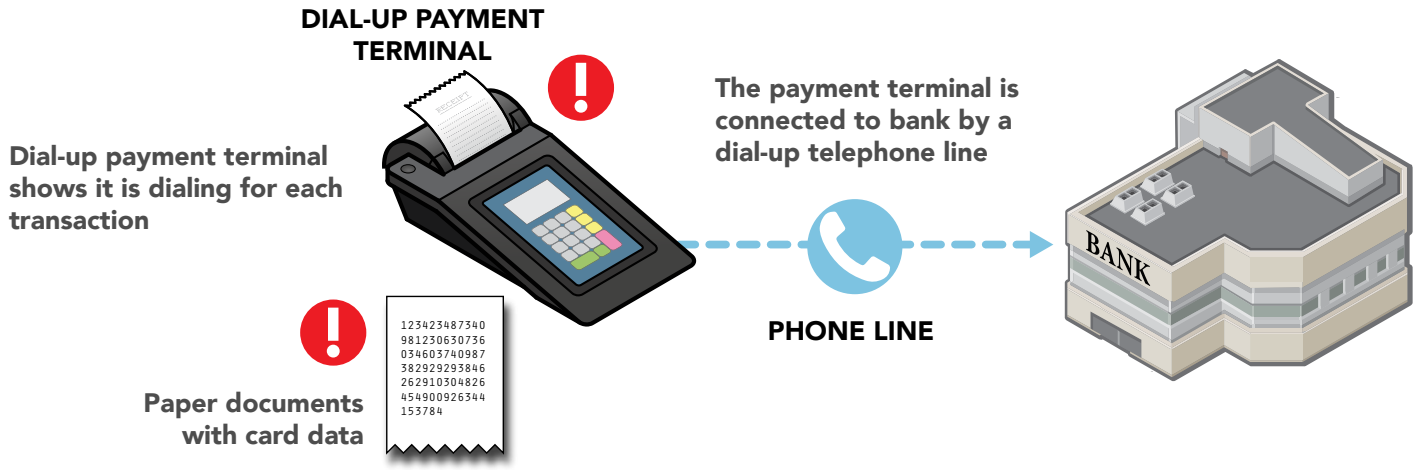
RISK PROFILE

LOWER

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



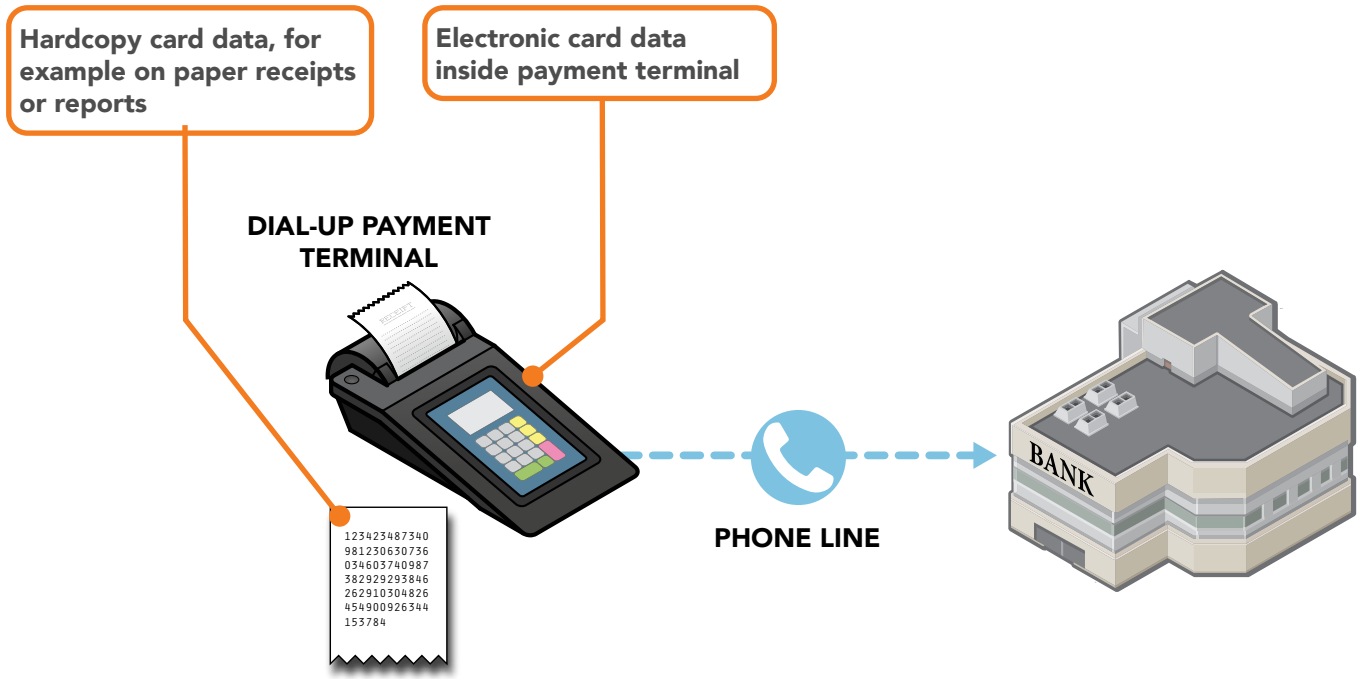
For this scenario, risks to card data are present at ! above. Risks explained on next page.

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

RISK PROFILE

LOWER

Where is your card data at risk?



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

RISK PROFILE

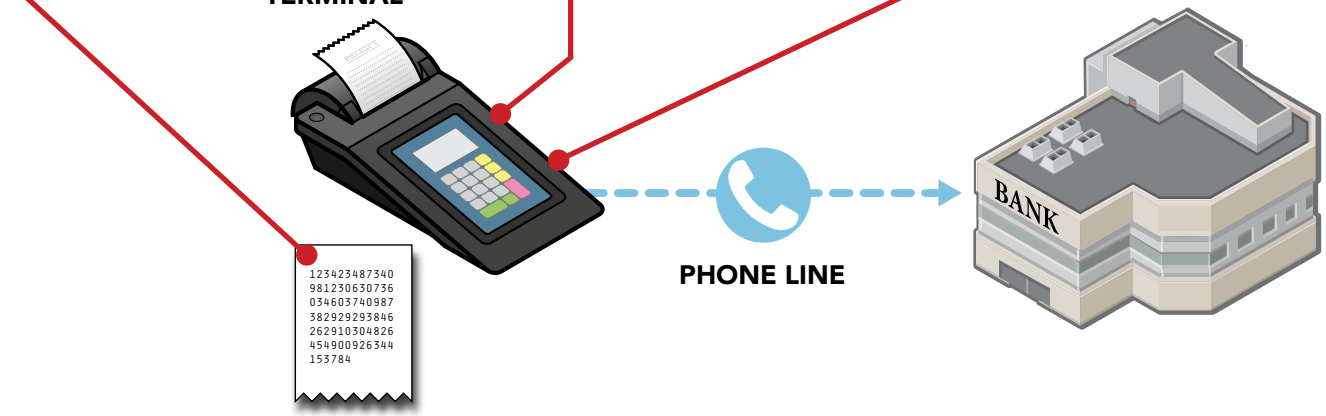
LOWER

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.



TYPE 1

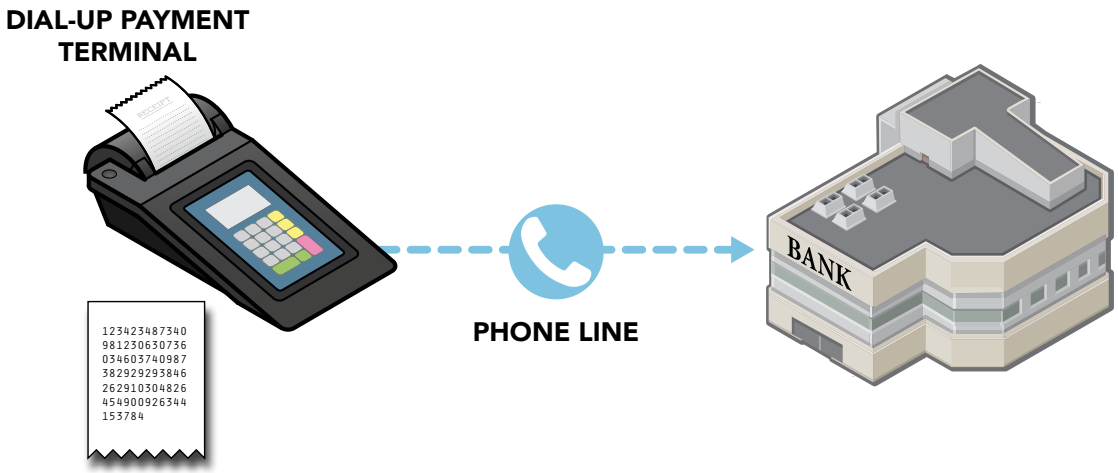
Dial-up payment terminal. Payments sent via phone line.

RISK PROFILE

LOWER

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.

TYPE 2

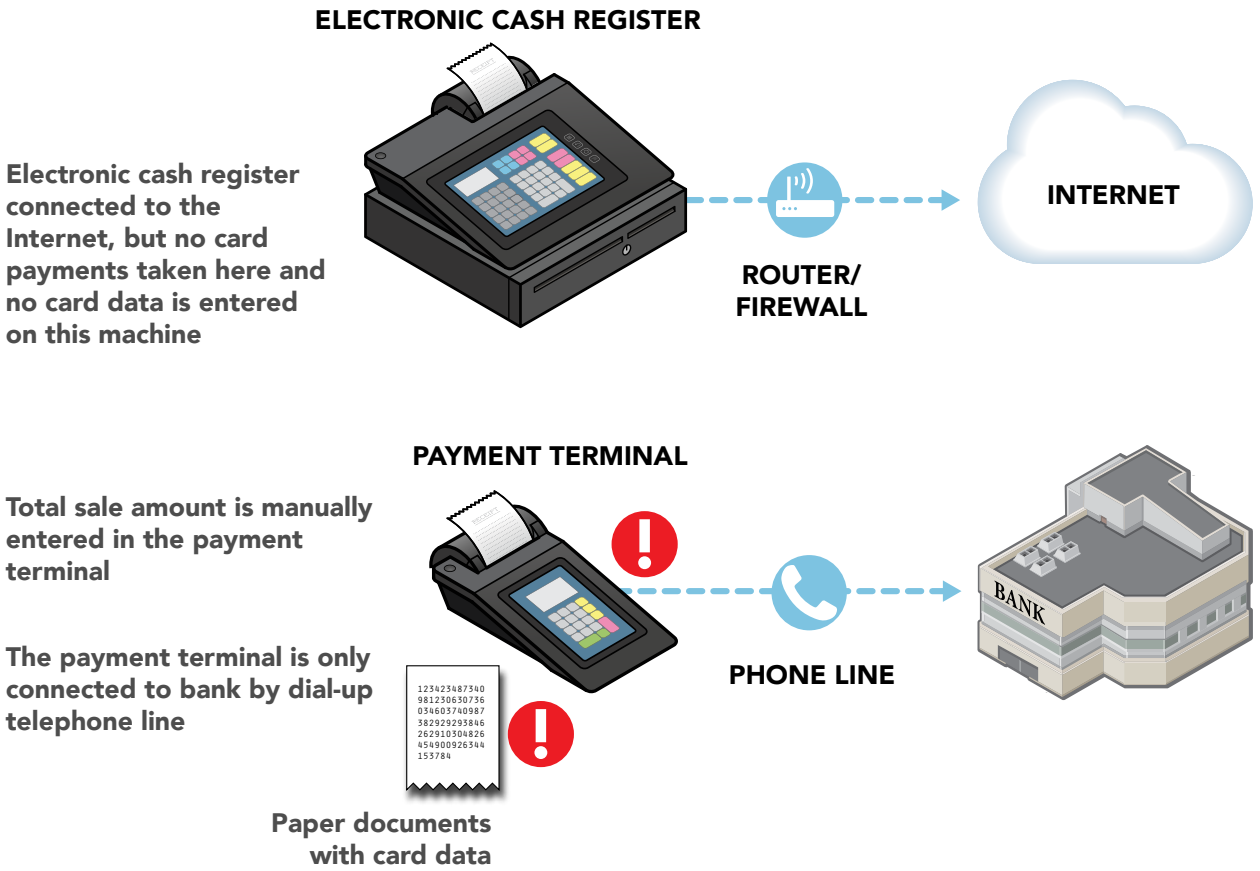
Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.

RISK PROFILE

LOWER

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



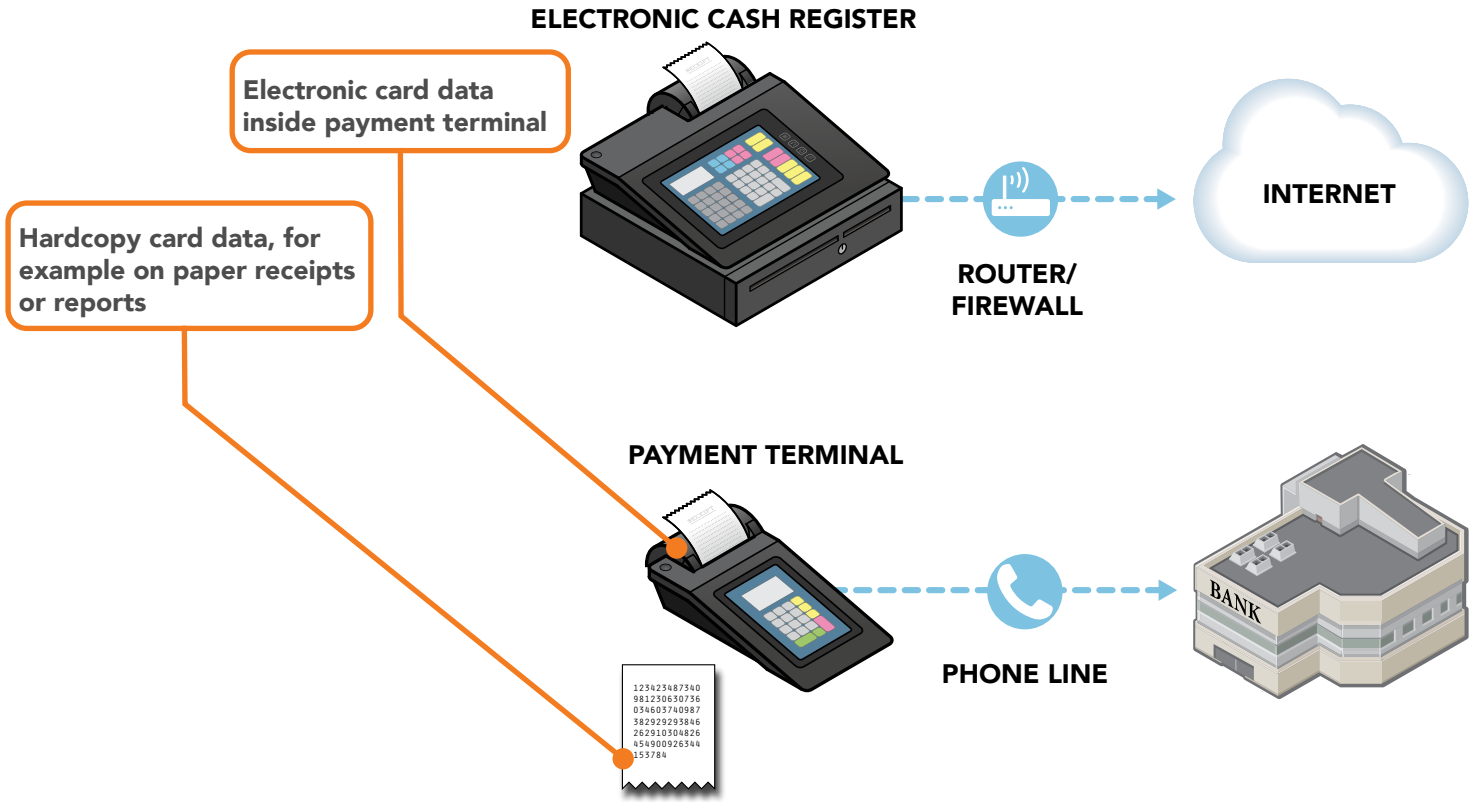
For this scenario, risks to card data are present at ❗ above. Risks explained on next page.

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

RISK PROFILE

LOWER

Where is your card data at risk?



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

RISK PROFILE

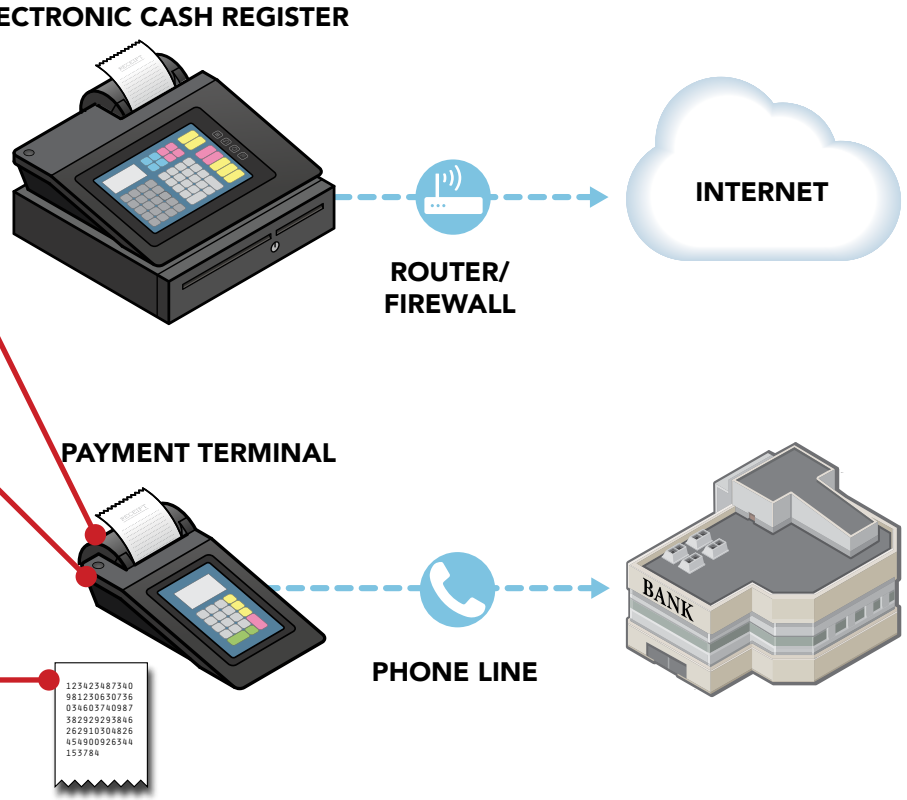
LOWER

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.



TYPE 2

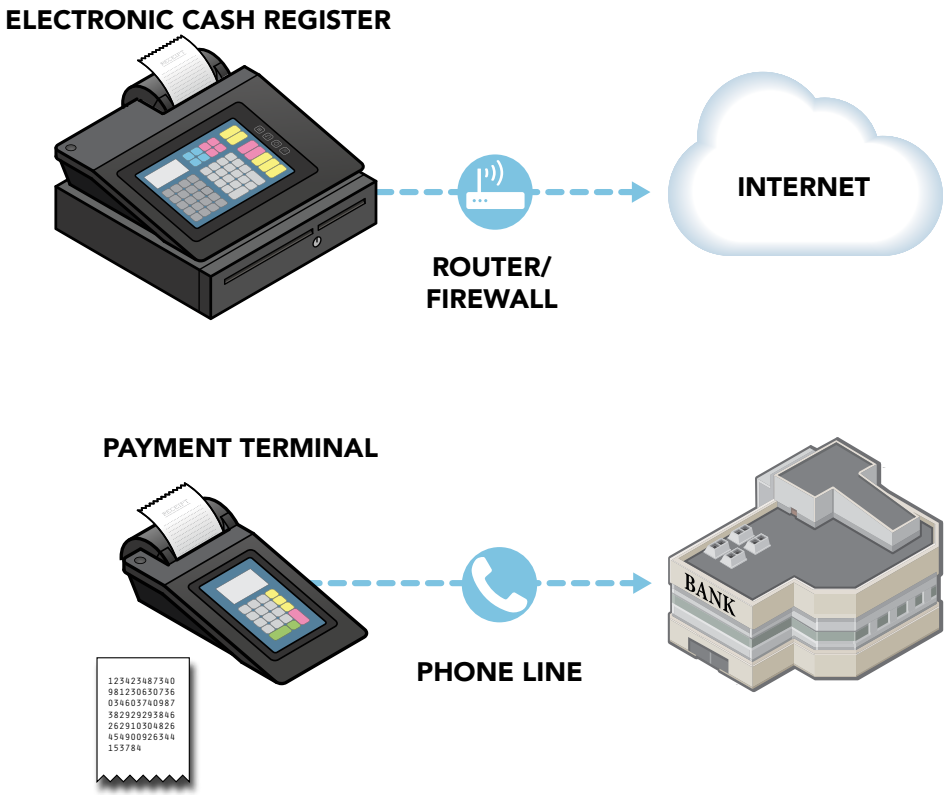
Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.

RISK PROFILE

LOWER

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.*

TYPE 3 — Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

RISK PROFILE

Is card data encrypted?

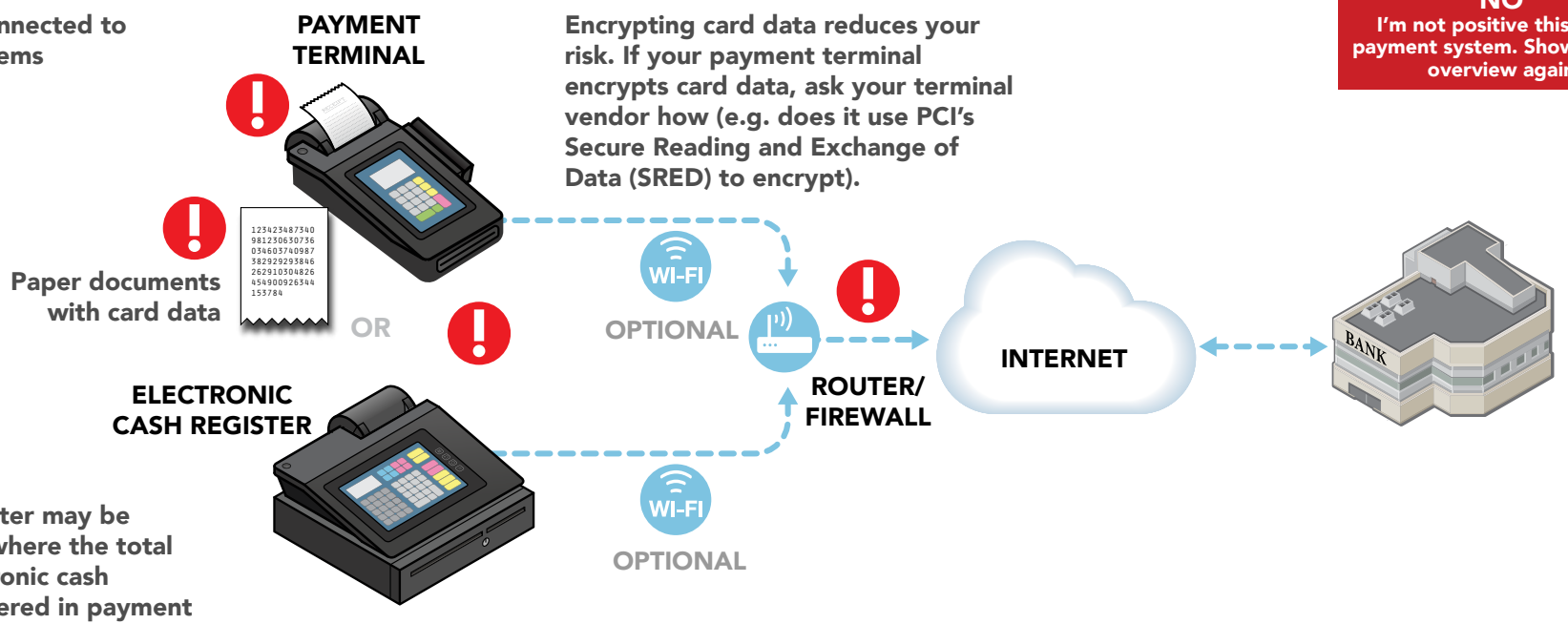
YES NO

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

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).

An 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.

