PAYMENT PROTECTION RESOURCES FOR SMALL MERCHANTS

Common Payment Systems

Version 1.0 | July 2016

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®

Payment system types at-a-glance

Type	Payment System Description
1	Dial-up payment terminal. Payments sent via phone line.
2	Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.
3	Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.
4	Encrypting payment terminal connected to electronic cash register. Payment sent via Internet by electronic cash register.
5	Encrypting payment terminal and electronic cash register connected to Internet. Payments sent via Internet.
6	Encrypting payment terminal and electronic cash register share non-card data (semi-integrated). Payments sent via Internet by payment terminal.
7	Integrated payment terminal and payment middleware share card data. Payments send via Internet.
8	Encrypting wireless payment terminal ("Pay-at-Table") with integrated payment terminal and "middleware." Payments sent via Internet.
9	Payment terminal connected to electronic cash register, with additional connected equipment. Payments sent via Internet.
10	E-commerce merchant with fully outsourced payment page. Payments sent via Internet by third-party provider.
11	E-commerce merchant accepts payments on own payment page and manages own website. Payments sent via Internet by merchant.
12	Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.
13	Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.
14	Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

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.

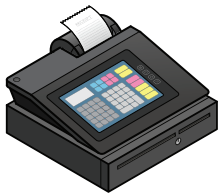
PROTECT CARD DATA AND YOUR BUSINESS WITH SECURITY BASICS:

- 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*.

What do these terms mean?

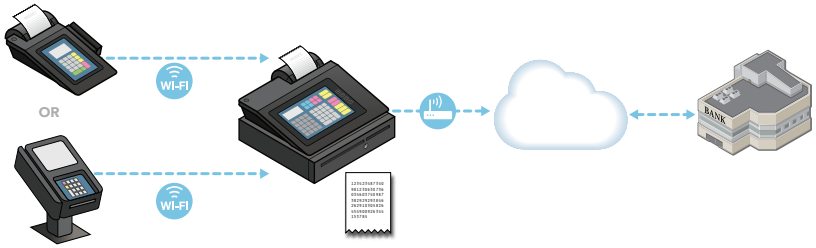
Depending on where in the world you are located, equipment used to take payments is called by different names. Here are the types we reference in this document and what they are commonly called.

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.

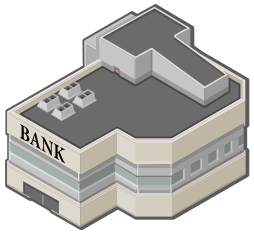


An **ELECTRONIC CASH REGISTER** (or till) registers and calculates transactions, and may print out receipts, but it does not accept customer card payments.

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 **PAYMENT SYSTEM** encompasses the entire process for accepting card payments in a retail location (including stores/shops and e-commerce storefrontsfronts), and 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), servers with e-commerce components such as payment pages, and the connections out to a merchant bank.



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.

TYPE 1

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

RISK PROFILE

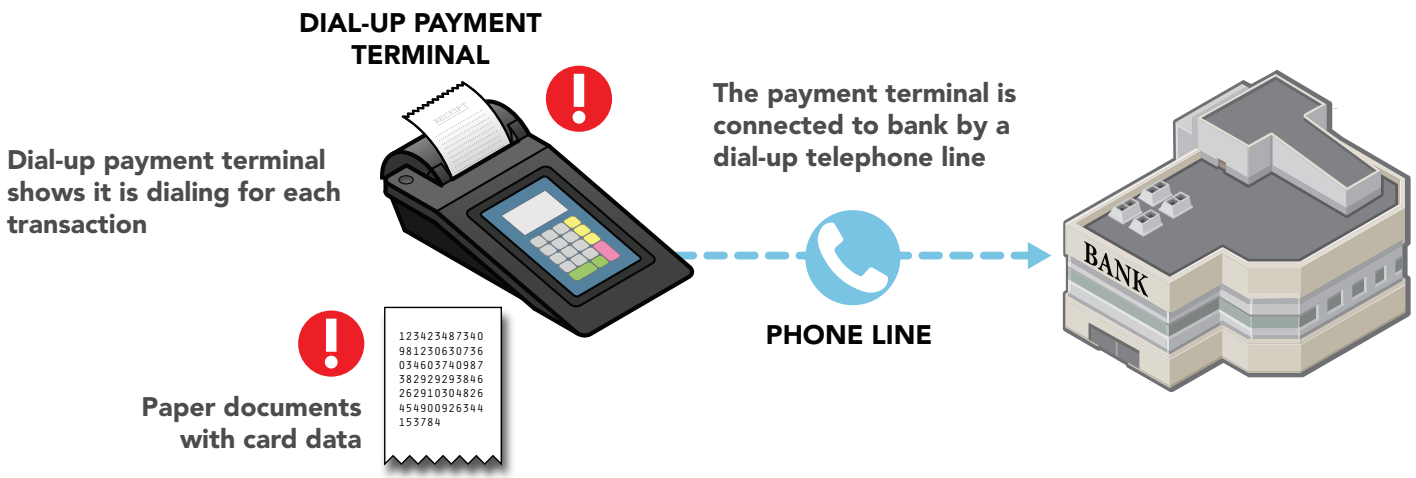
Chip LOWER

Mag Stripe LOWER

TYPE 1 OVERVIEW | TYPE 1 RISKS | TYPE 1 THREATS | TYPE 1 PROTECTIONS

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.



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

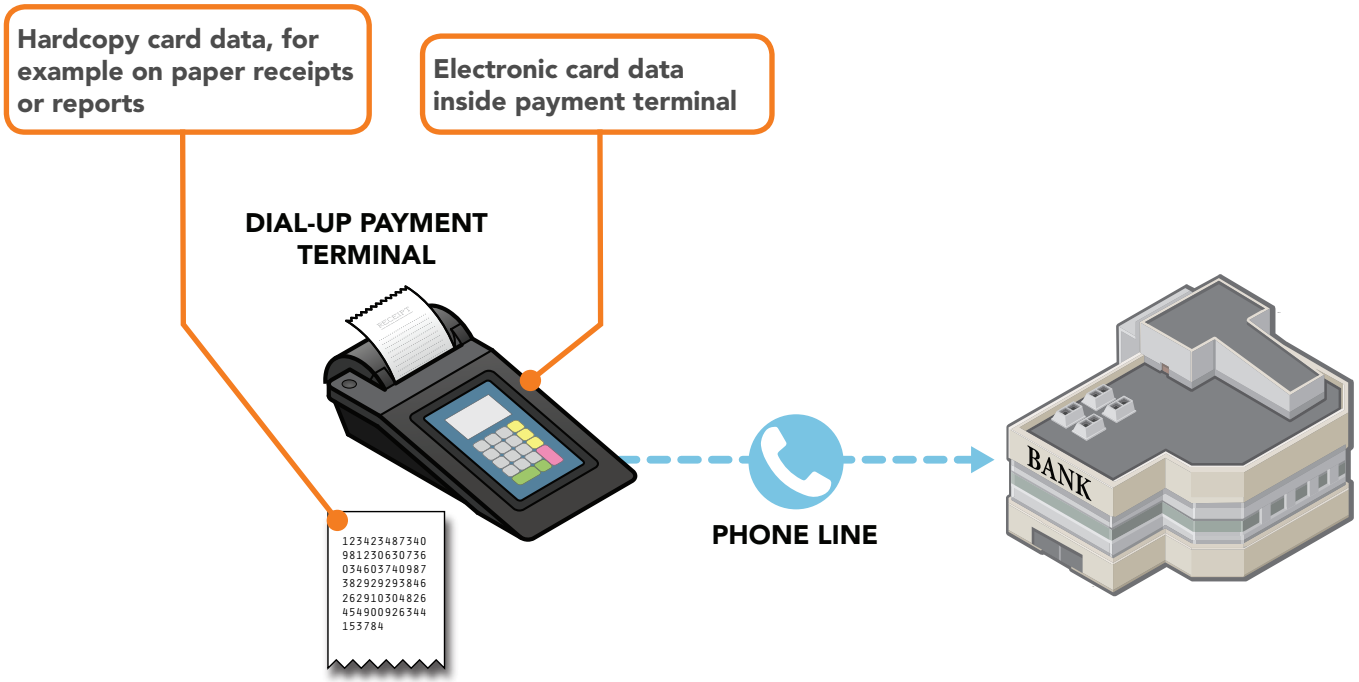
Dial-up payment terminal. Payments sent via phone line.

RISK PROFILE

Chip LOWER

Mag Stripe LOWER

Where is your card data at risk?