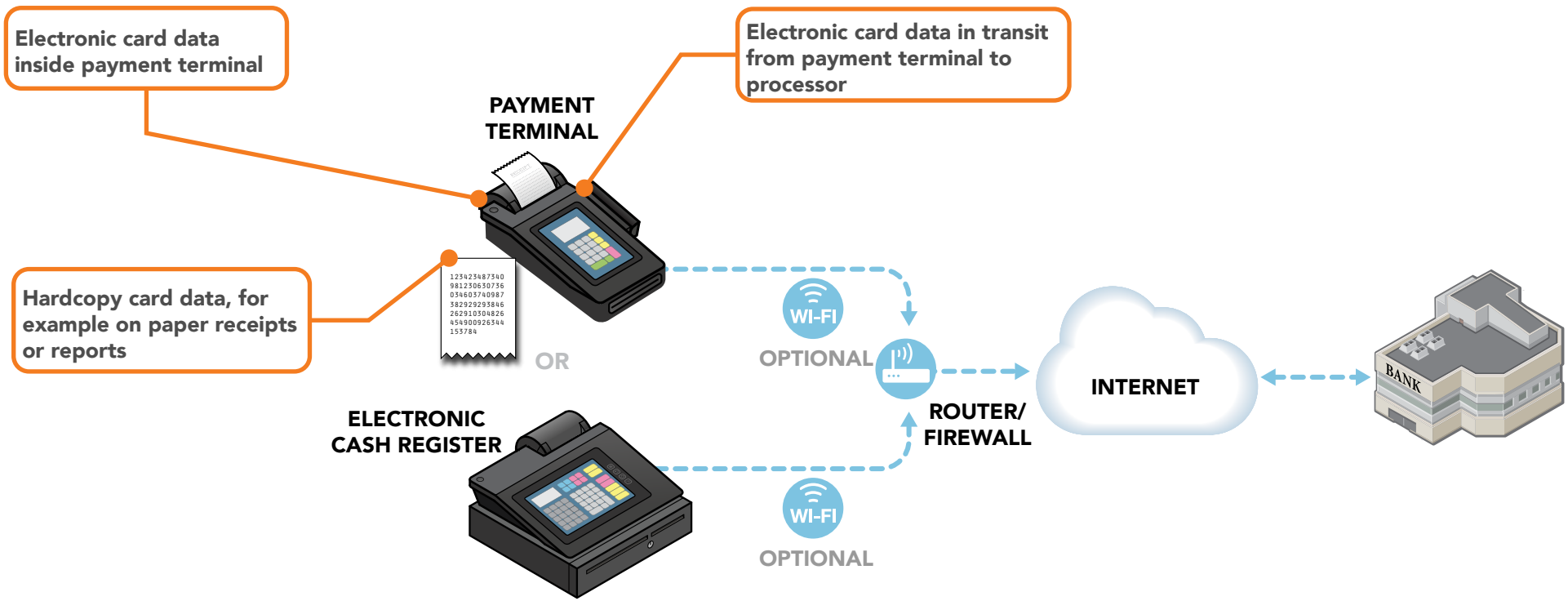
Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

RISK PROFILE

Is card data encrypted?

YES NO

Where is your card data at risk?



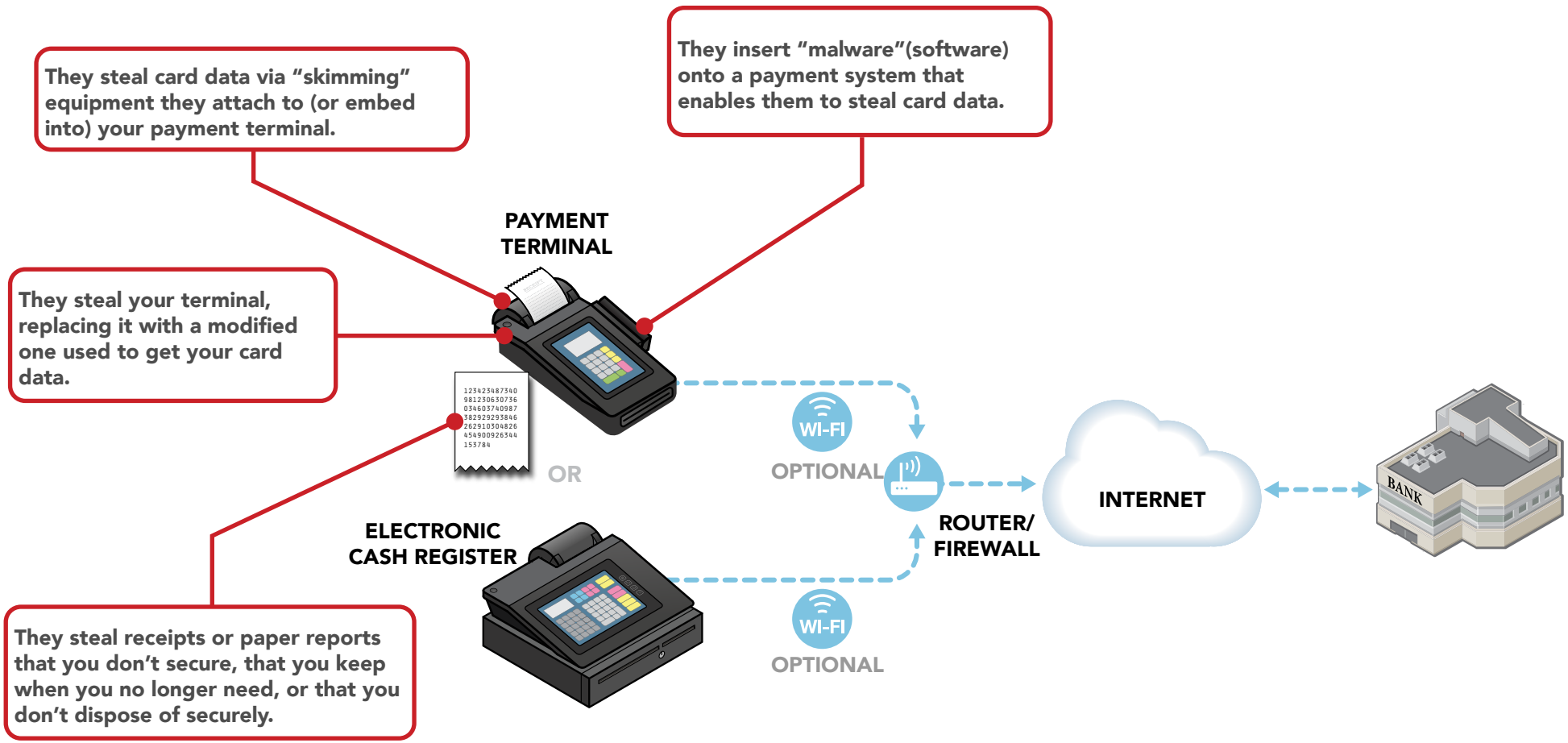
Payment terminal and electronic cash register separately connected to the Internet. Payments sent via Internet by payment terminal.

RISK PROFILE

Is card data encrypted?

YES NO

How do criminals get your card data?



TYPE 3

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

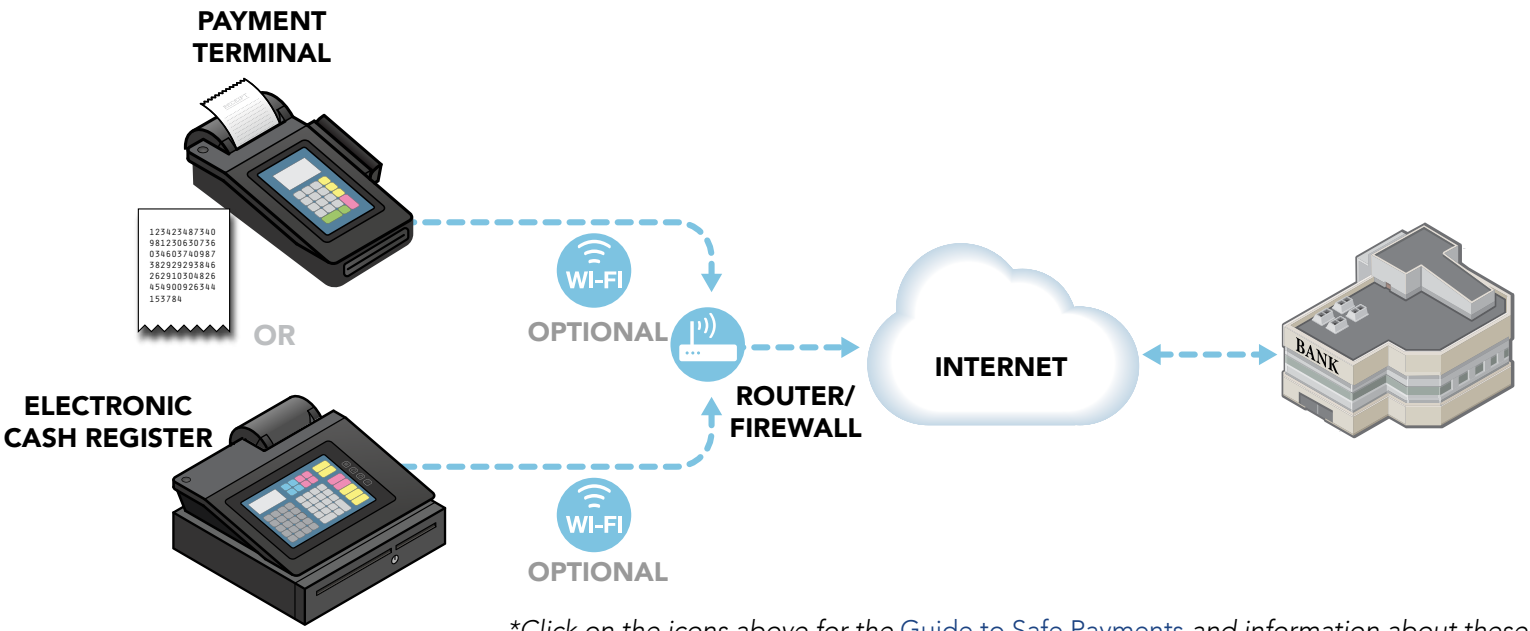
RISK PROFILE

Is card data encrypted?

YES NO

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.

TYPE 4

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

RISK PROFILE

Is card data encrypted?

YES NO

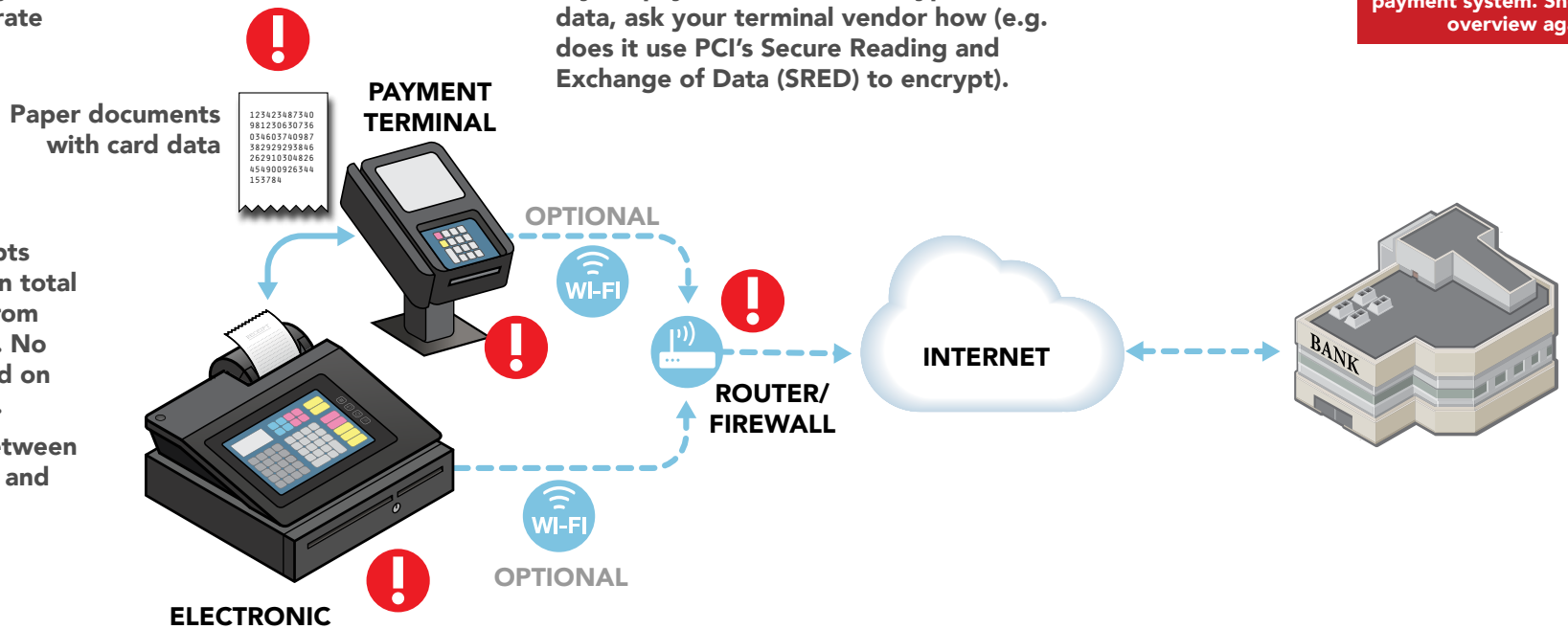
If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

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

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

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.

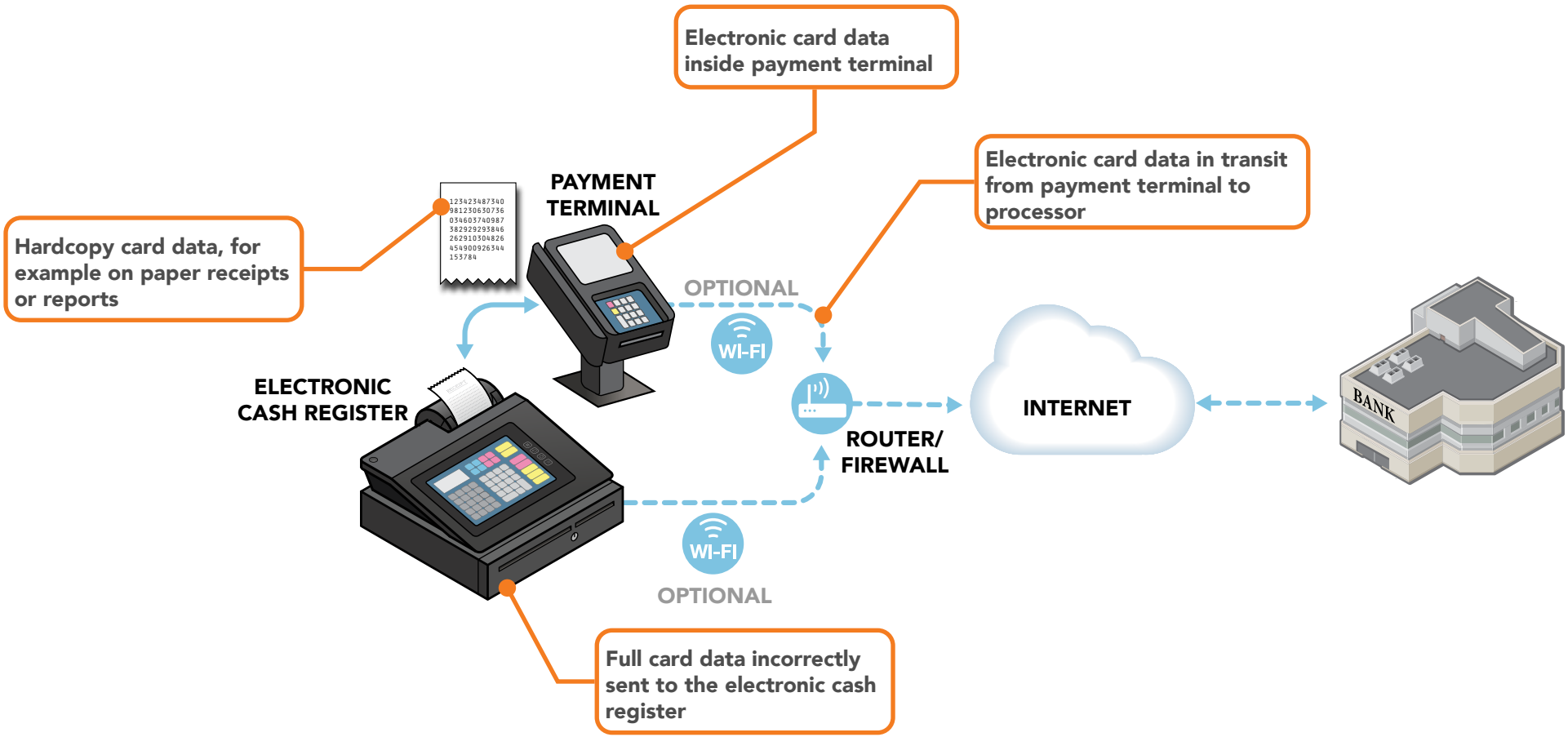
TYPE 4

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

RISK PROFILE

Is card data encrypted?

Where is your card data at risk?



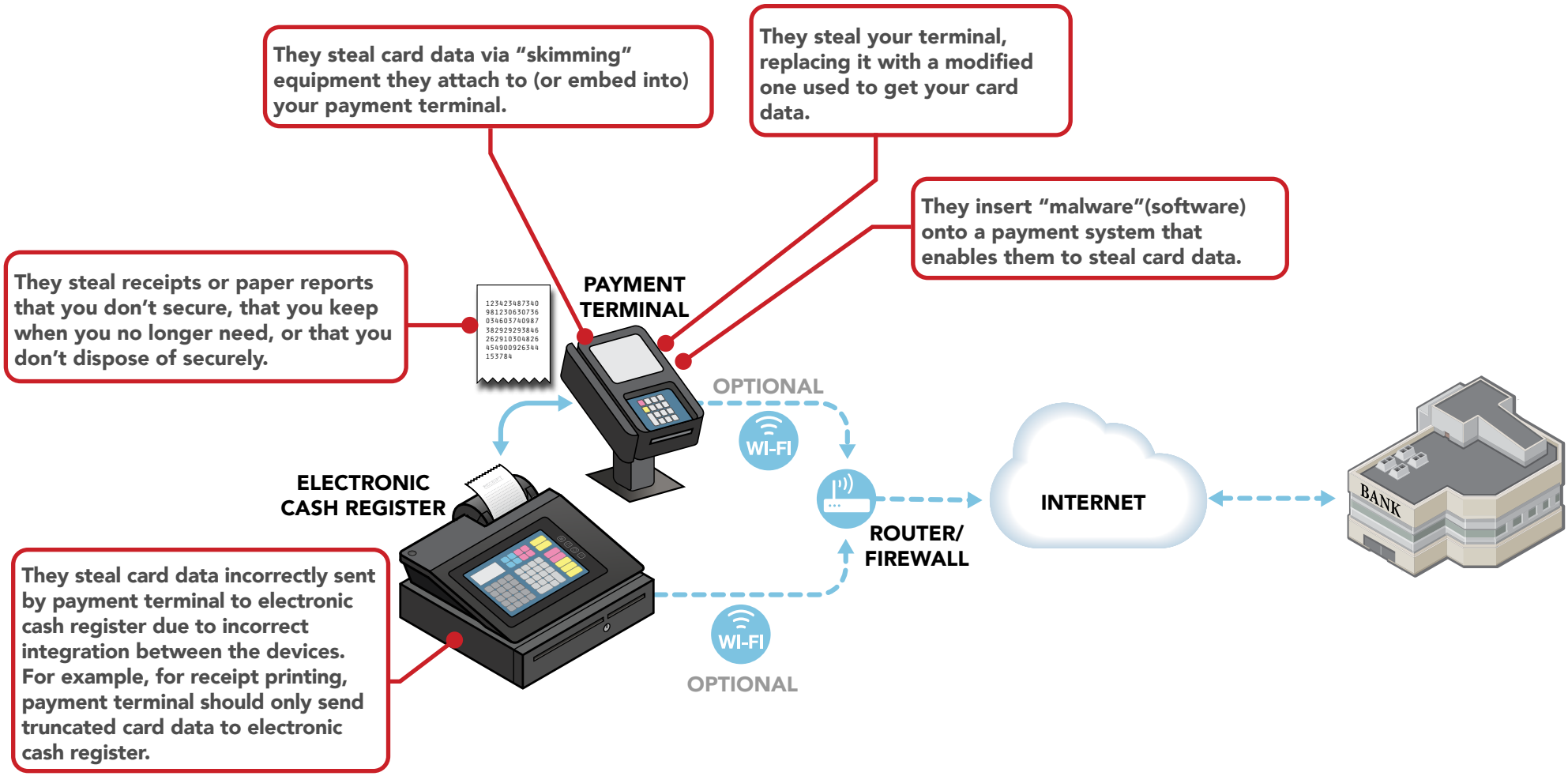
Payment terminal and electronic cash register share non-card data. Payment sent via Internet by payment terminal.

RISK PROFILE

Is card data encrypted?

YES NO

How do criminals get your card data?



TYPE 4

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

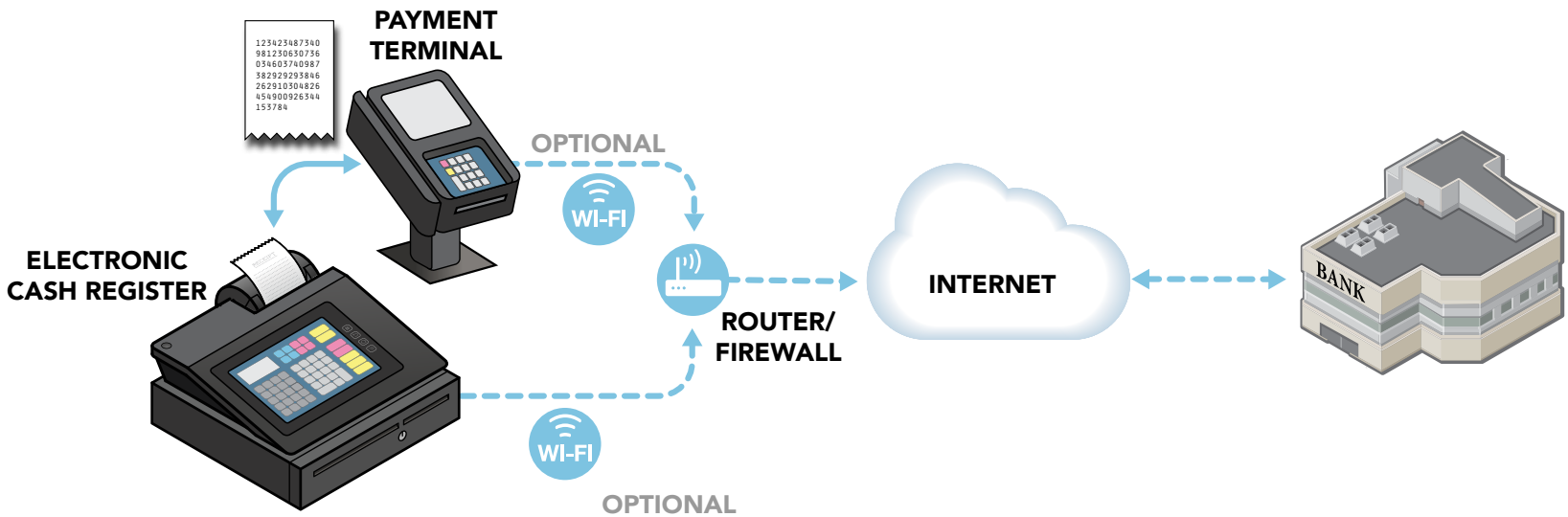
RISK PROFILE

Is card data encrypted?

YES NO

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.

TYPE 5

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

RISK PROFILE

Is card data encrypted?

YES NO

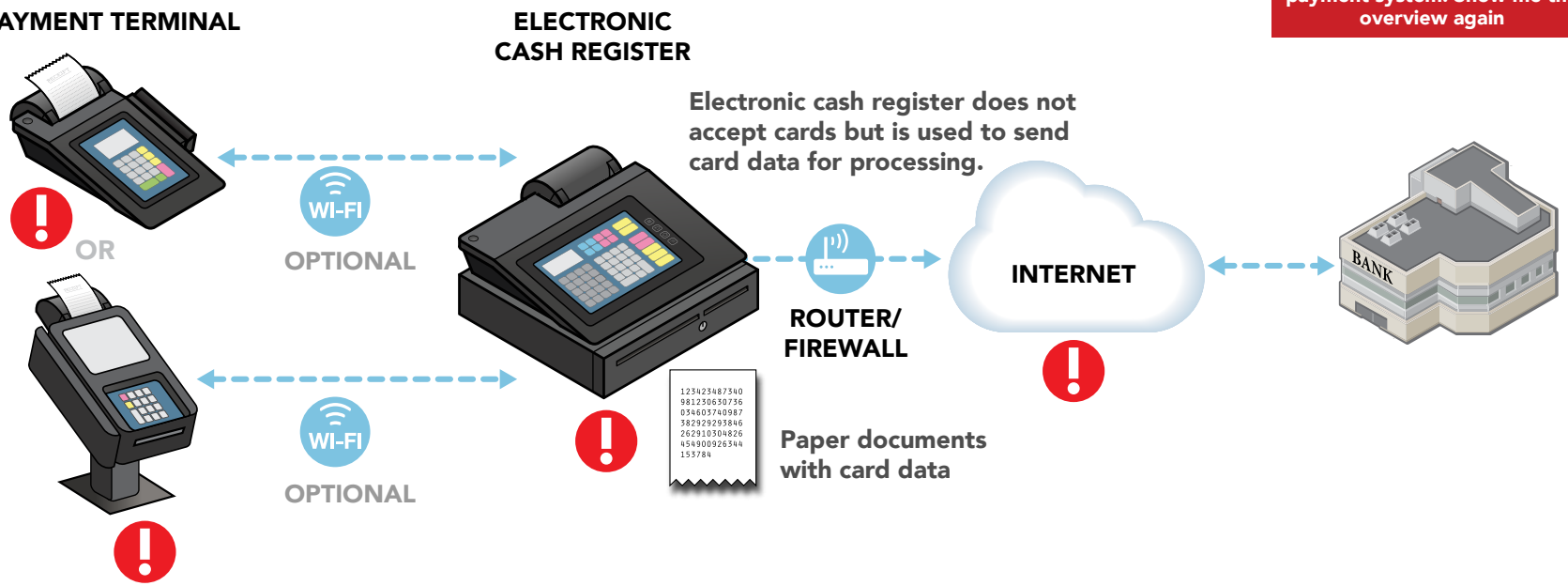
If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

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

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



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

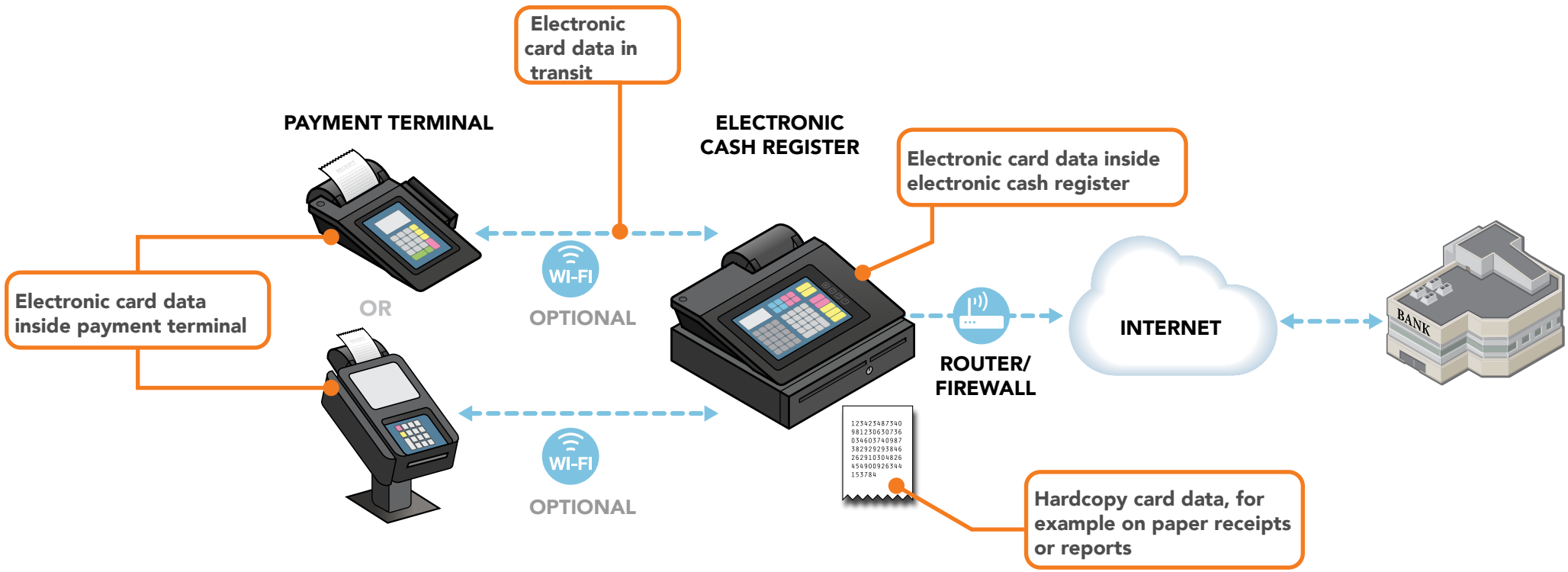
Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

RISK PROFILE

Is card data encrypted?

YES NO

Where is your card data at risk?



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

RISK PROFILE

Is card data encrypted?

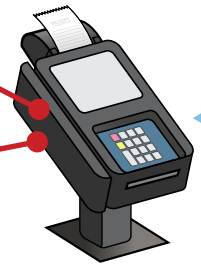
YES NO

How do criminals get your card data?

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

PAYMENT TERMINAL

OR



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

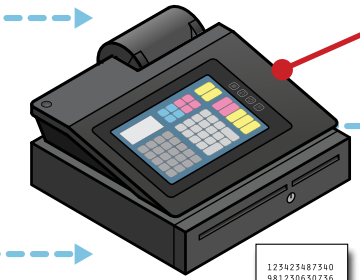
WI-FI

OPTIONAL

WI-FI

OPTIONAL

ELECTRONIC CASH REGISTER



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

ROUTER/ FIREWALL

INTERNET

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.

TYPE 5

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

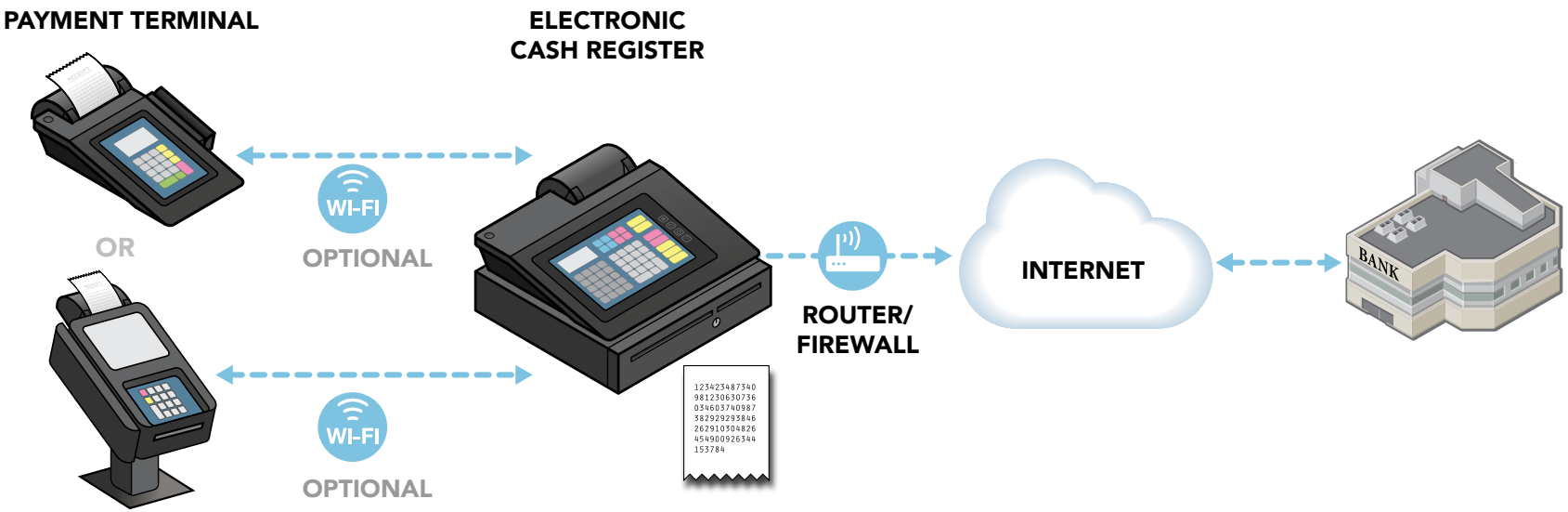
RISK PROFILE

Is card data encrypted?

YES NO

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.

TYPE 6

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

RISK PROFILE

Is card data encrypted?

YES NO

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

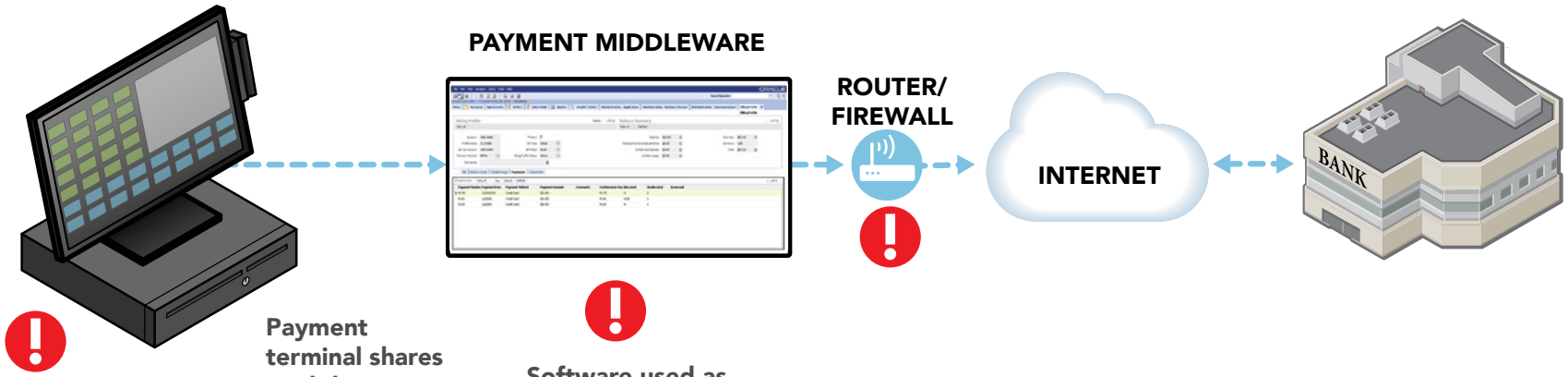
Payment terminal and electronic cash register combined

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).



Payment terminal shares card data with payment middleware

Software used as part of payment transaction

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

TYPE 6

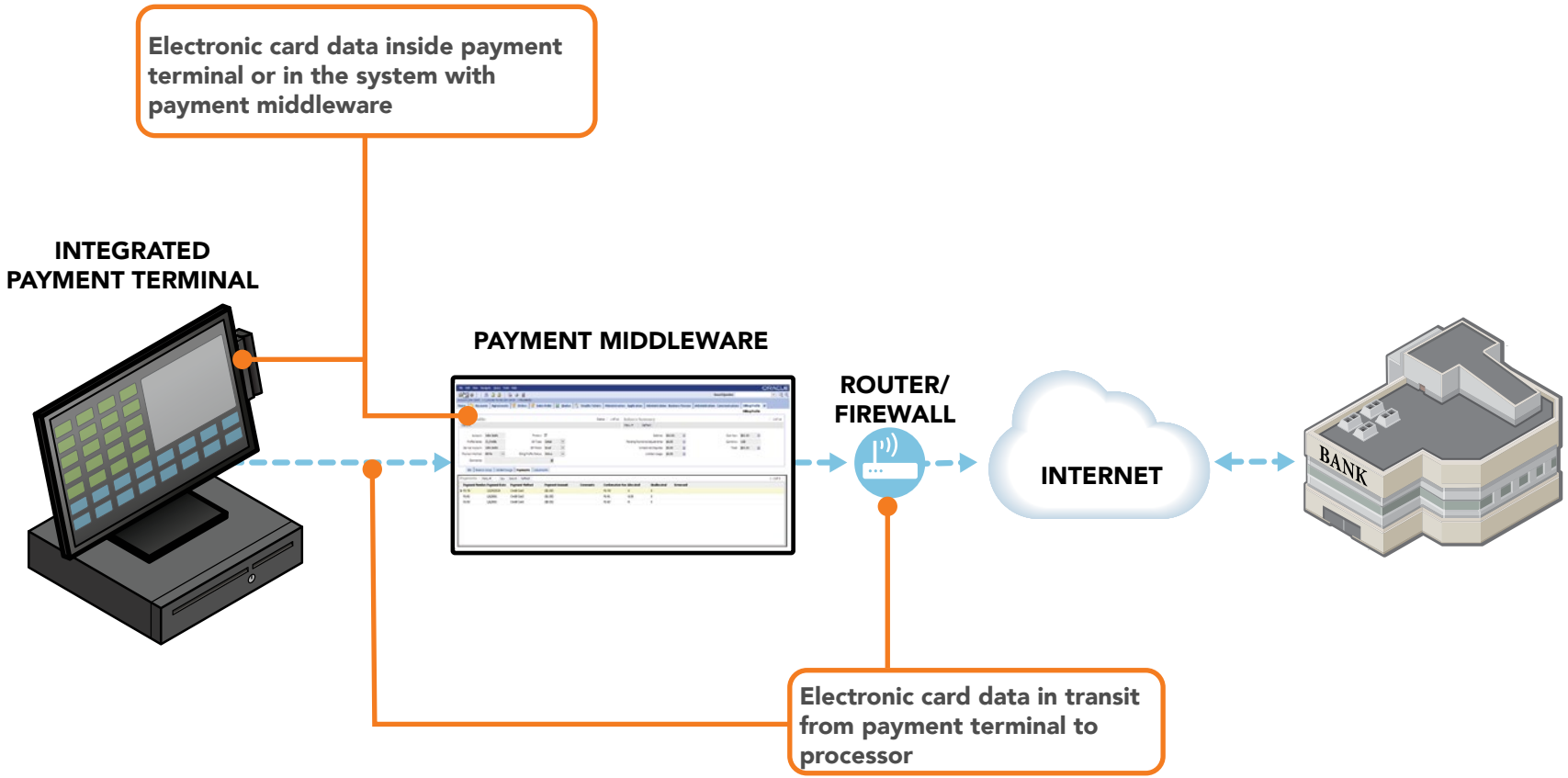
Integrated payment terminal and payment middleware share card data. Payments sent via Internet.

RISK PROFILE

Is card data encrypted?

YES NO

Where is your card data at risk?



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

RISK PROFILE

Is card data encrypted?

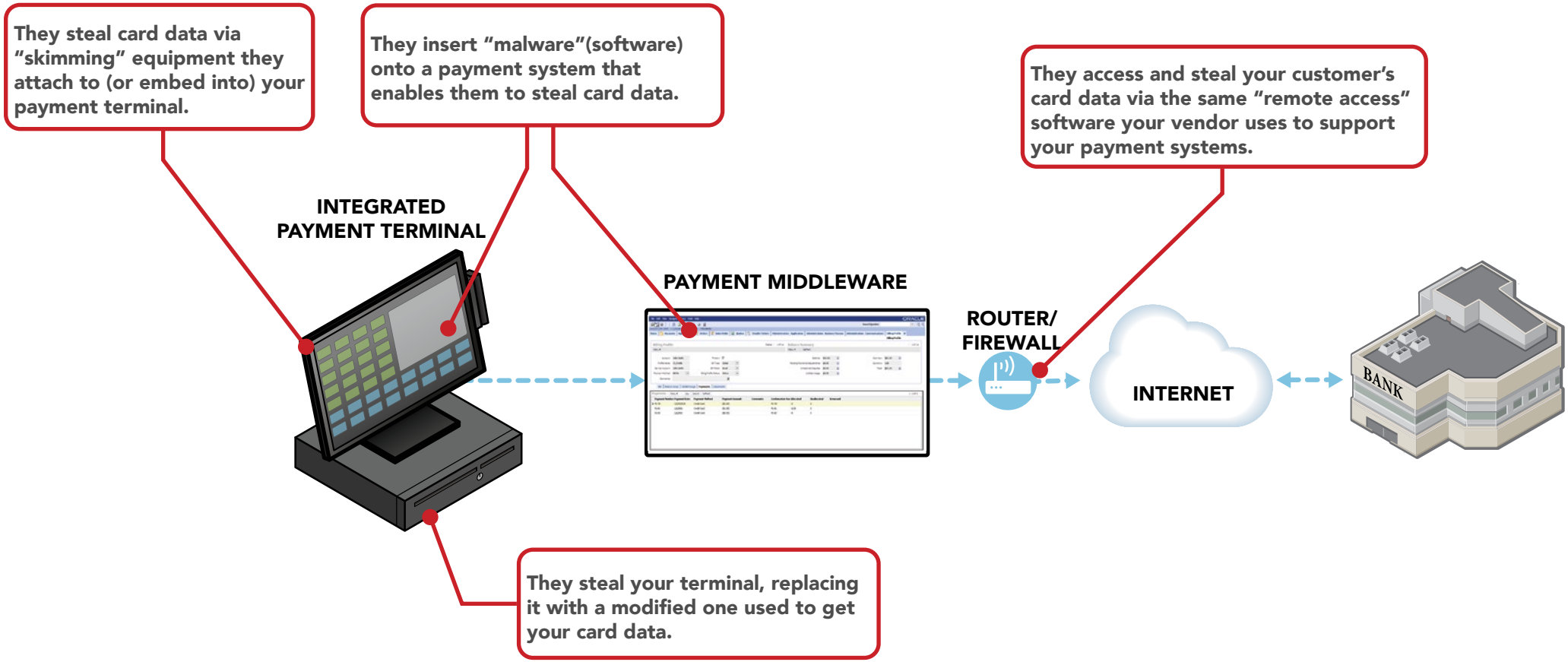
YES NO

How do criminals get your card data?

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

They 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.

TYPE 6

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

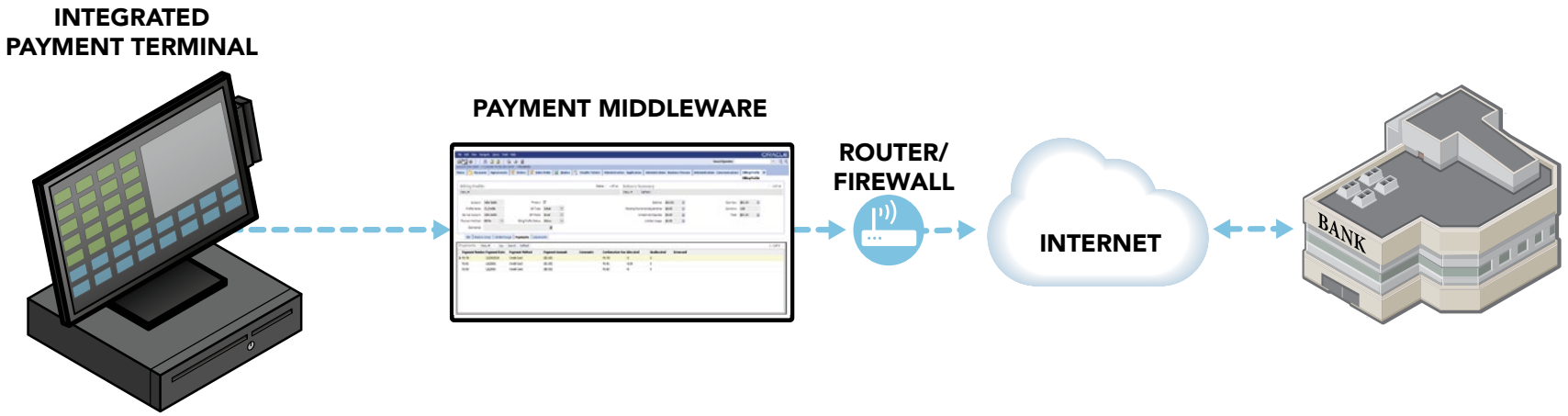
RISK PROFILE

Is card data encrypted?

YES NO

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.

TYPE 7

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

RISK PROFILE

Is card data encrypted?

YES NO

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

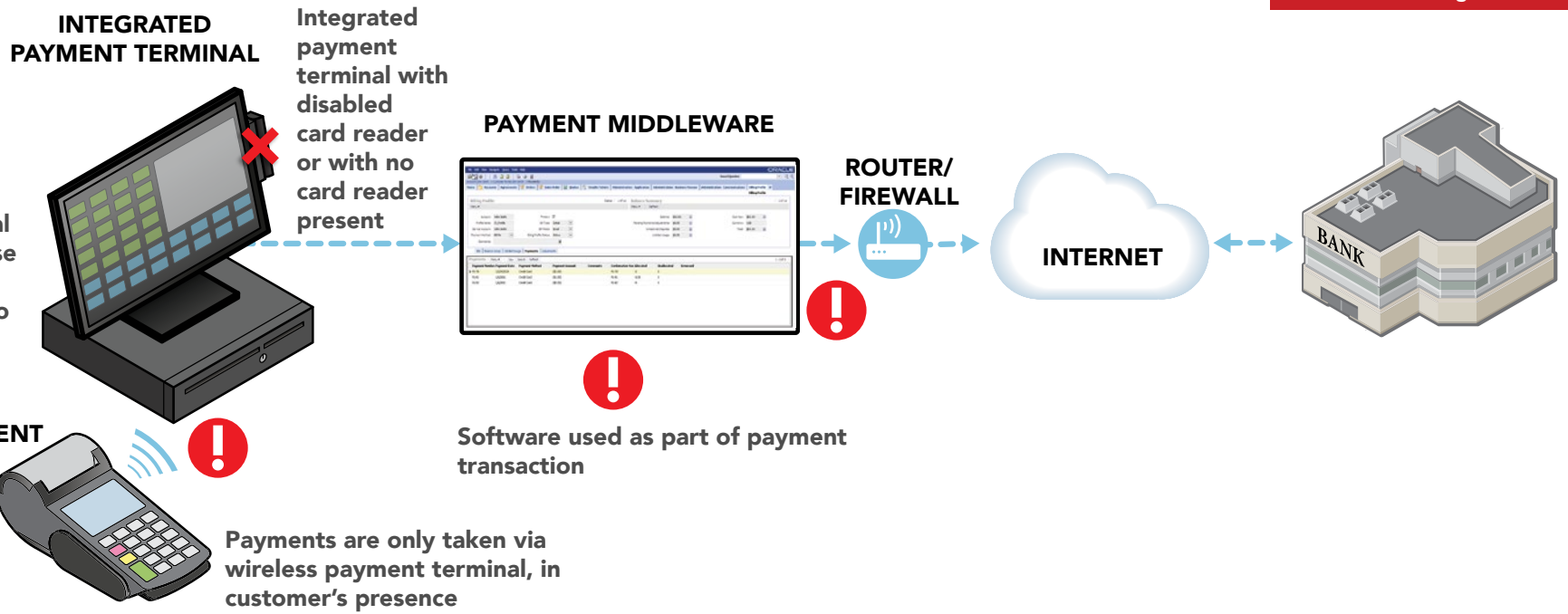
YES
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

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

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).



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

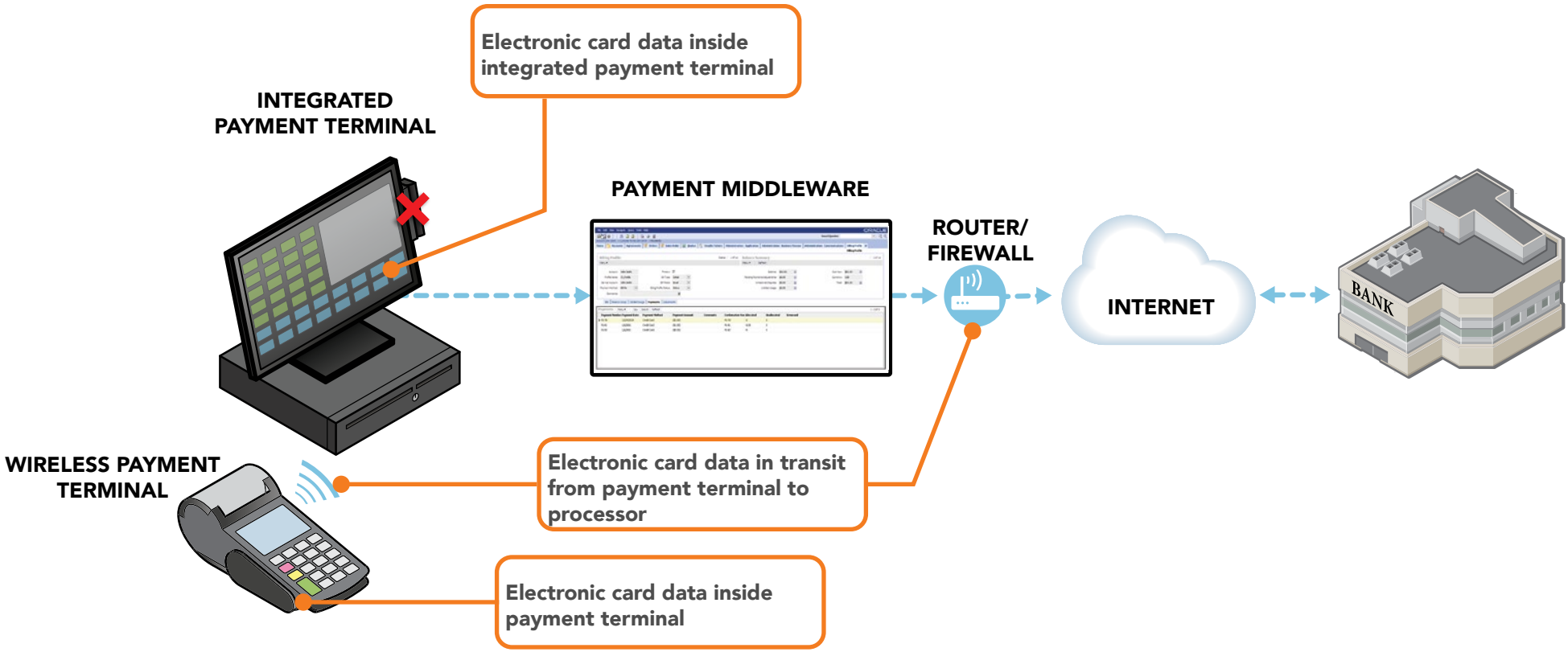
TYPE 7

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

RISK PROFILE

Is card data encrypted?

Where is your card data at risk?