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

RISK PROFILE

Chip LOWER

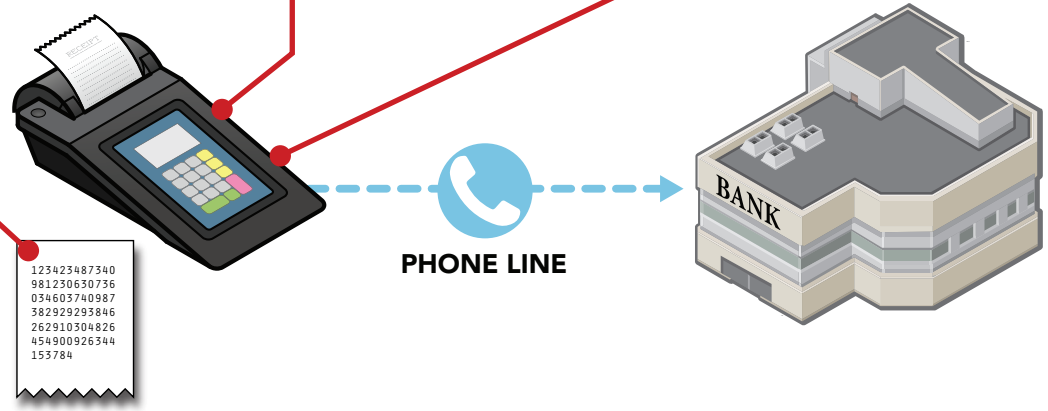
Mag Stripe LOWER

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.



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

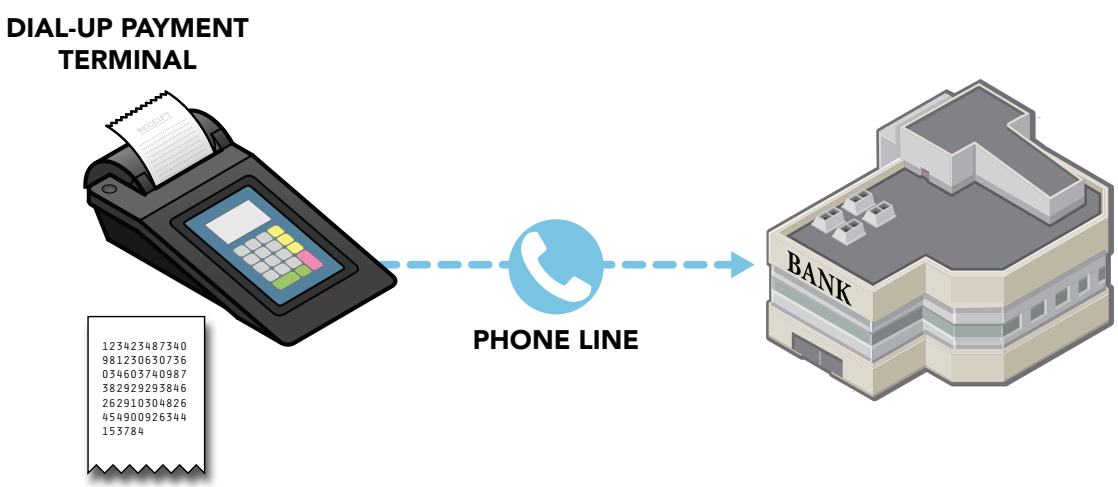
RISK PROFILE

Chip LOWER

Mag Stripe 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



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

TYPE 2

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

RISK PROFILE

Chip: LOWER

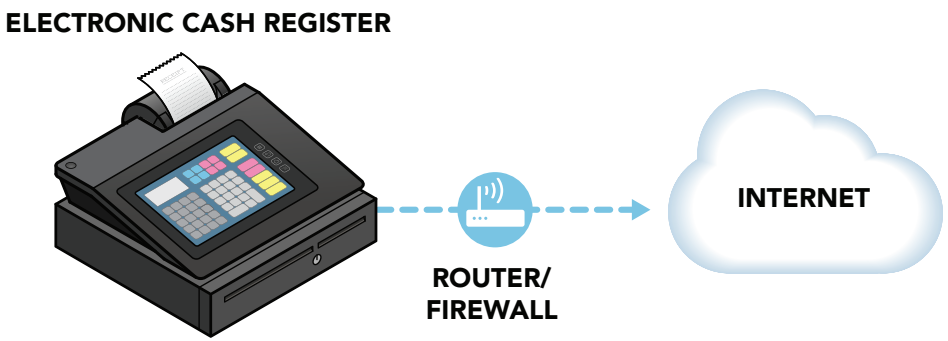
Mag Stripe: LOWER

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.

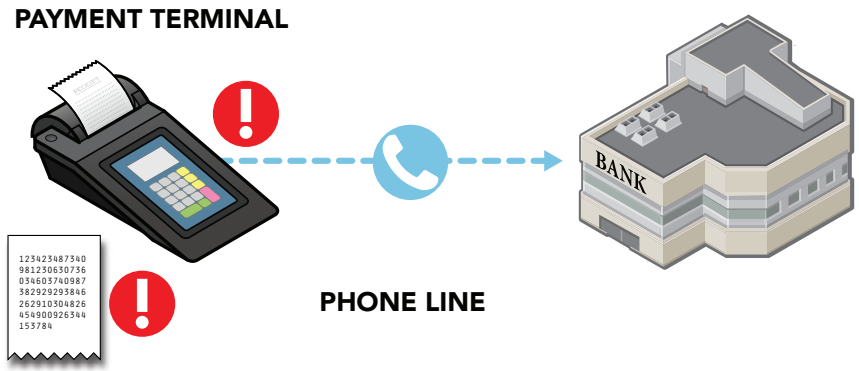
BACK
to previous diagram.