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

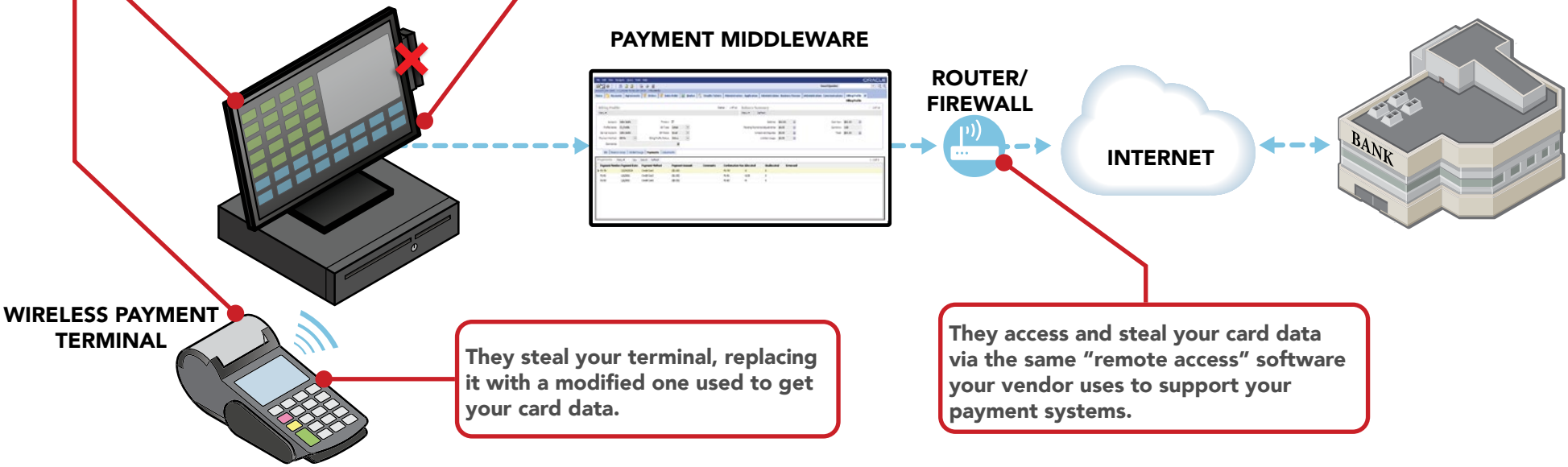
RISK PROFILE

Is card data encrypted?

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.

TYPE 7

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

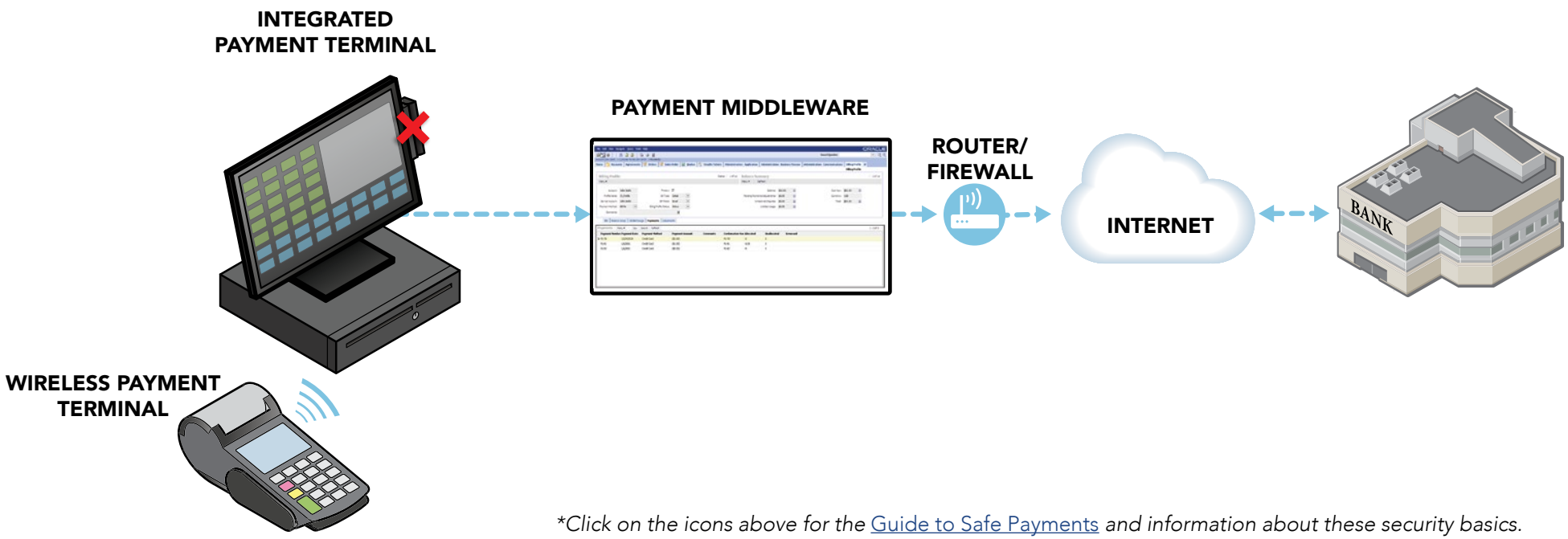
RISK PROFILE

Is card data encrypted?

YES NO

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.

TYPE 8

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

RISK PROFILE

Is card data encrypted?

YES NO

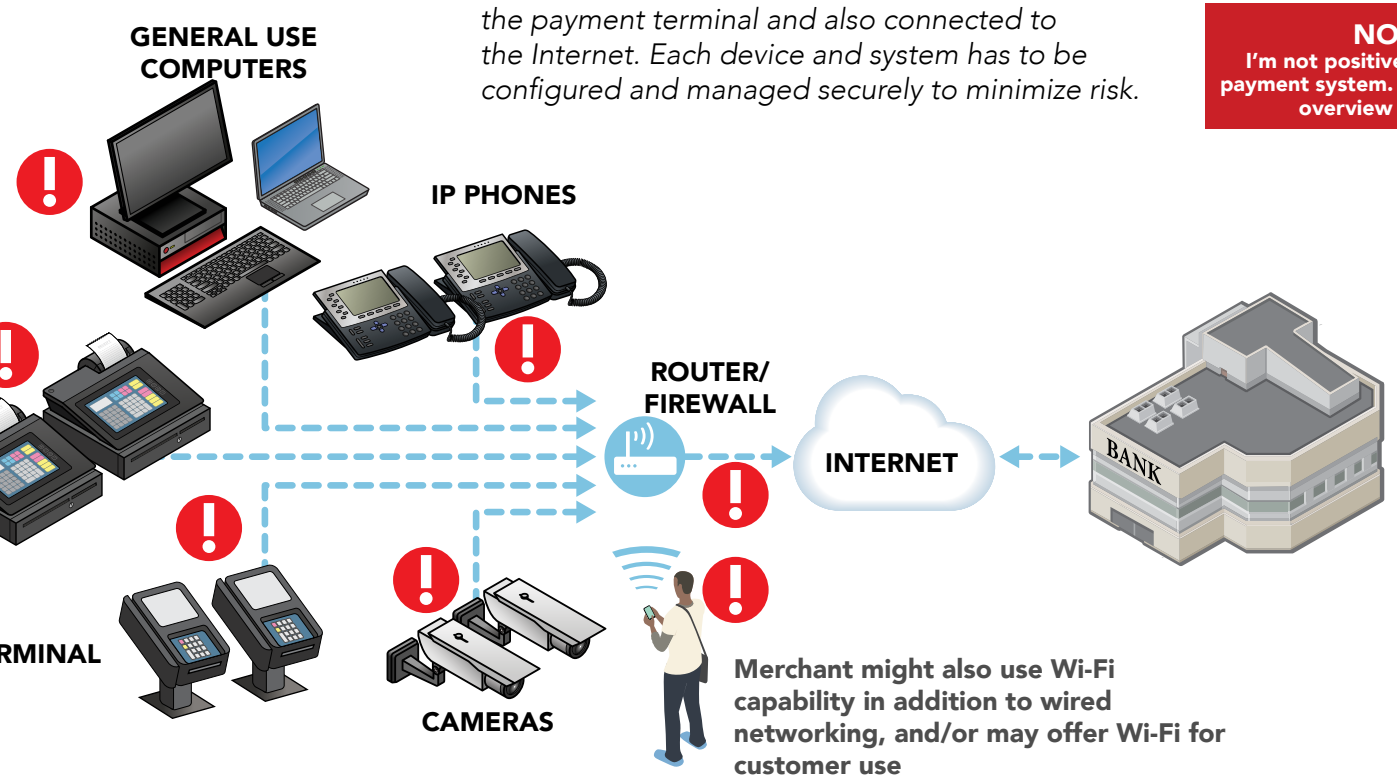
If you are using a PCI-listed Point-to-Point Encryption (P2PE) solution, go to Type 15.

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

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.

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).



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

Merchant might also use Wi-Fi capability in addition to wired networking, and/or may offer Wi-Fi for customer use

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

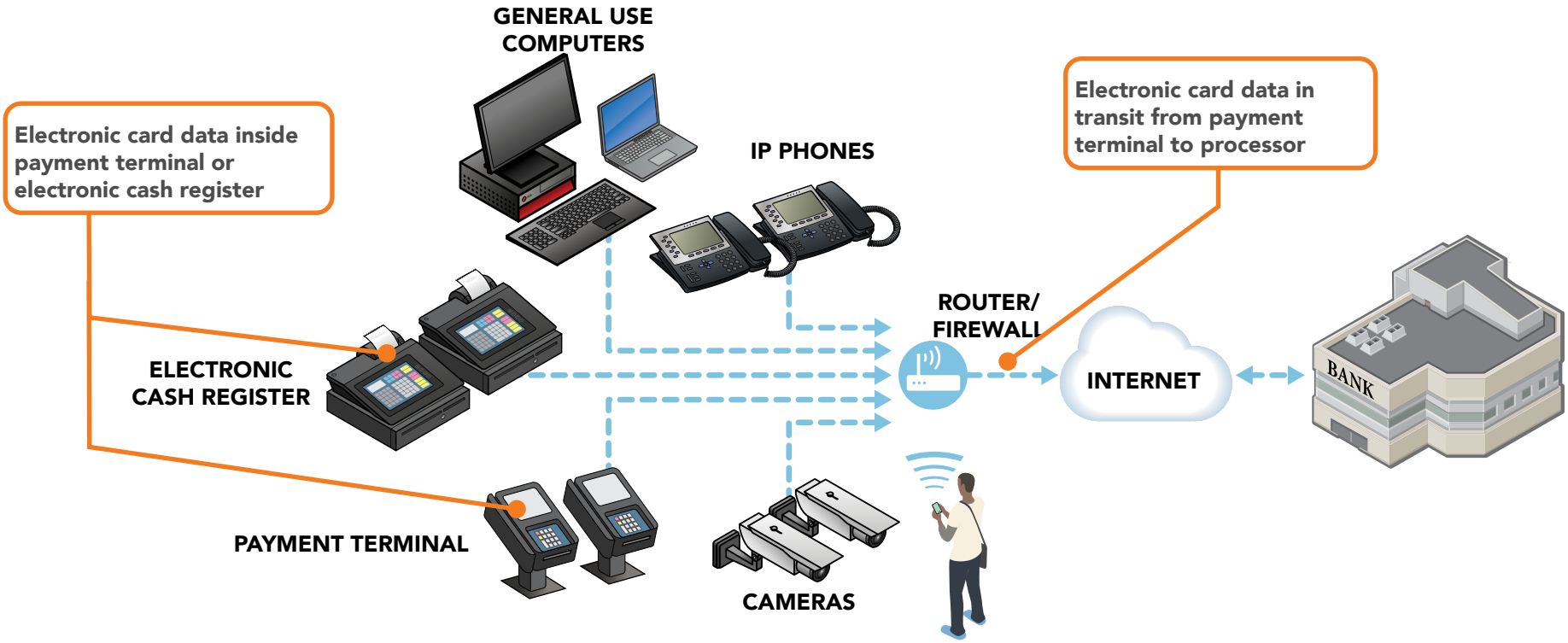
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

RISK PROFILE

Is card data encrypted?

YES NO

Where is your card data at risk?



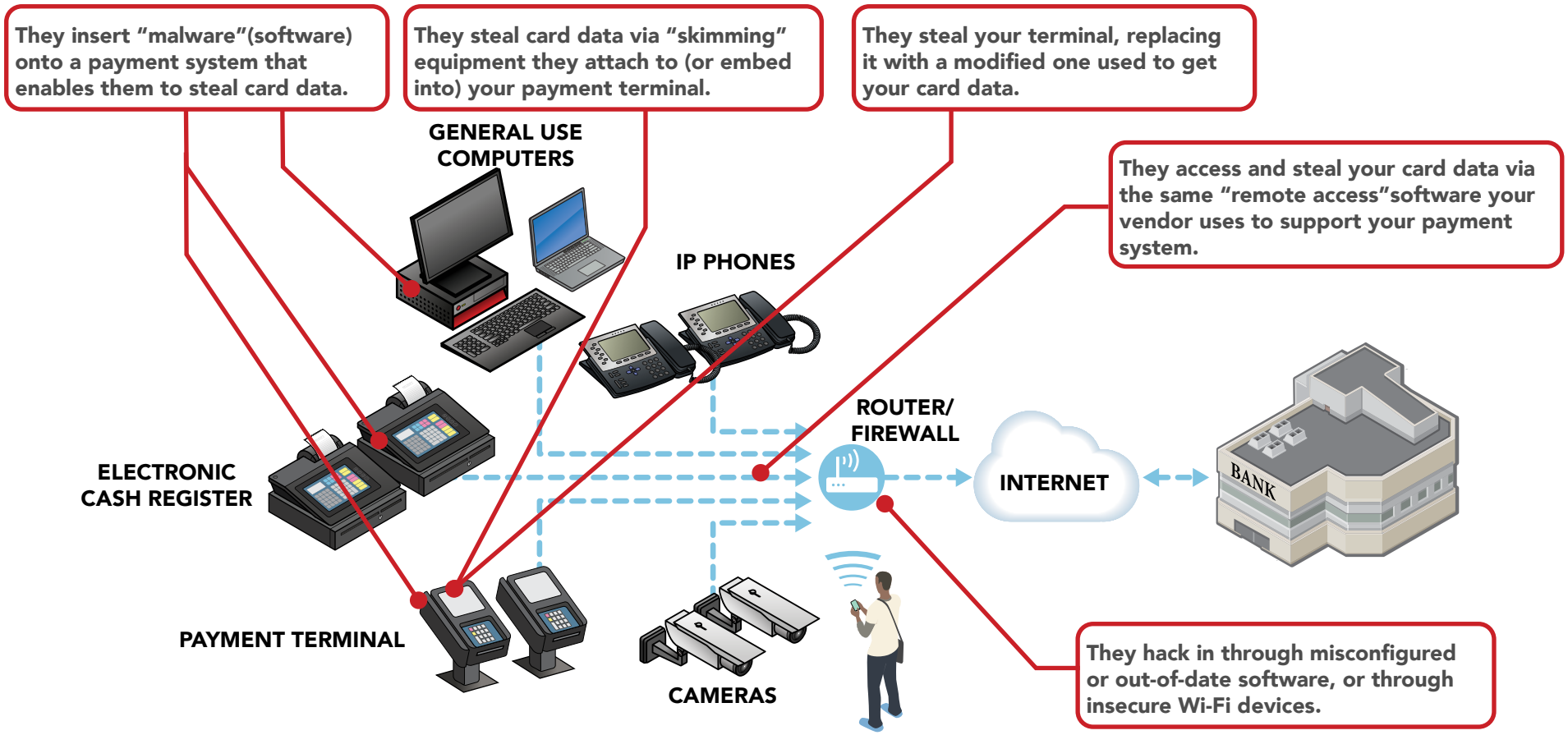
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

RISK PROFILE

Is card data encrypted?

YES NO

How do criminals get your card data?



TYPE 8

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

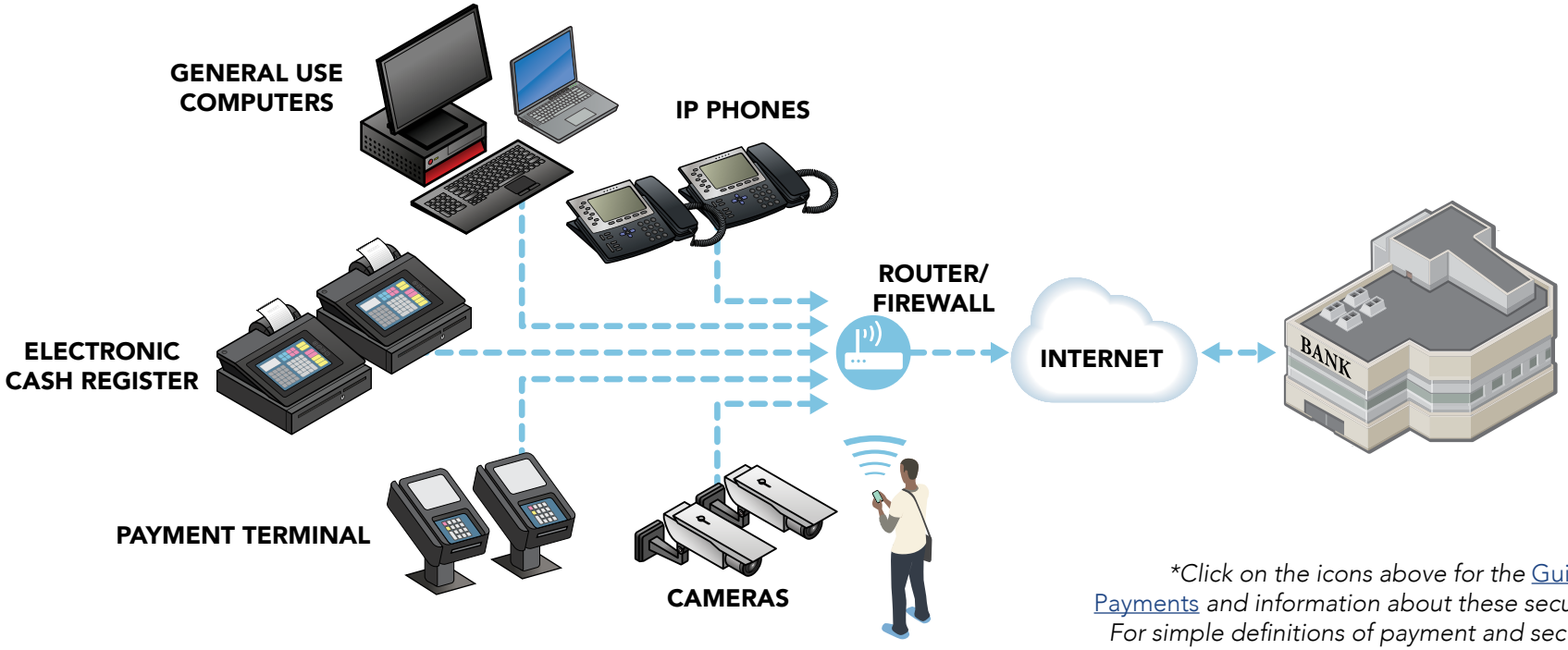
RISK PROFILE

Is card data encrypted?

YES NO

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.

TYPE 9

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

RISK PROFILE

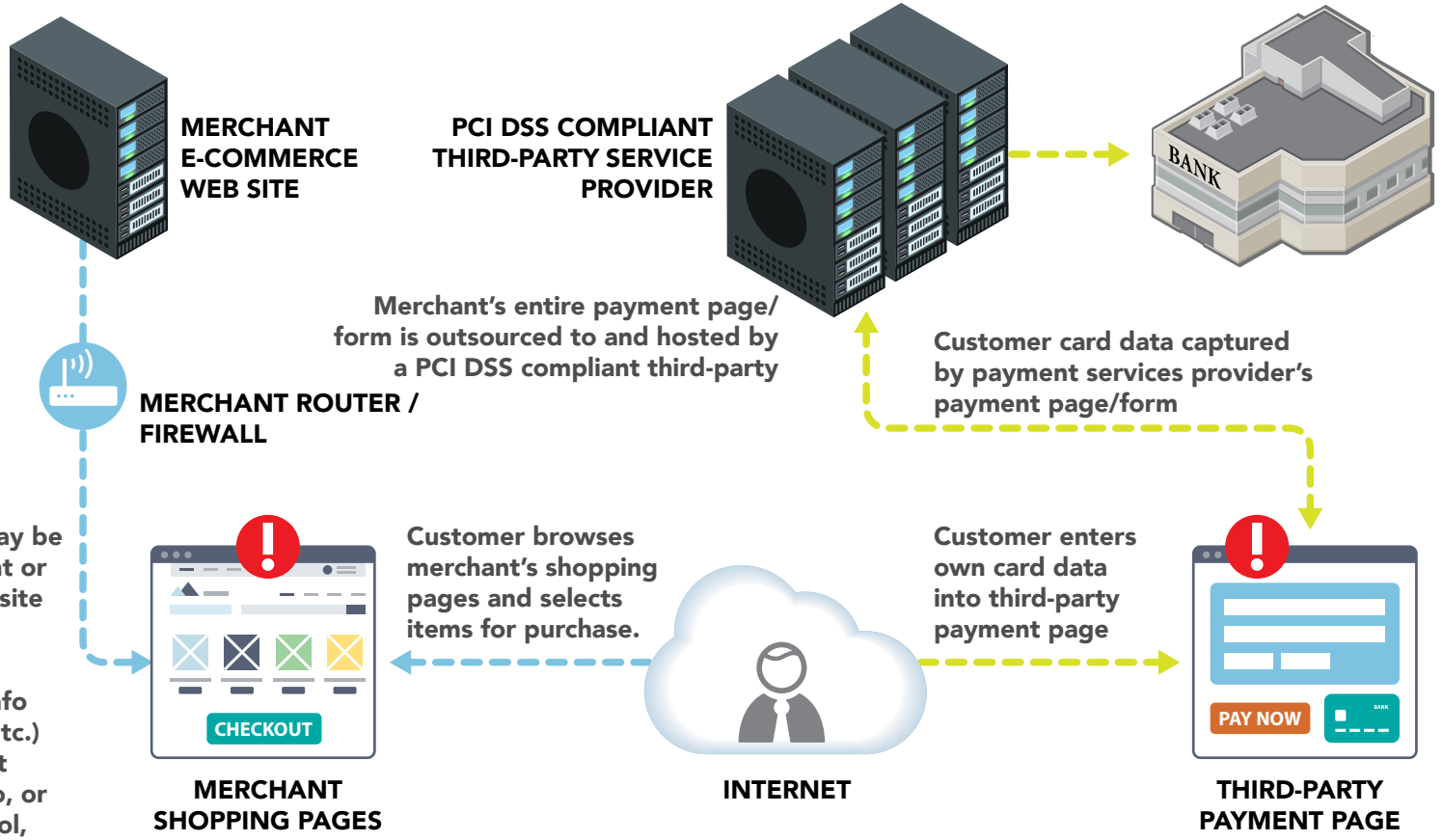
LOWER

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)

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.

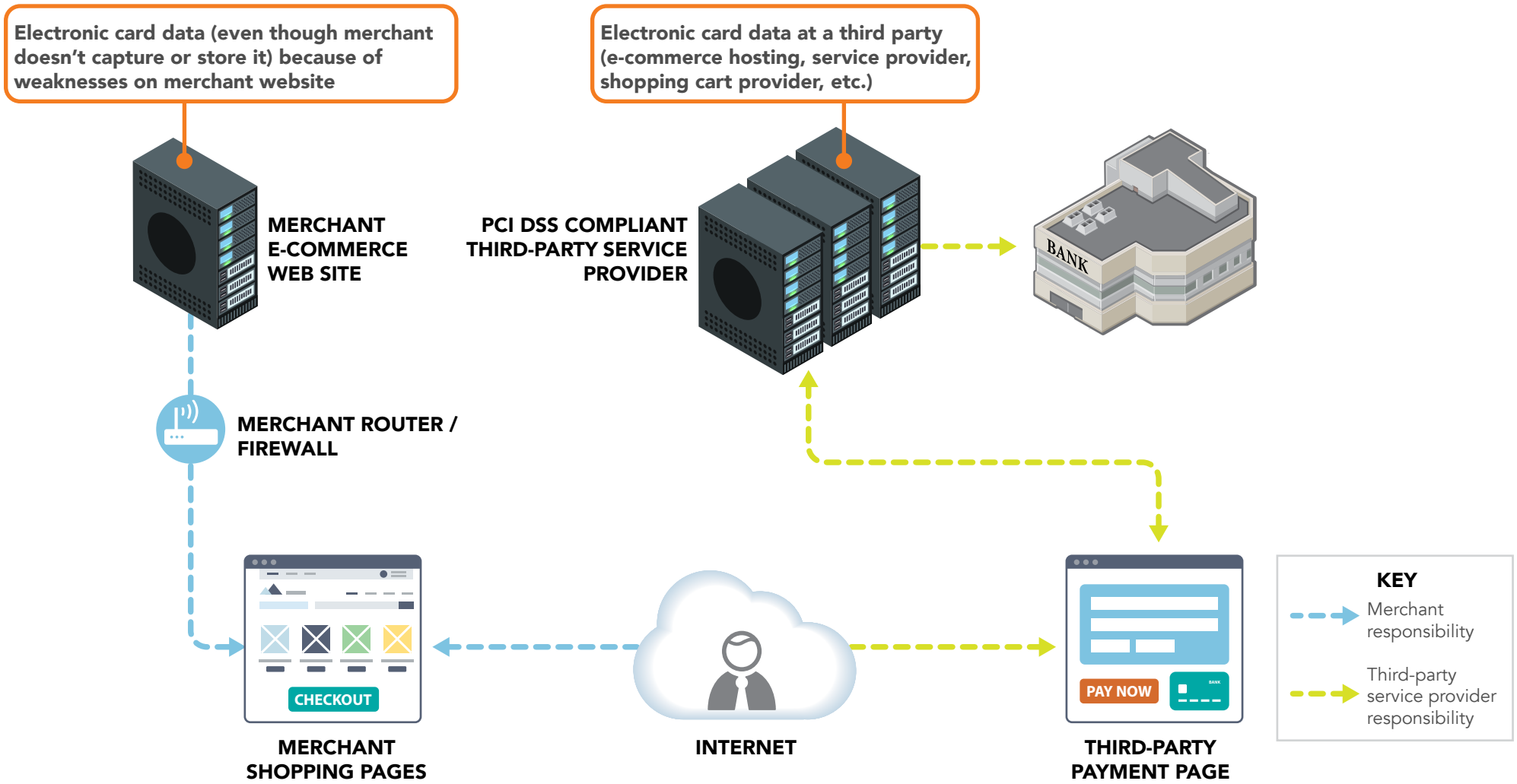
TYPE 9

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

RISK PROFILE

LOWER

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.

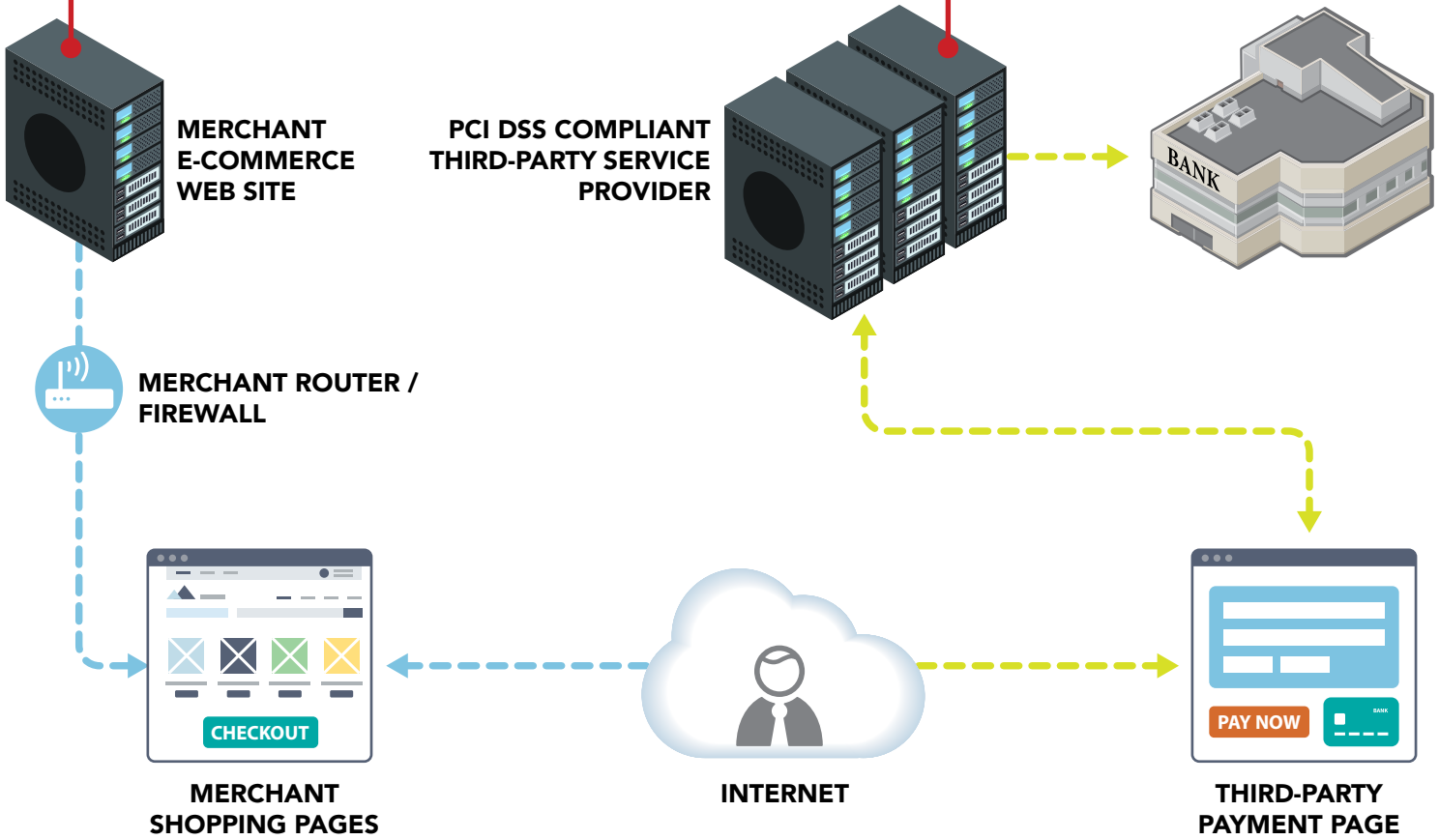
RISK PROFILE

LOWER

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.).



TYPE 9

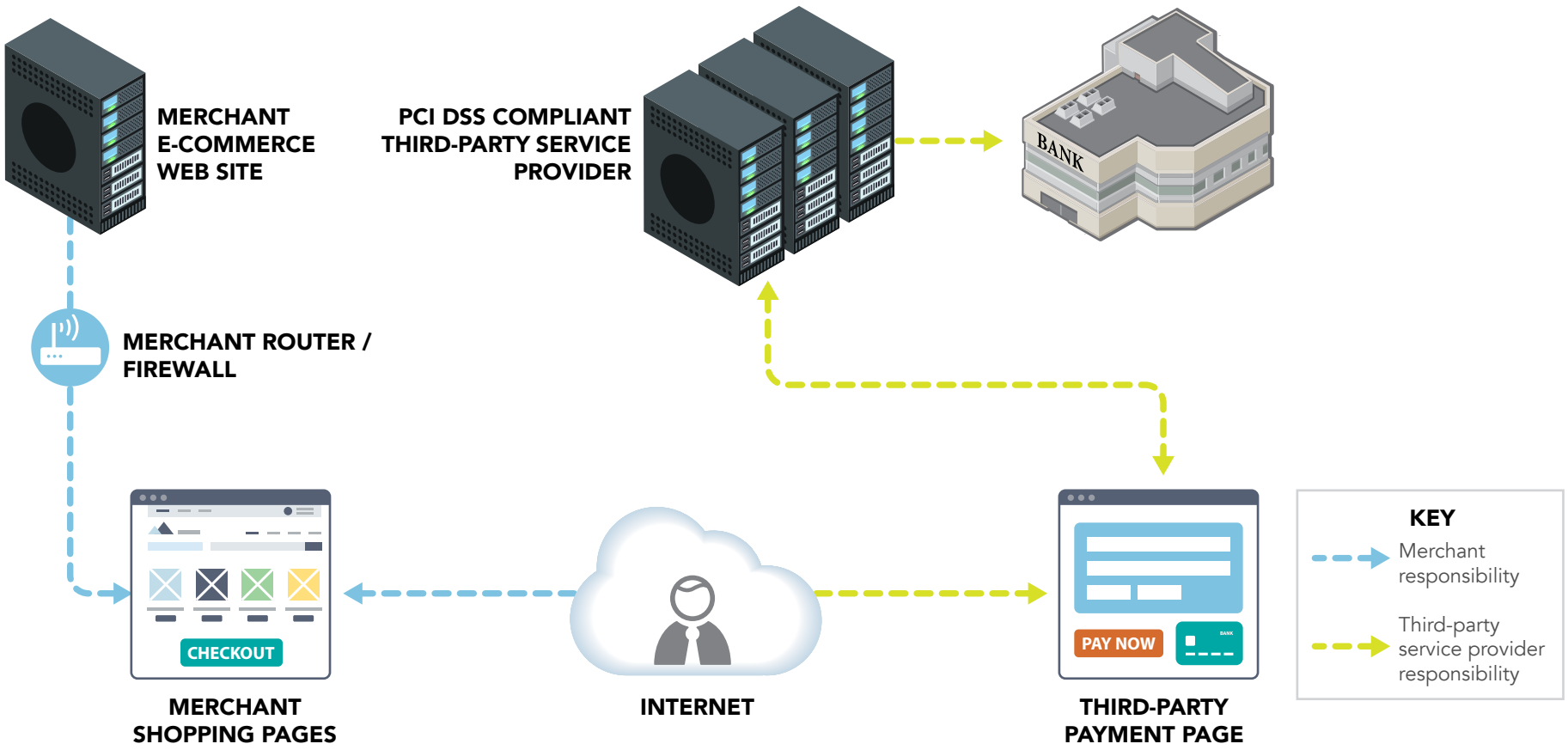
E-commerce merchant with fully-outsourced payment page/form. Payments sent by PCI DSS compliant third-party service provider.

RISK PROFILE

LOWER

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.*

TYPE 10

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.

RISK PROFILE

HIGHER

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).

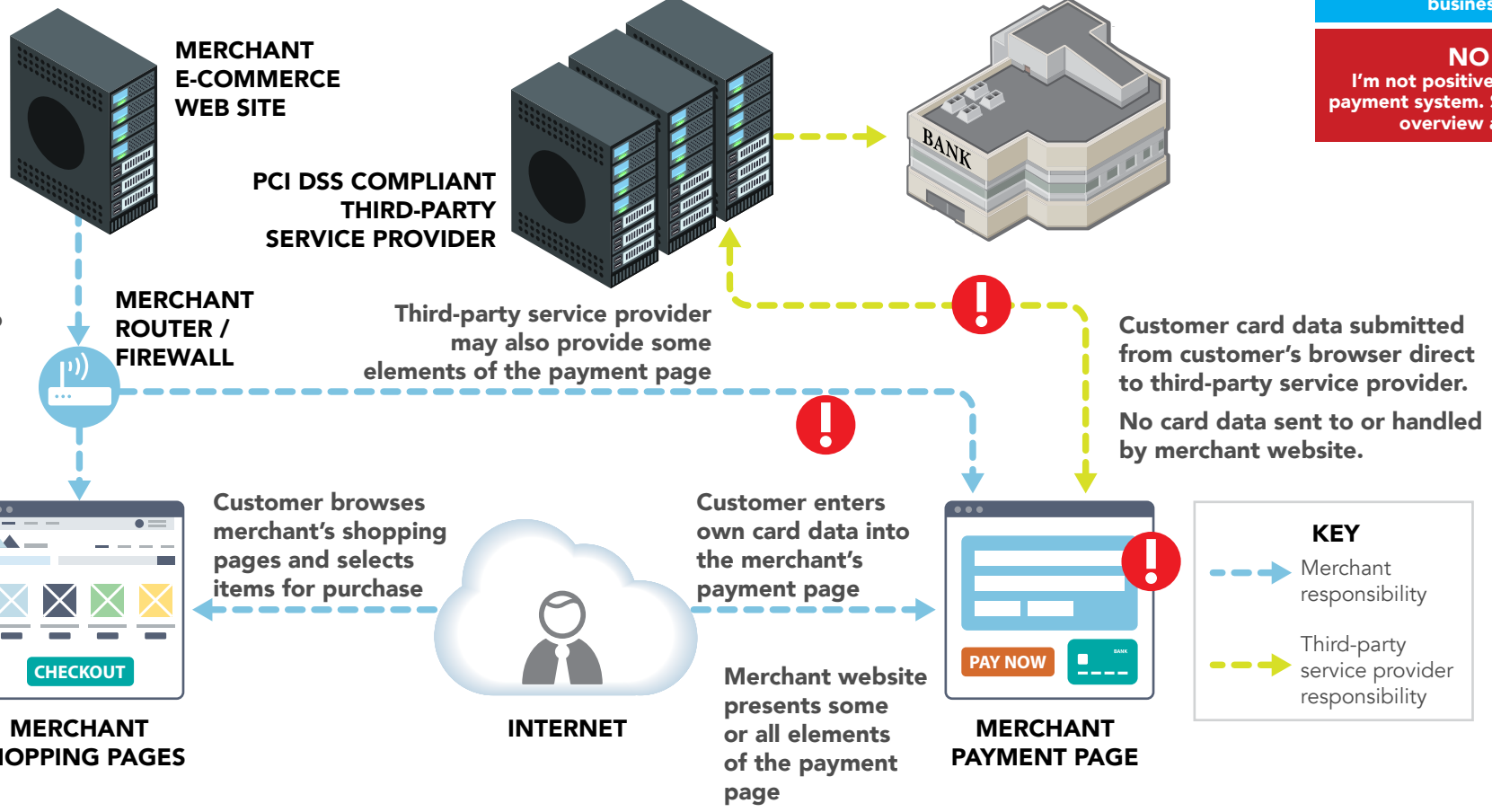
In both cases, card data is sent direct from the customer browser to the third-party service provider.

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

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.



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

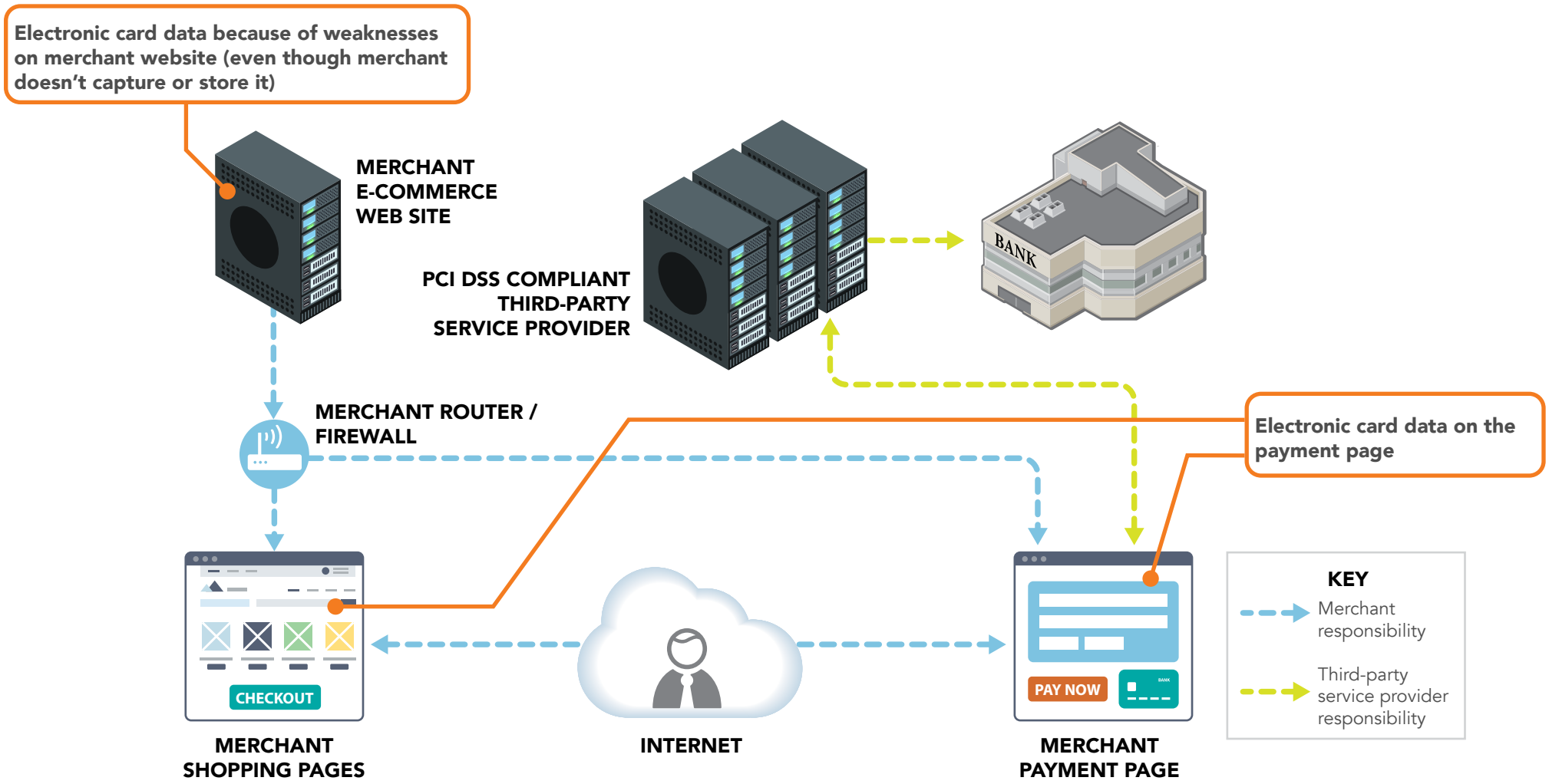
TYPE 10

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.

RISK PROFILE

HIGHER

Where is your card data at risk?

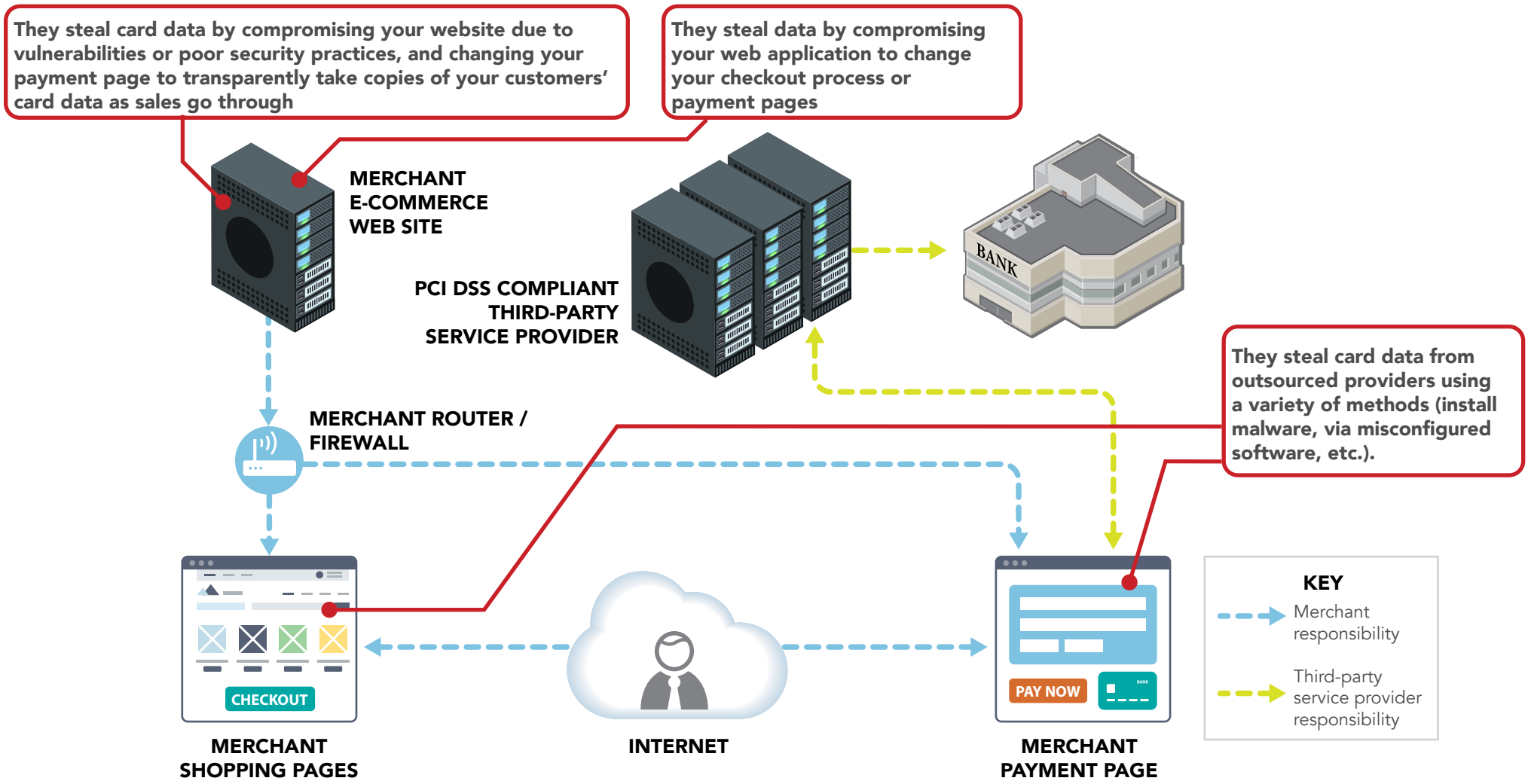


E-commerce merchant fully or partially presents the payment page to customers. Payments sent from customer browser direct to PCI DSS compliant third-party service provider.

RISK PROFILE

HIGHER

How do criminals get your card data?



TYPE 10

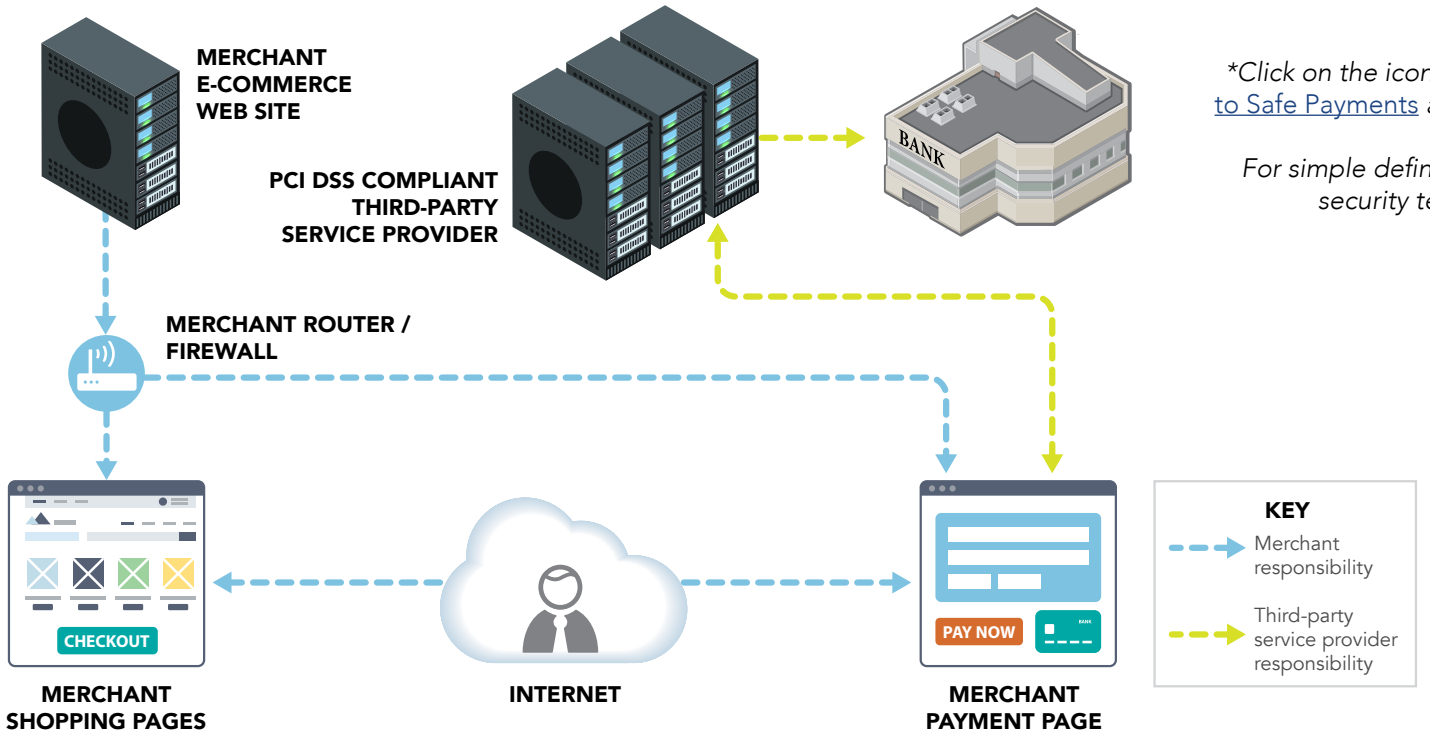
E-commerce merchant fully or partially presents the payment page to customers. Payments sent from customer browser direct to PCI DSS compliant third-party service provider.

RISK PROFILE

HIGHER

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.

TYPE 11

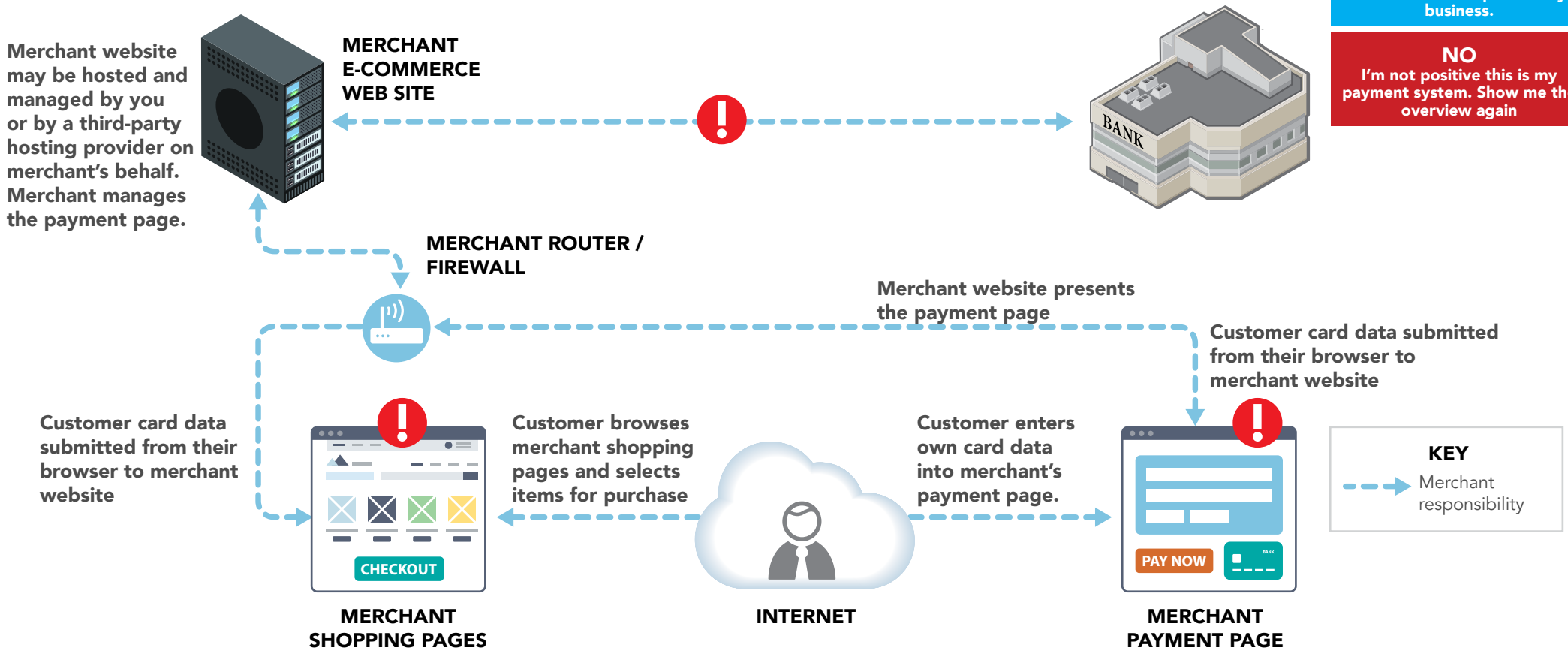
E-commerce merchant accepts card data using payment page presented to customers from own website. Payments sent via the merchant website.

RISK PROFILE

HIGHER

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.

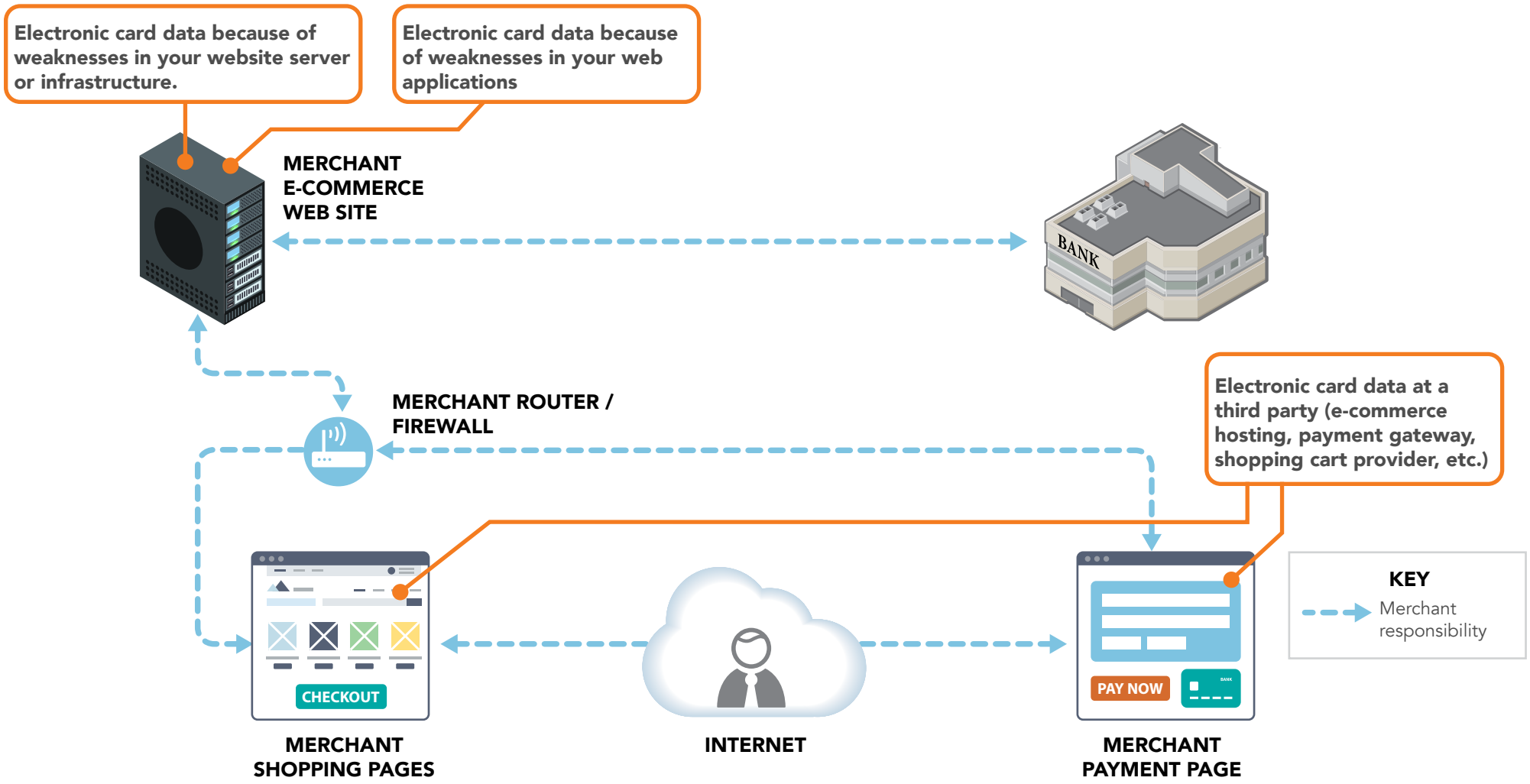
TYPE 11

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

RISK PROFILE

HIGHER

Where is your card data at risk?



TYPE 11

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

RISK PROFILE

HIGHER

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.

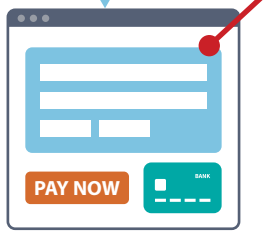
MERCHANT E-COMMERCE WEB SITE

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

MERCHANT ROUTER / FIREWALL

MERCHANT SHOPPING PAGES

INTERNET



MERCHANT PAYMENT PAGE

KEY

Merchant responsibility

TYPE 11

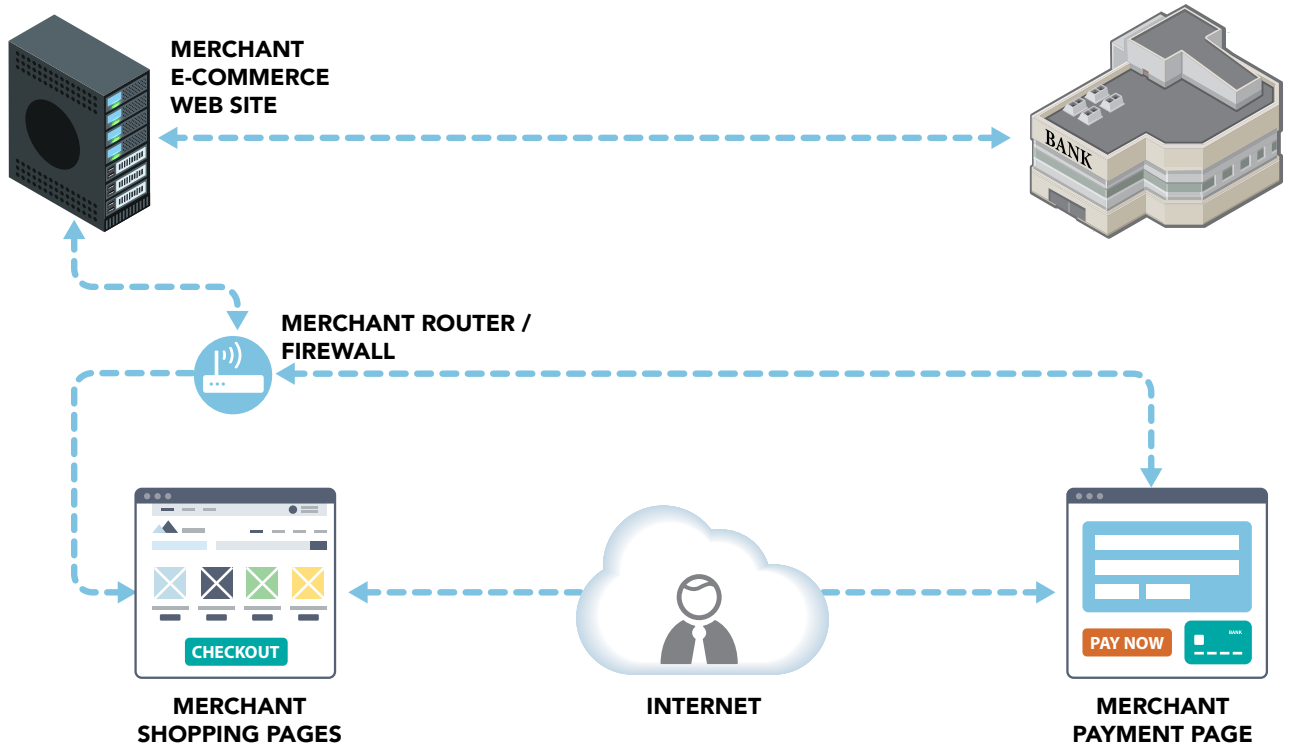
E-commerce merchant accepts card data using payment page presented to customers from own website. Payments sent via the merchant website.

RISK PROFILE

HIGHER

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.

TYPE 12

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

RISK PROFILE

LOWER

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

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.)

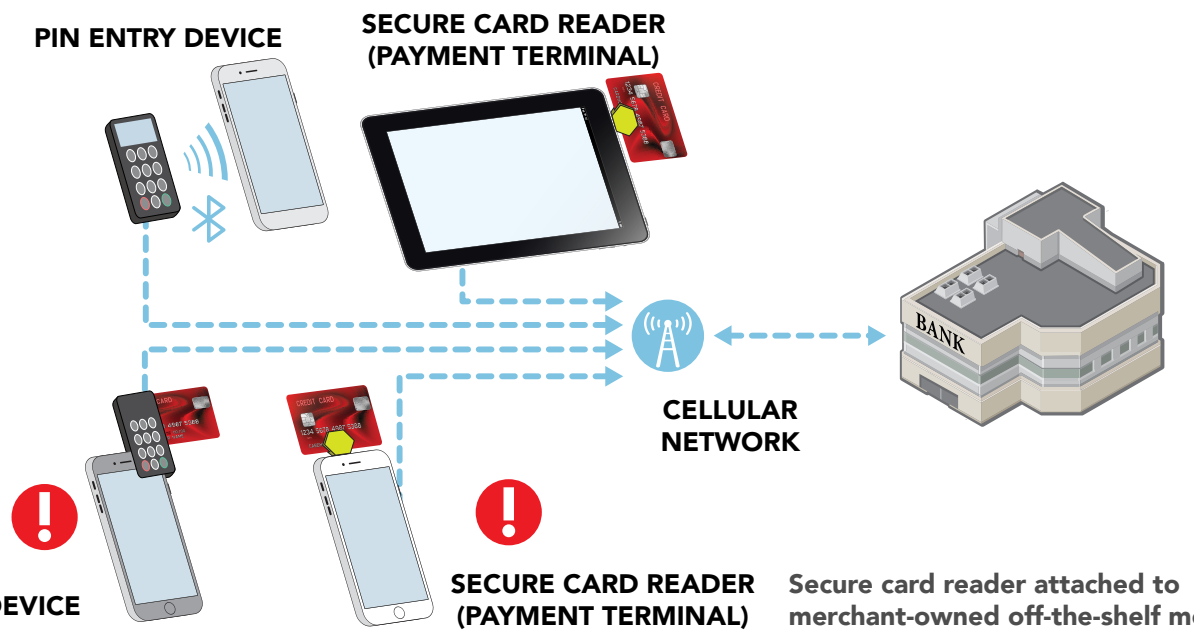
Secure card reader is listed on the PCI SSC website as an approved SCR. Ask your vendor or check here to confirm (select SCR under "device type"): PCI-listed PTS Devices.

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



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

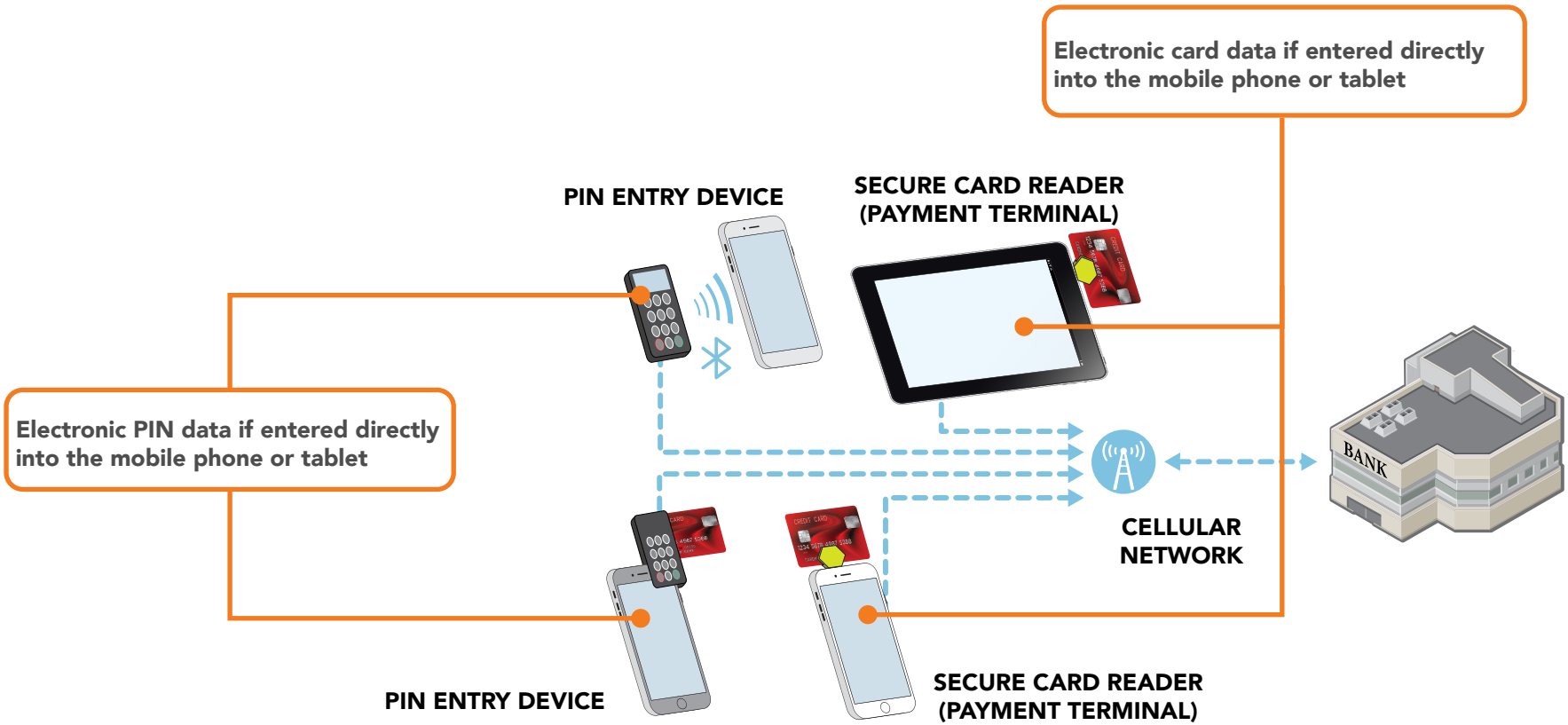
For this scenario, risks to card data are present at ❗ above. Risks explained on next page.

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

RISK PROFILE

LOWER

Where is your card data at risk?



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

RISK PROFILE

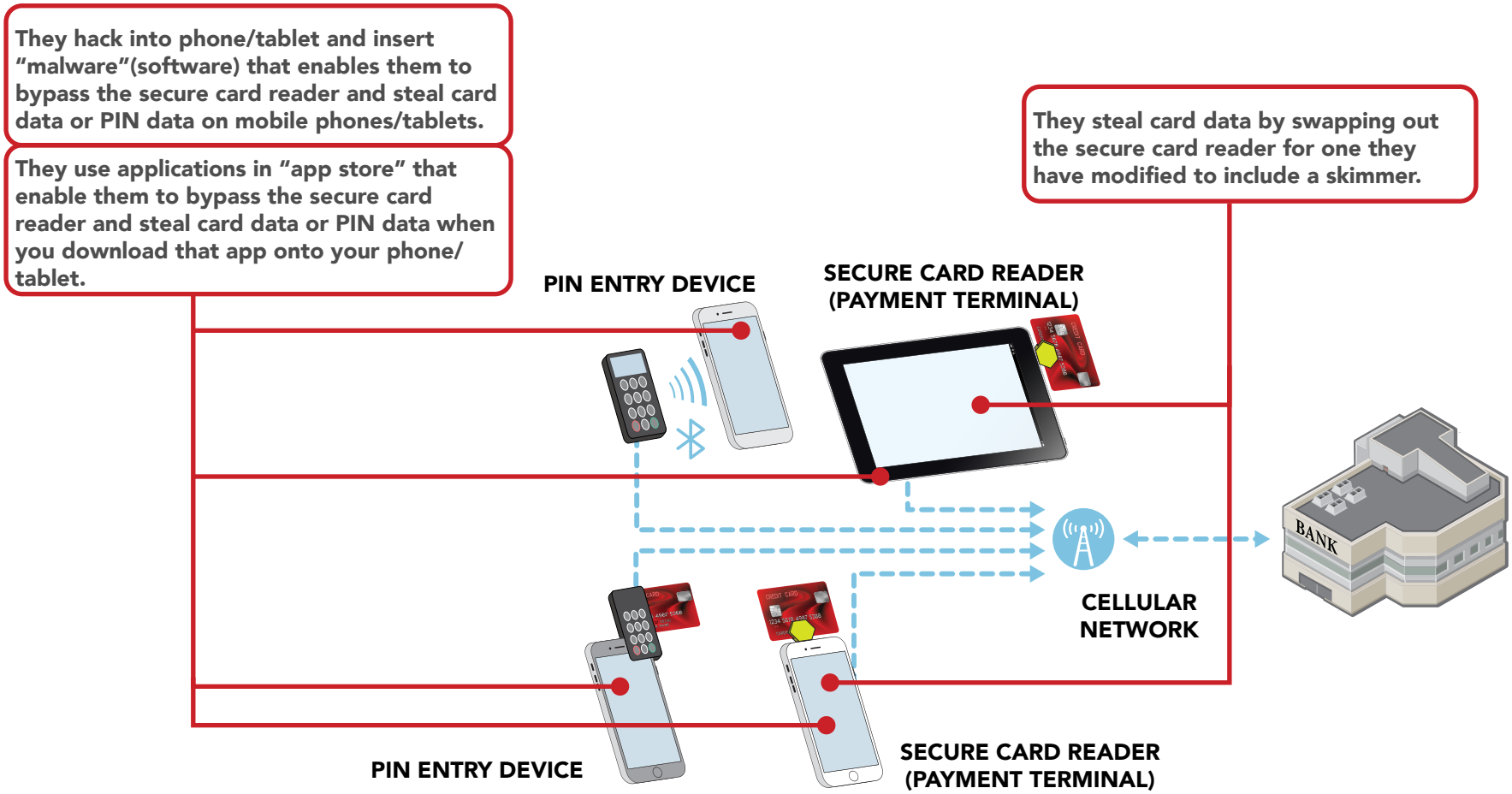
LOWER

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.



TYPE 12

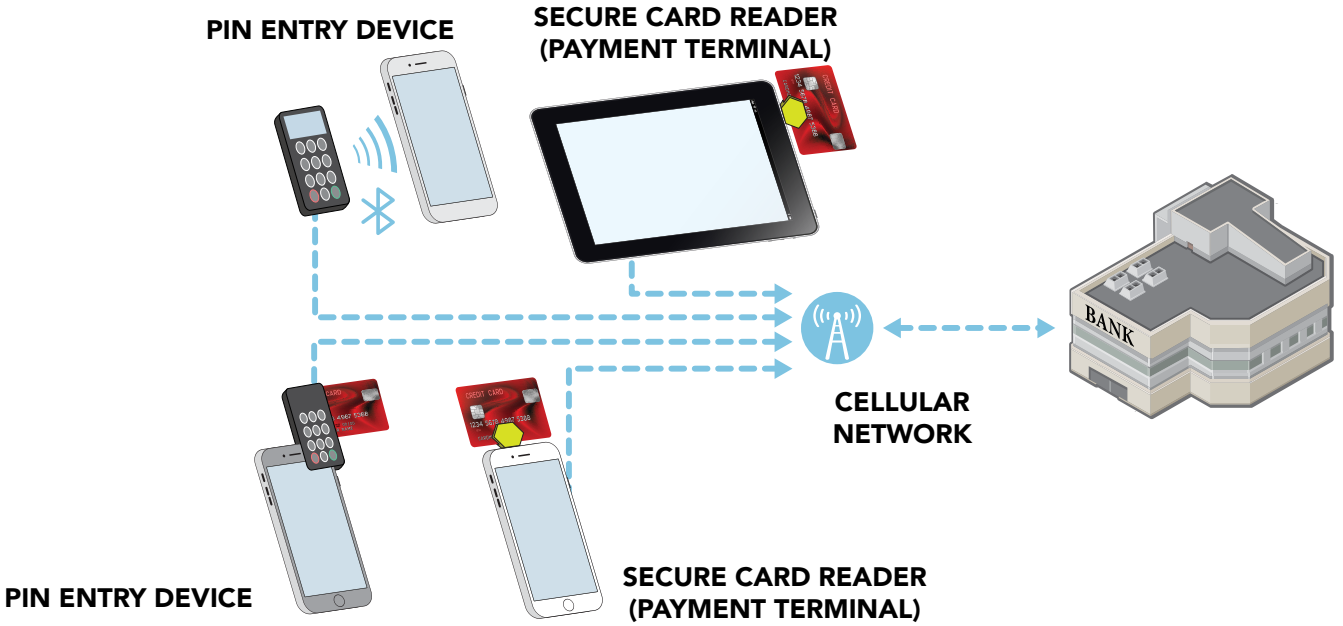
PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

RISK PROFILE

LOWER

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
- Ask your vendor partners for help if you need it
- Protect your business from the Internet
- Use a secure card reader and PIN entry device
- Make your card data useless to criminals
- Protect card data and only keep what you need
- Protect in-house access to your card data
- 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.

TYPE 13

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

RISK PROFILE

MODERATE

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

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

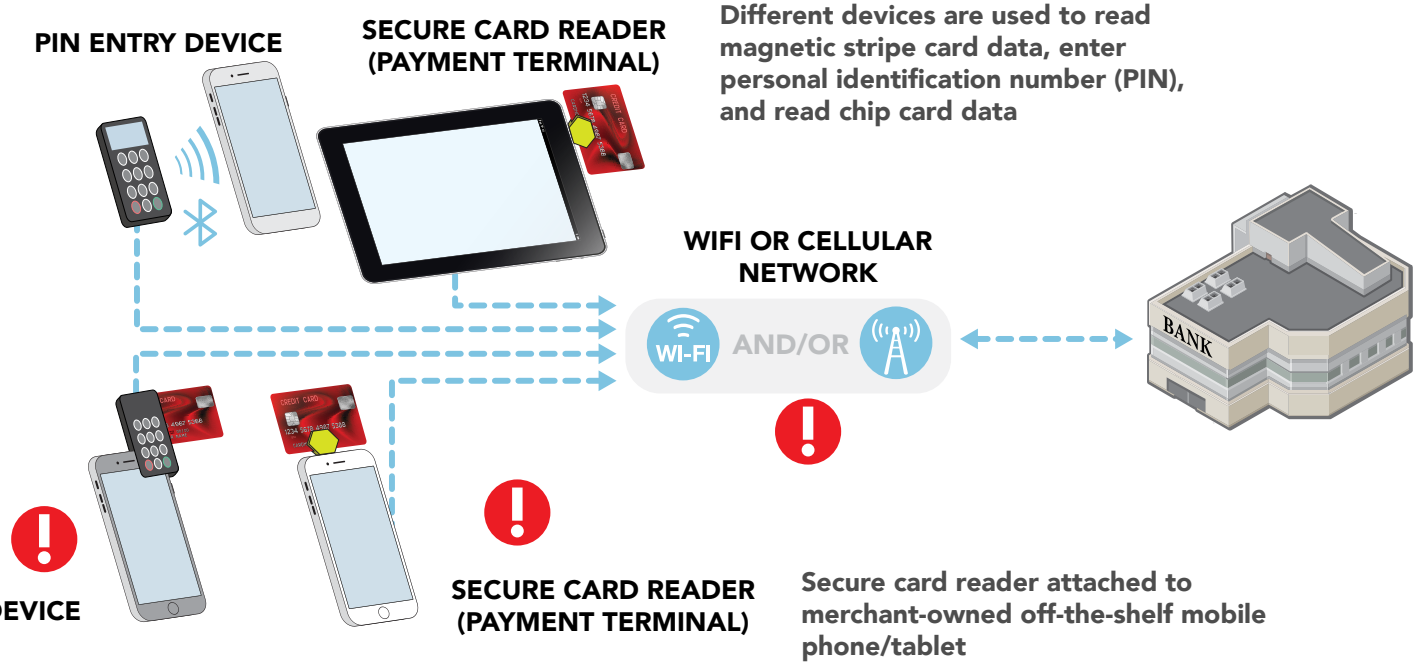
For merchants when at non-fixed locations (flea market, trade show, etc.)

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.



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

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

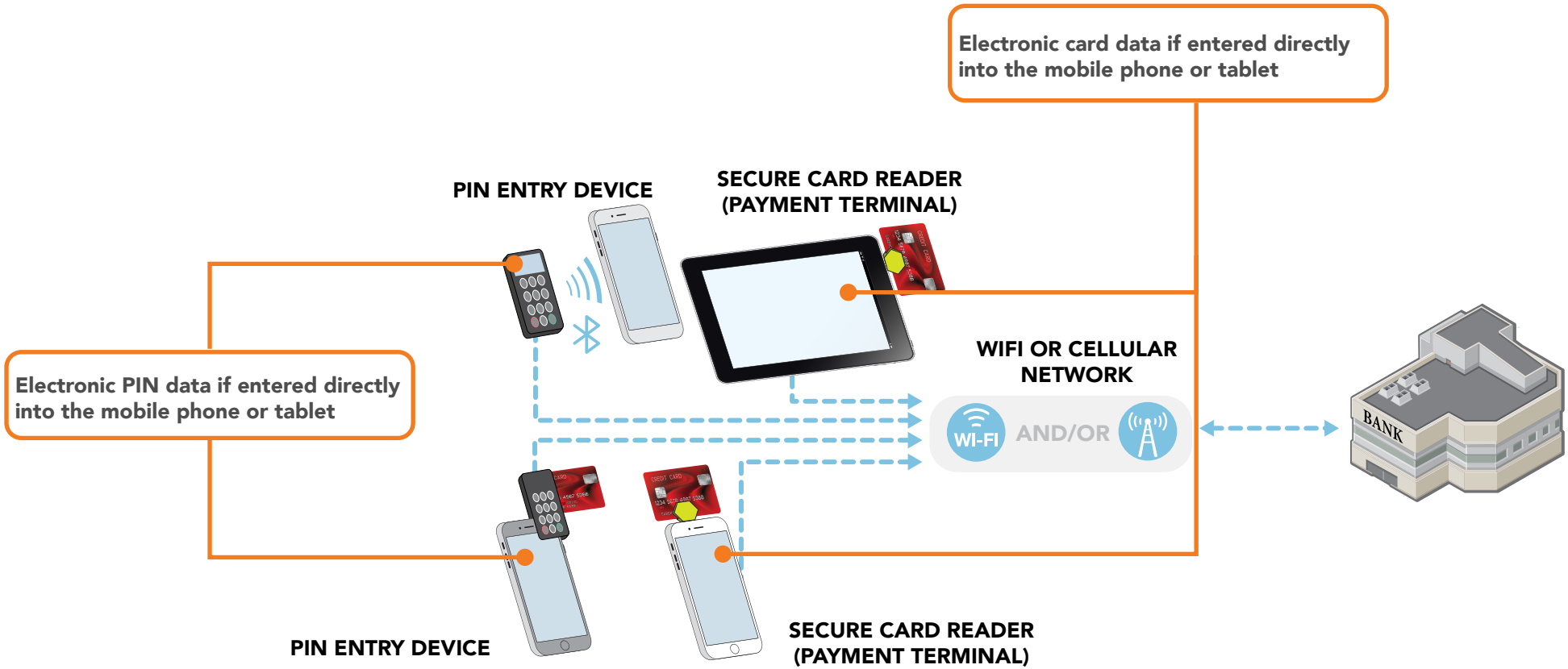
For this scenario, risks to card data are present at ❗ above. Risks explained on next page.

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

RISK PROFILE

MODERATE

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.

RISK PROFILE

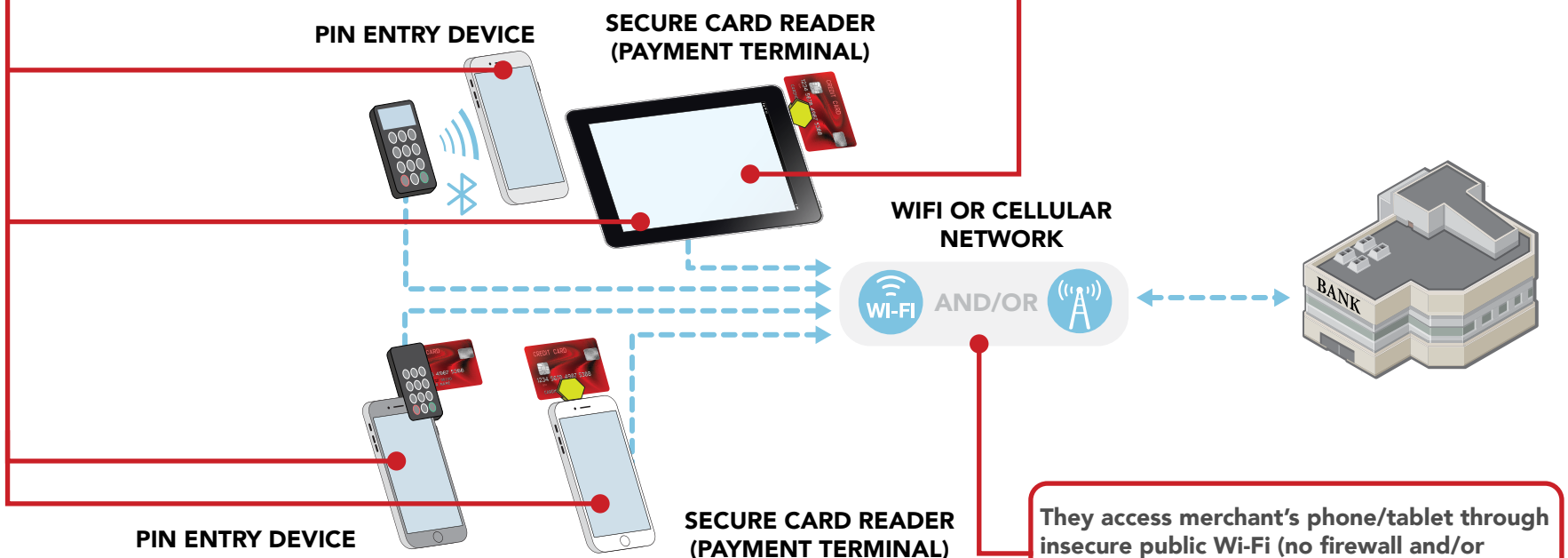
MODERATE

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

TYPE 13

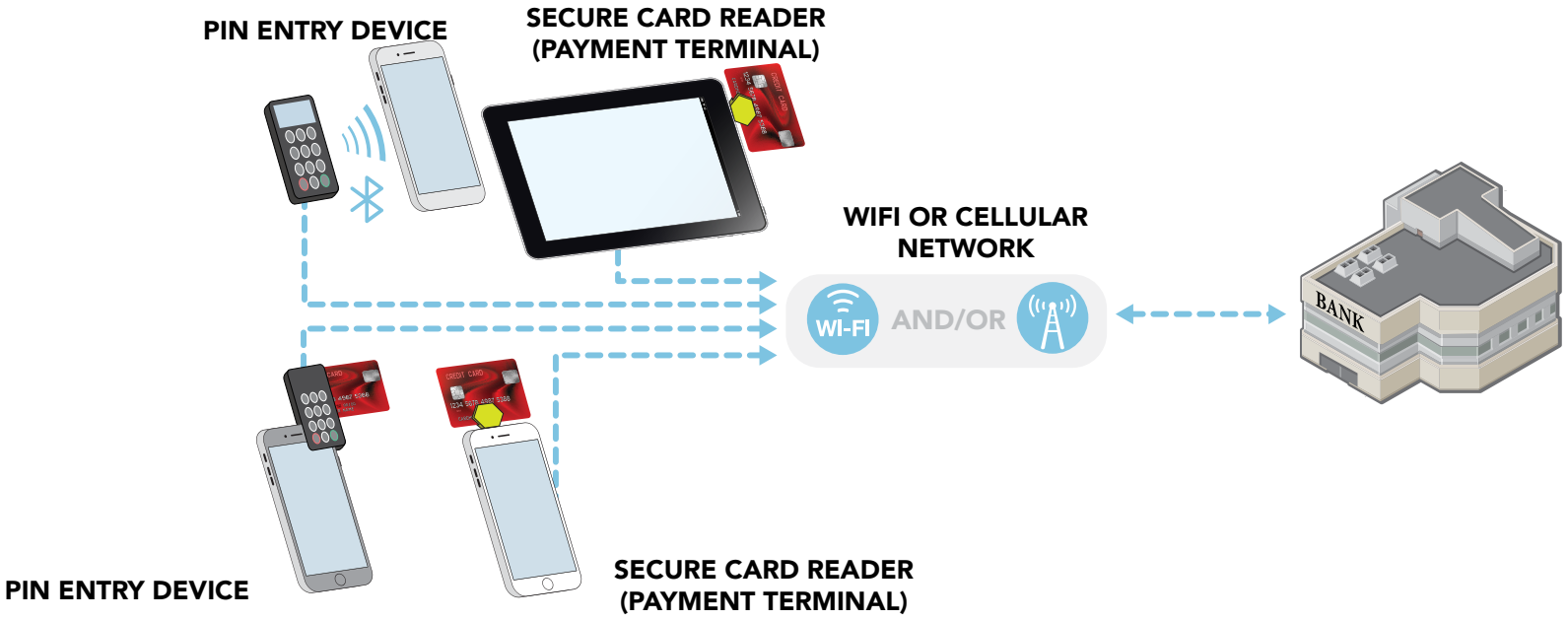
PCI-listed encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.

RISK PROFILE

MODERATE

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
- Install patches from your payment terminal vendor
- Ask your vendor partners for help if you need it
- 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 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.

TYPE 14

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

RISK PROFILE

LOWER

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.

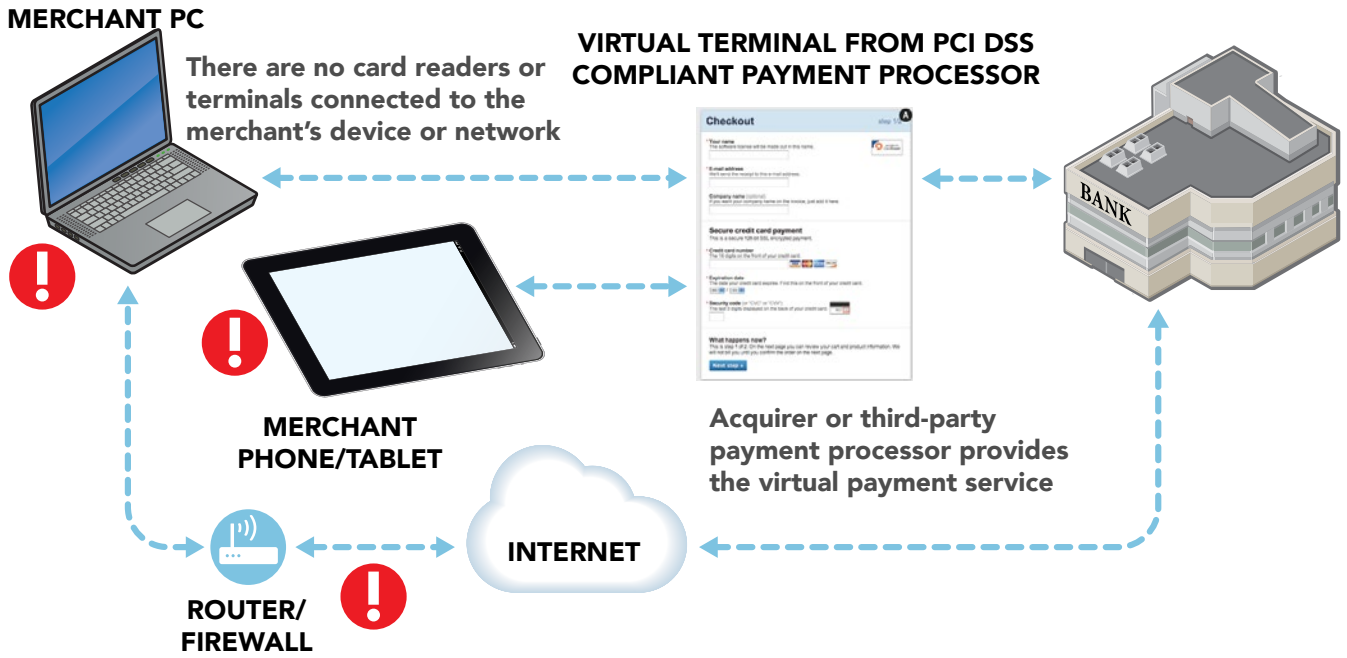
NO
I'm not positive this is my payment system. Show me the overview again

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.

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)



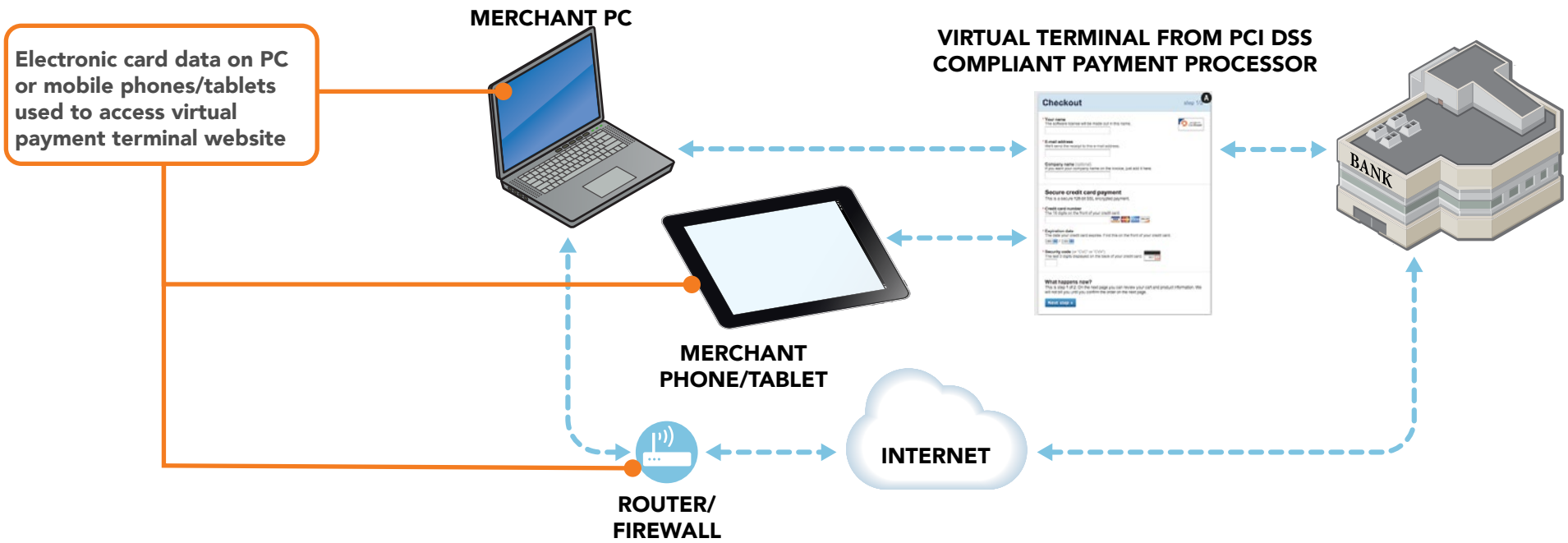
For this scenario, risks to card data are present at ! above. Risks explained on next page.

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

RISK PROFILE

LOWER

Where is your card data at risk?



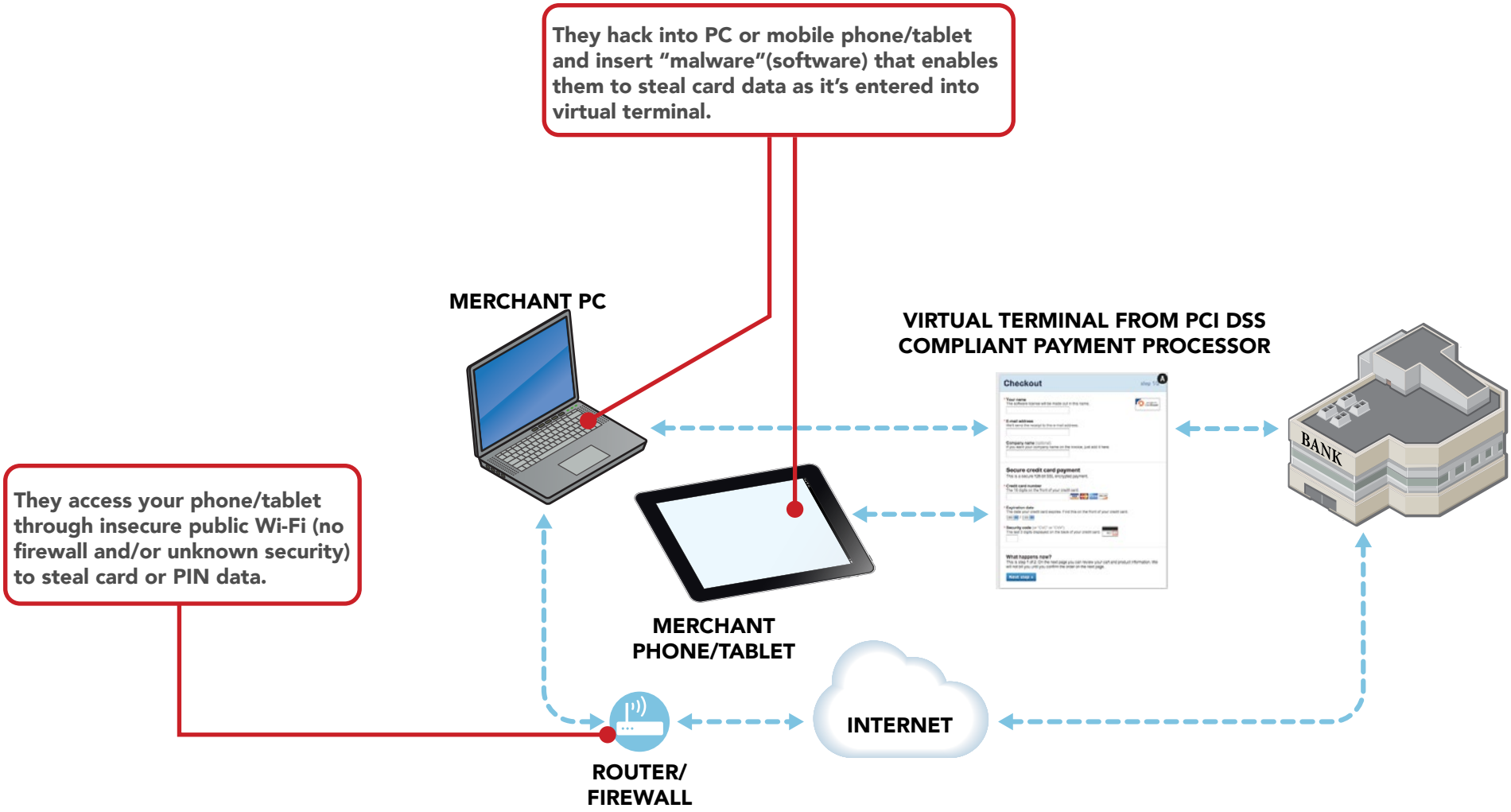
Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

RISK PROFILE

LOWER

How do criminals get your card 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.



TYPE 14

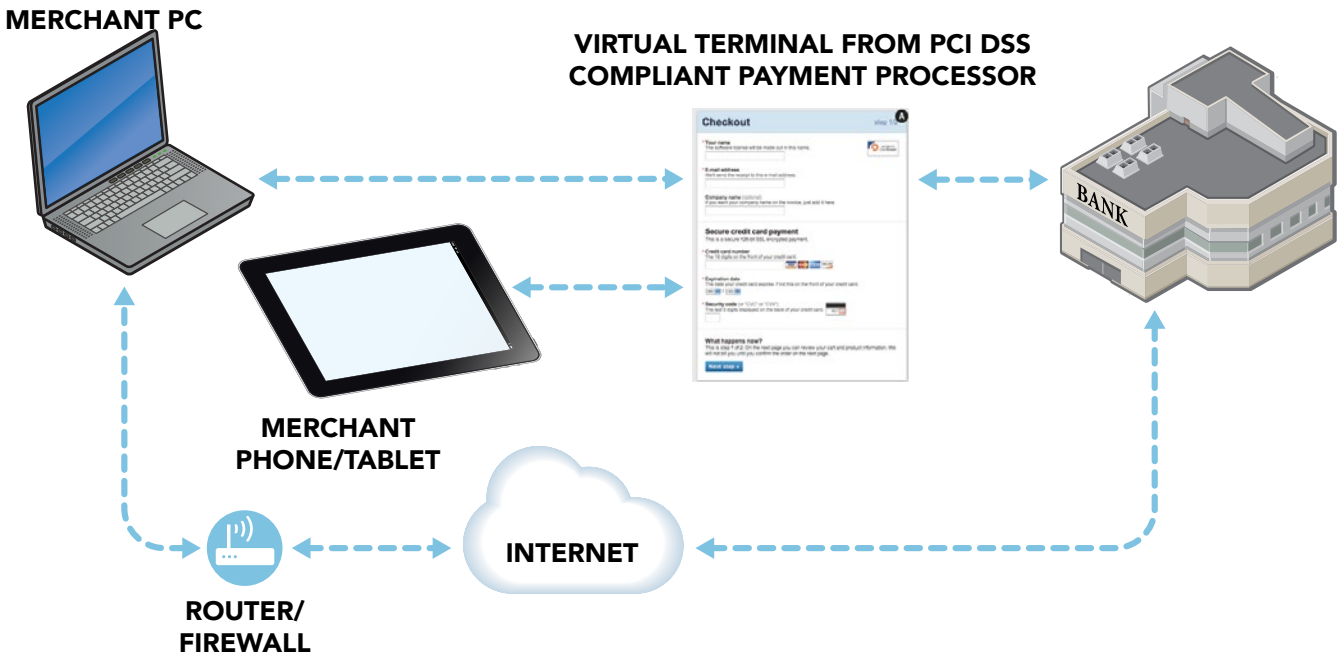
Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

RISK PROFILE

LOWER

How do you start to protect card data today?*

- Use strong passwords
- Use anti-virus software
- Install patches from your payment terminal vendor
- Get regular vulnerability scanning
- Ask your vendor partners for help if you need it
- Use a firewall (or personal firewall software if using public Wi-Fi)
- 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.

TYPE 15

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

RISK PROFILE

LOWEST

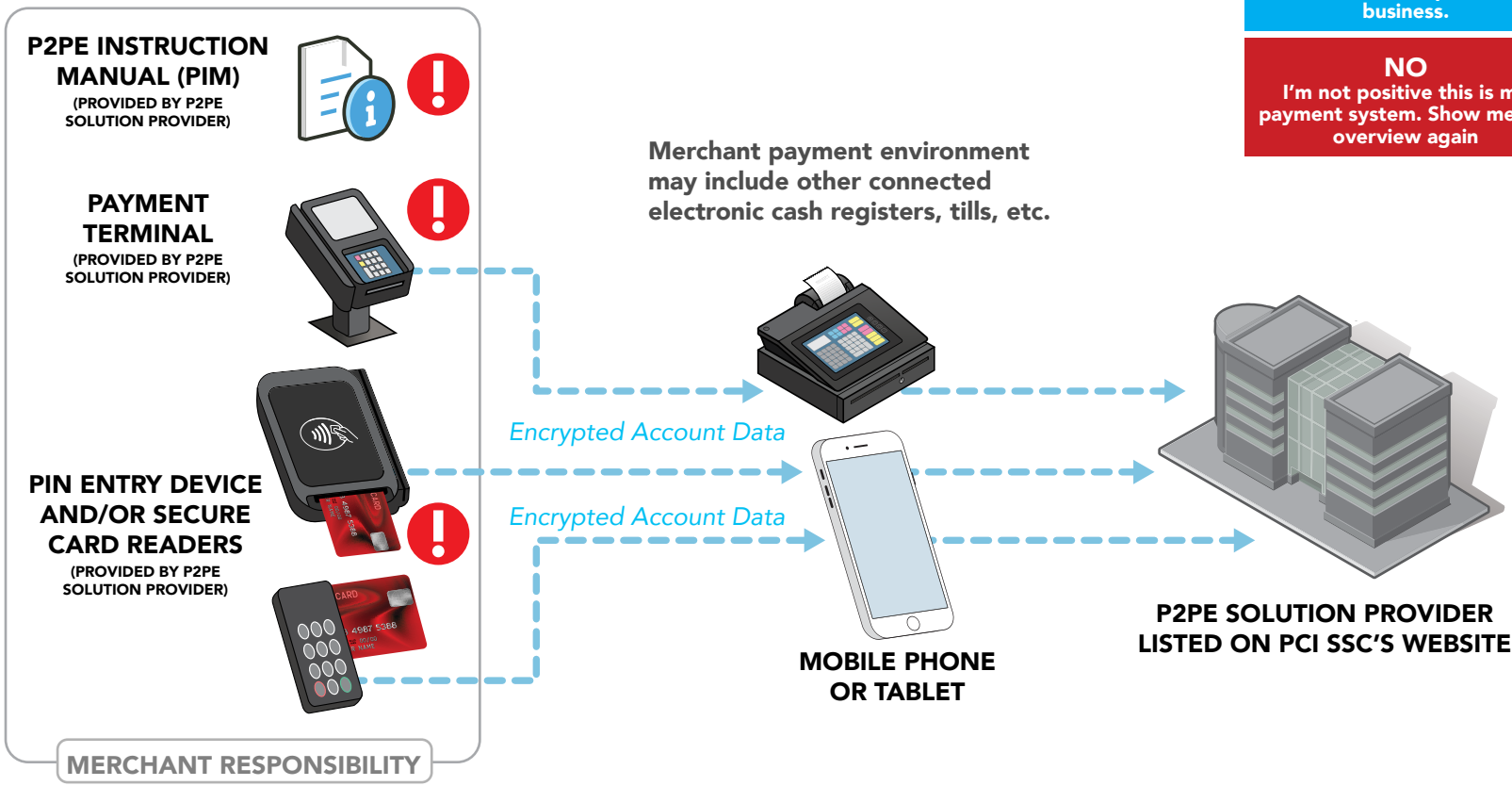
YES
This is my payment system, and I have reviewed the Risks, Threats, and Protections tabs. I'm ready to download the Evaluation Form to my computer now to understand how I can better protect my business.

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

The solution in 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.

TYPE 15

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

RISK PROFILE

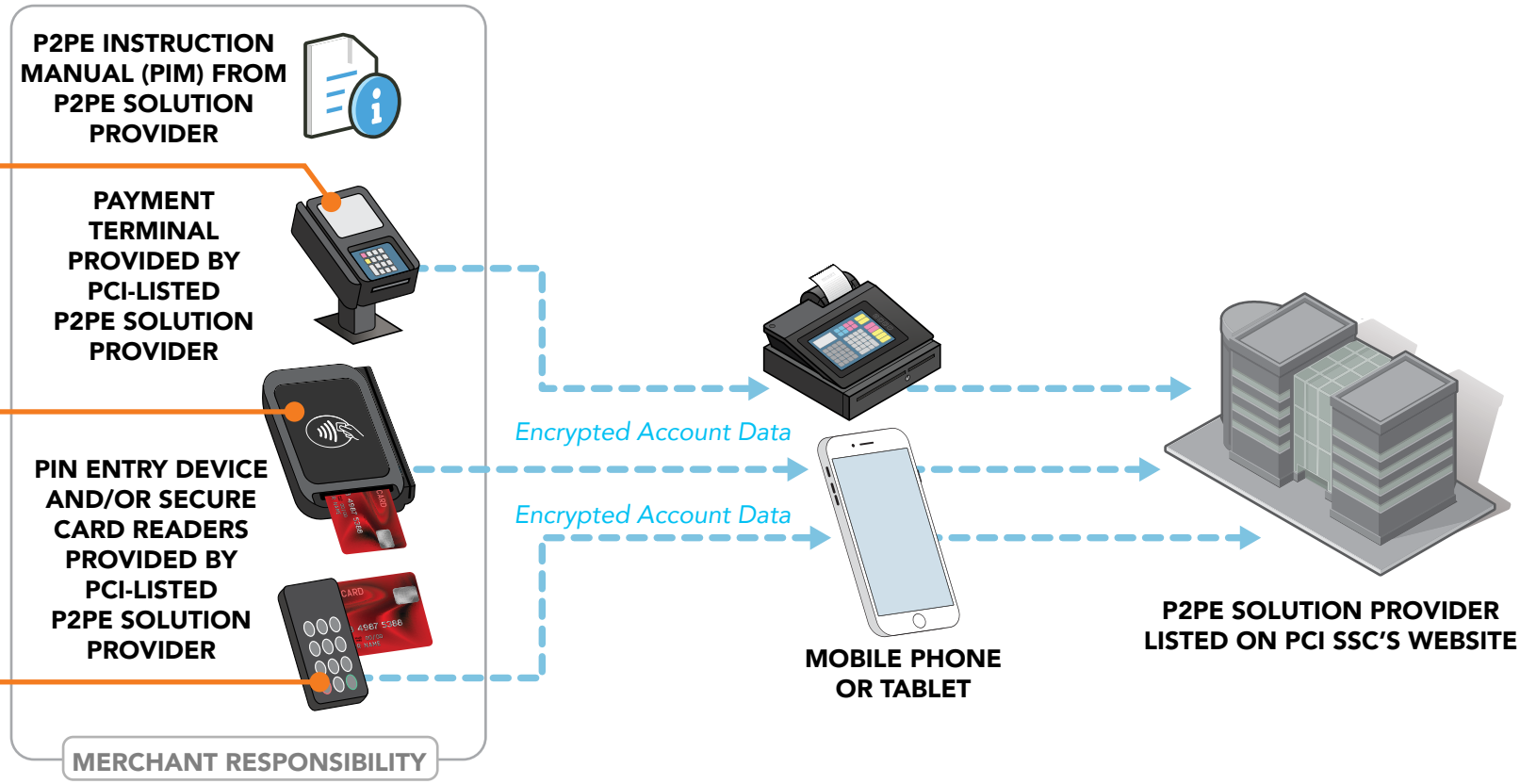
LOWEST

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.



TYPE 15

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

RISK PROFILE

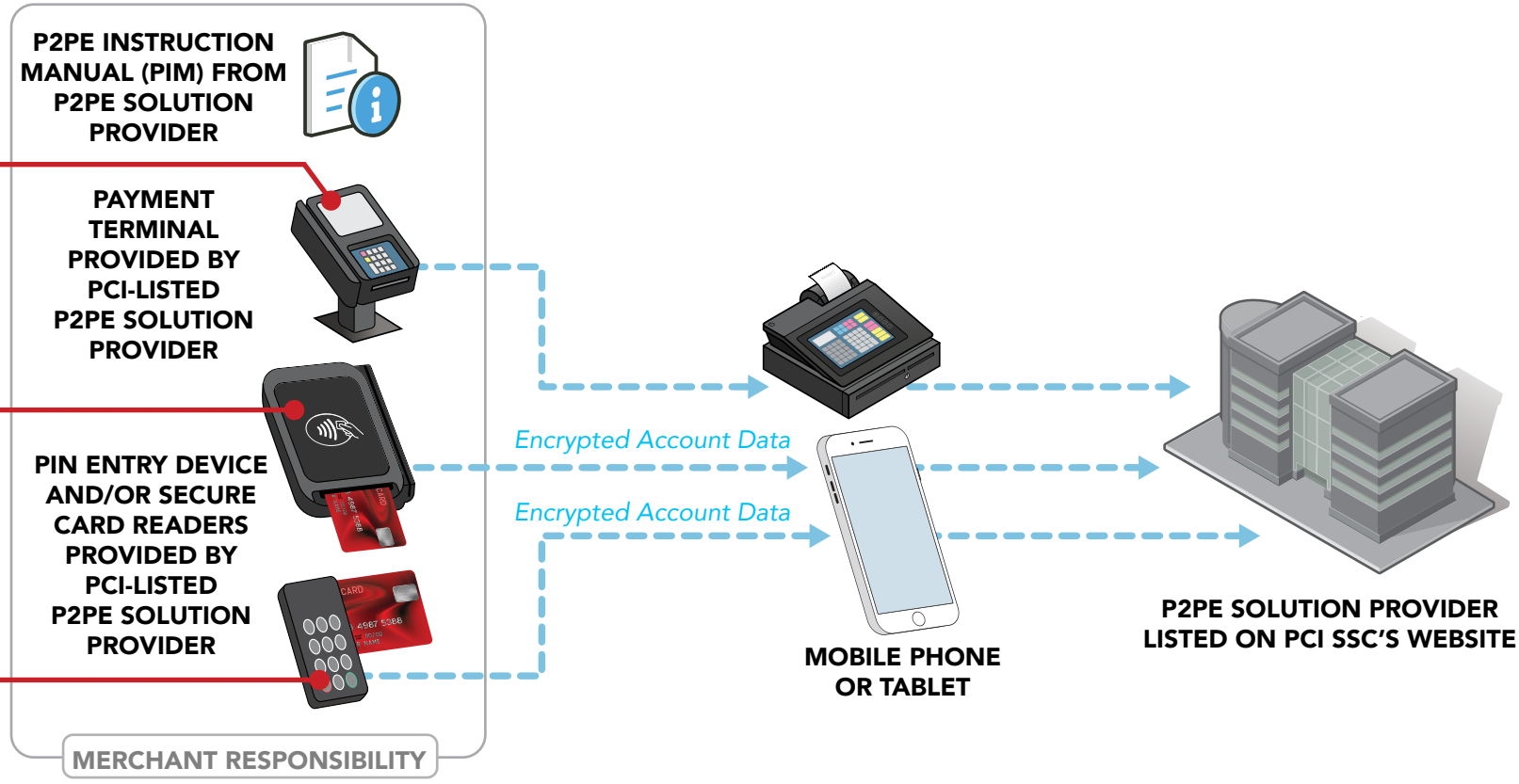
LOWEST

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



TYPE 15

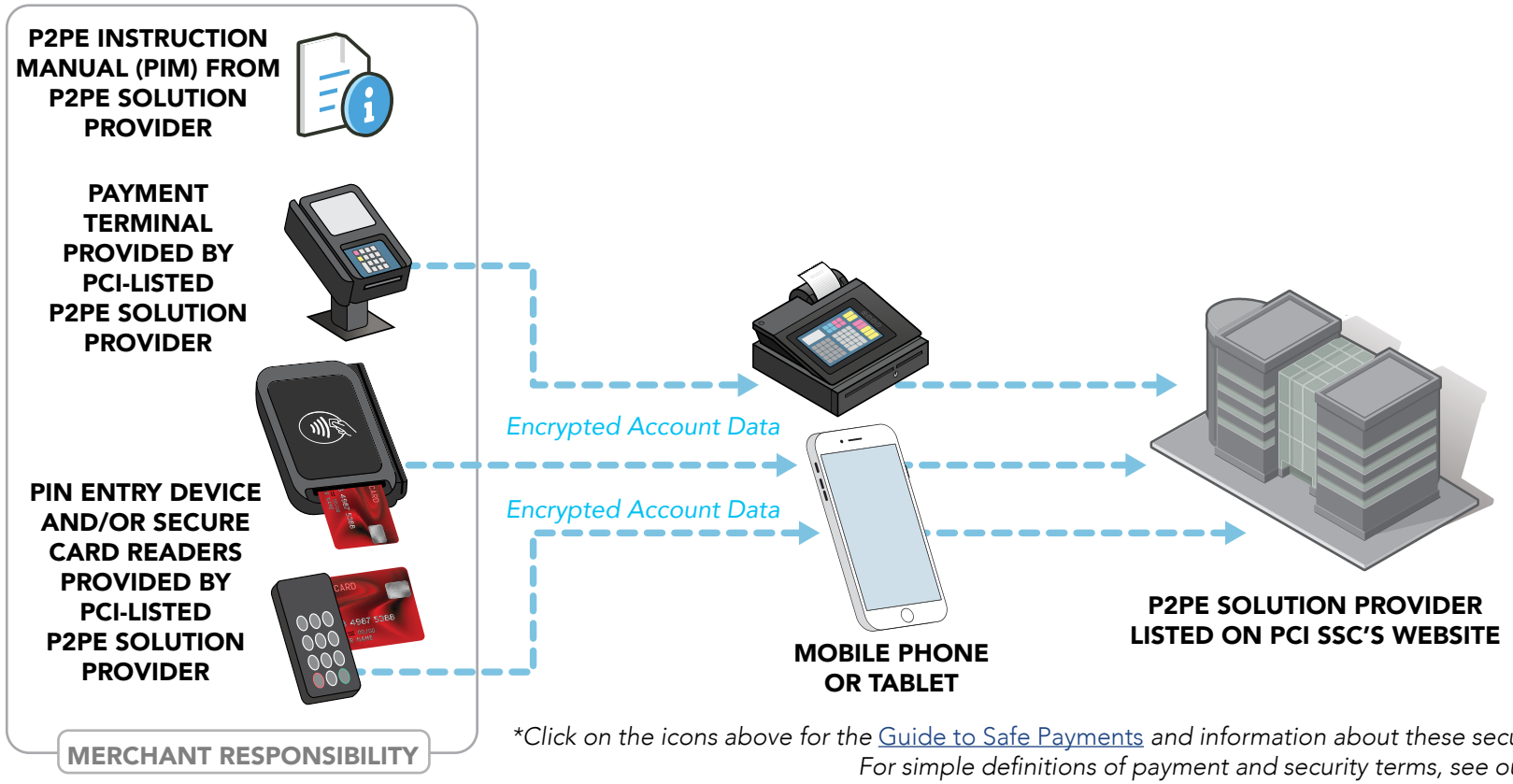
Payment terminal encrypts card data via a PCI-listed Point-to-Point Encryption Solution. Payments sent to PCI-listed P2PE Solution Provider.

RISK PROFILE

LOWEST

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.*

TYPE 16

Common Petroleum & Fuels Environment

RISK PROFILE

HIGHER

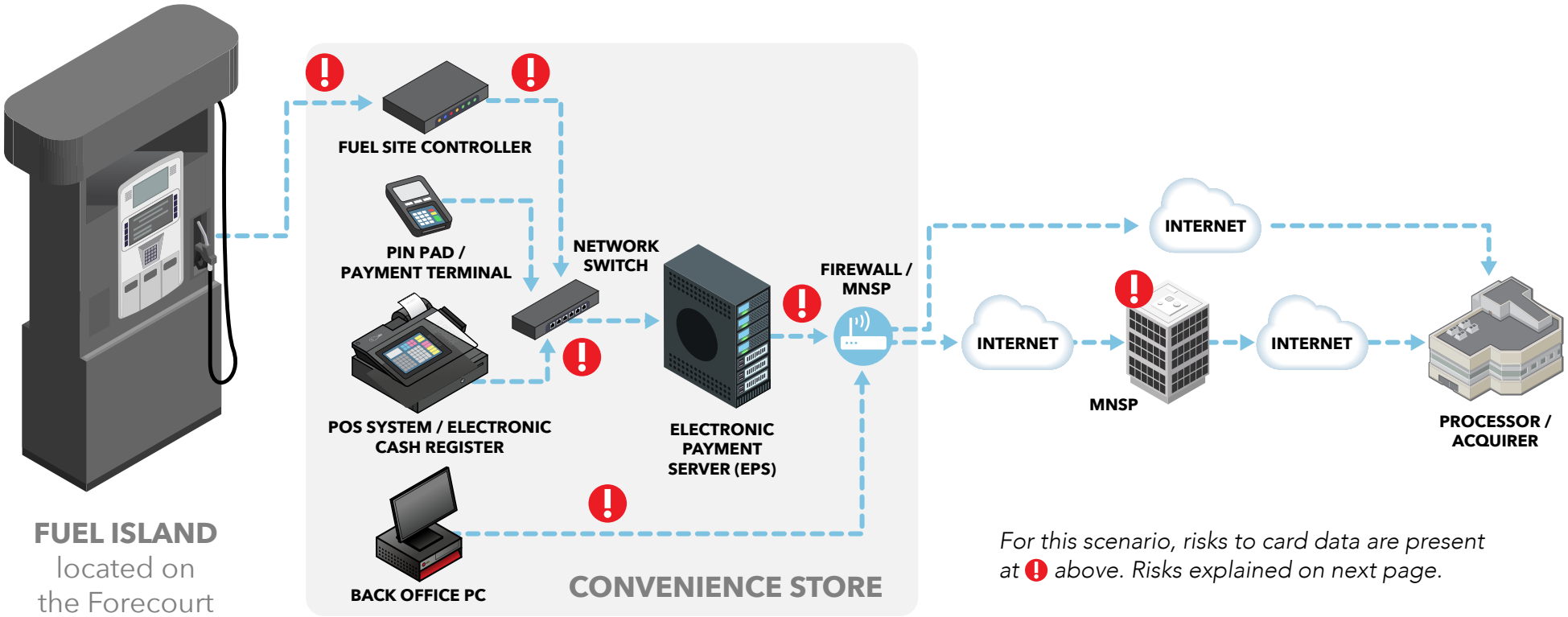
This typical petroleum retail point of sale has connections to the fuel dispensers residing in the forecourt, allowing consumers to pay for directly at the pump / fueling station. This is similar to an unattended terminal. However, pay at the pump also offers fleet card holders the ability to pay with their fleet card and other, accurate qualifications such as a Driver or Vehicle ID number.

Outside at the fuel island:
The consumer presents their card to the fuel dispenser card reader (wave, tap, or insert). The card reader sends the payment information to the fuel/site controller, which then sends the payment information to the EPS, which then sends the payment information to the payment processor / acquirer.

Inside the convenience store:
The consumer presents their card to the PIN Pad/Payment terminal card reader (wave, tap, or insert). The PIN pad sends the payment information either to the POS system or directly to the Electronic Payment Server (EPS), which then sends the payment information to the payment processor / acquirer.

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.

Common Petroleum & Fuels Environment

RISK PROFILE
HIGHER

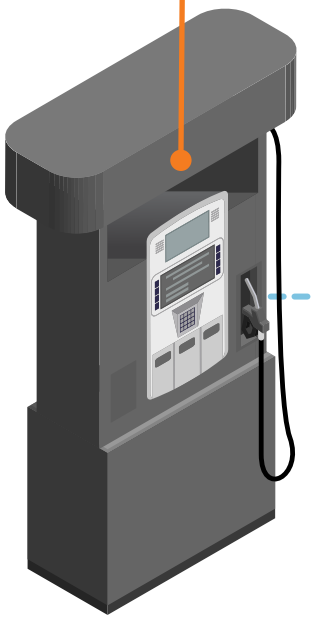
Where is your card data at risk?

Skimmers or Shimmers to skim card data. Most often skimmers and shimmers are found inside the fuel dispenser. Regular inspections will aid in detection of rogue devices inserted into this equipment

Fuel Dispenser PIN Pad to Fuel Site controller is typically not encrypted and is susceptible to attack if intercepted. Fuel/Site controller password must be reset from default – may be overlooked by installation technicians

PIN Pad to POS Technician enables encryption

Electronic card data in transit from payment terminal to processor



FUEL SITE CONTROLLER

PIN PAD / PAYMENT TERMINAL

NETWORK SWITCH

POS SYSTEM / ELECTRONIC CASH REGISTER

ELECTRONIC PAYMENT SERVER (EPS)

FIREWALL / MNSP

INTERNET

INTERNET

INTERNET

MNSP

PROCESSOR / ACQUIRER

POS to EPS

EPS to firewall/MNSP (Managed Network Service Provider) transactions may not be encrypted, creating theft risk of data in motion

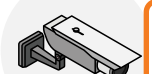
FUEL ISLAND located on the Forecourt

BACK OFFICE PC

CONVENIENCE STORE

Back Office PC to POS for price book, end of day accounting, etc

Tank Monitoring or other monitoring systems feeding information to the POS

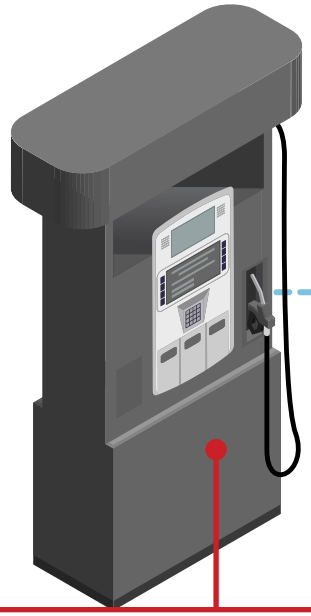


Store devices such as surveillance system or cooler monitoring system connected to Back Office PC

Common Petroleum & Fuels Environment

RISK PROFILE
HIGHER

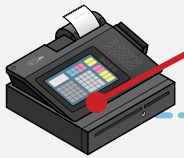
How do criminals get your card data?



FUEL SITE CONTROLLER

PIN PAD / PAYMENT TERMINAL

NETWORK SWITCH



POS SYSTEM / ELECTRONIC CASH REGISTER

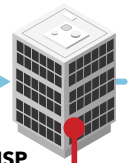
ELECTRONIC PAYMENT SERVER (EPS)

BACK OFFICE PC

FIREWALL / MNSP

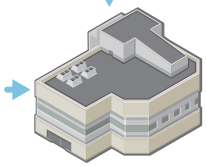
INTERNET

INTERNET



MNSP

INTERNET



PROCESSOR / ACQUIRER

POS System
- "Skimming" equipment attached to (or embedded into) your payment terminal.
- PIN pad overlay devices can harvest payment card data and steal consumer PINs.

POS System / EPS
- An attack can occur by mis-configured or vulnerable remote access solutions
- Deliberate or unintentional by technician, vendor or anyone with remote access
- Cloud configuration downloads
- Vendor management portals
- Remote Key Management

Unattended Terminal
- Skimming
- Pump doors that are easy to open because of weak / default locks
- Outdated un-secure card readers
- Untrusted assets connected for upgrades (Pump Techs laptop)
- Fraudsters posing as a pump tech
- Insecure forecourt controller communications

Back Office PC
- Remote access to back office PC
- Additional network cards that can bypass firewall protections
- Shared credentials across applications
- Applications that push data into the CDE, such as automated fuel pricing solutions
- Bypassing network security controls (firewall)
- Malware/software inserted onto a payment terminal that facilitates the theft of card data

Mobile Payments / Above Site
- eCommerce Threats

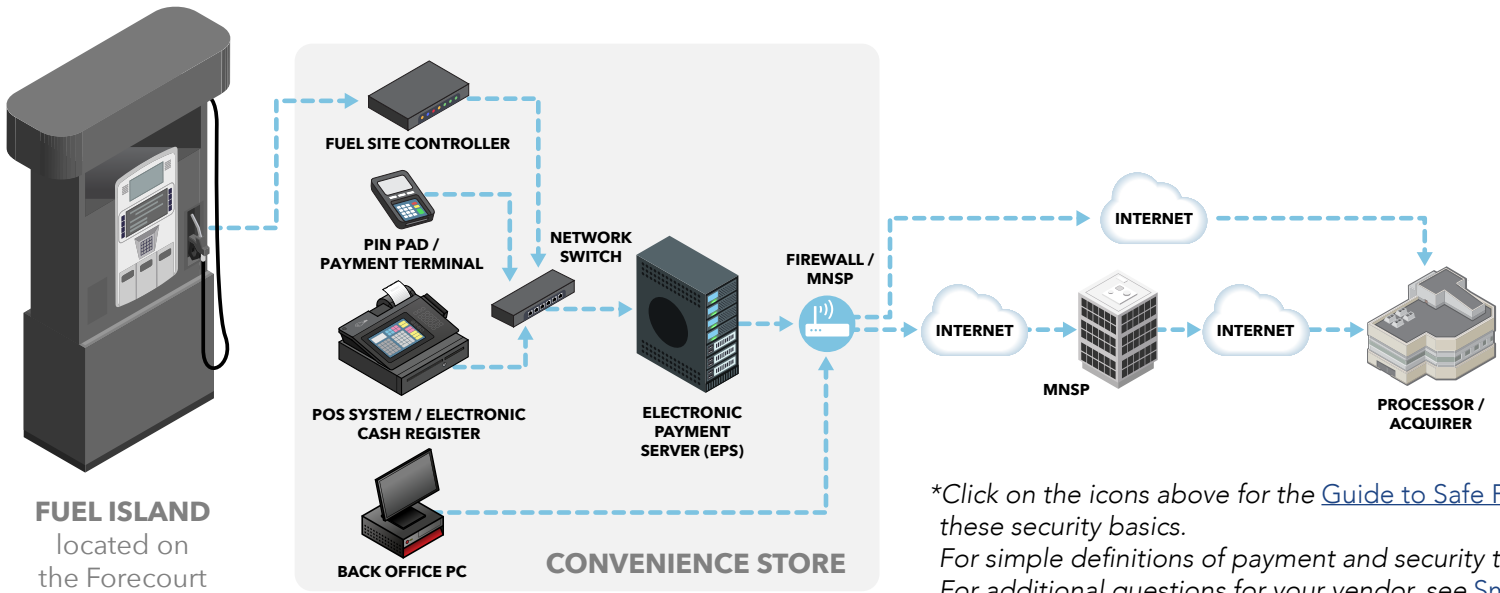
Firewall/MNSP
- Access via misconfigured or out-of-date software
- Access via insecure Wi-Fi devices
- Intentional bypassing of firewall rules and or physical connections
- Unauthorized devices attached to the network

Common Petroleum & Fuels Environment

RISK PROFILE
HIGHER

How do you start to protect card data today?*

- Change default passwords, use strong passwords, Multi-factor Authentication (MFA)
- Protect card data and only keep what you need
- Regularly inspect your payment terminals for modification, changes, or other visual clues that suggest tampering or alteration
- Install software patches from your payment terminal vendor
- Use a robust, business grade firewall appliance with unified threat management
- Ask your PCI Qualified Integrator & Reseller (QIR) or your hardware/software vendor for help
- 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
- Protect network and USB ports
- Use secure payment systems
- Protect all systems from the Internet
- Use anti-virus or "application allow" 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.
For additional questions for your vendor, see Small Merchant Questions for Vendors.

Resources

Infographics and Videos

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

PCI Data Security Essentials for Small Merchants and Related Guidance

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