Electronic cash register connected to the Internet, but no card payments taken here



Total sale amount is manually entered in the payment terminal

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



Paper documents with card data

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

TYPE 2

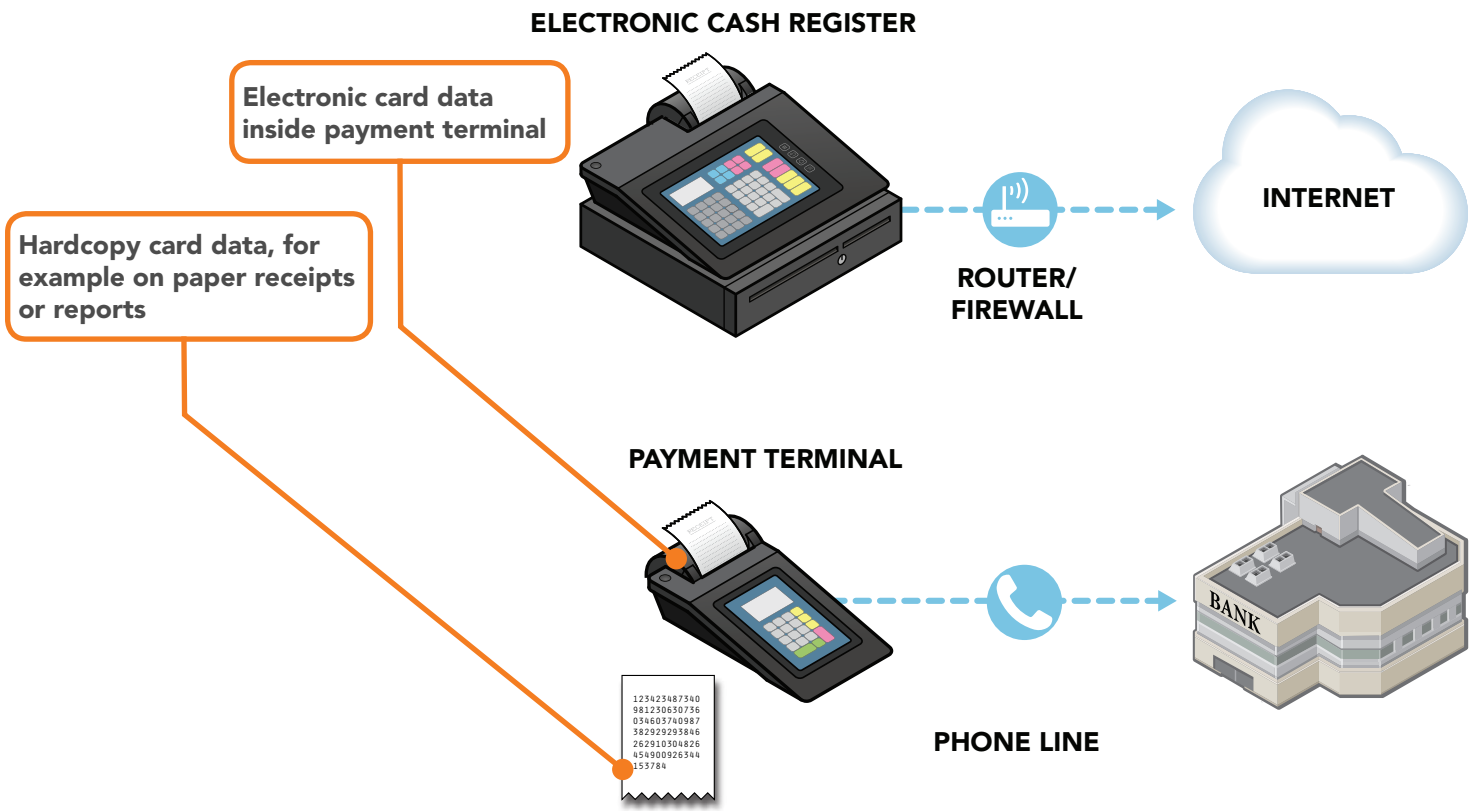
Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.

RISK PROFILE

Chip LOWER

Mag Stripe 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

Chip: LOWER

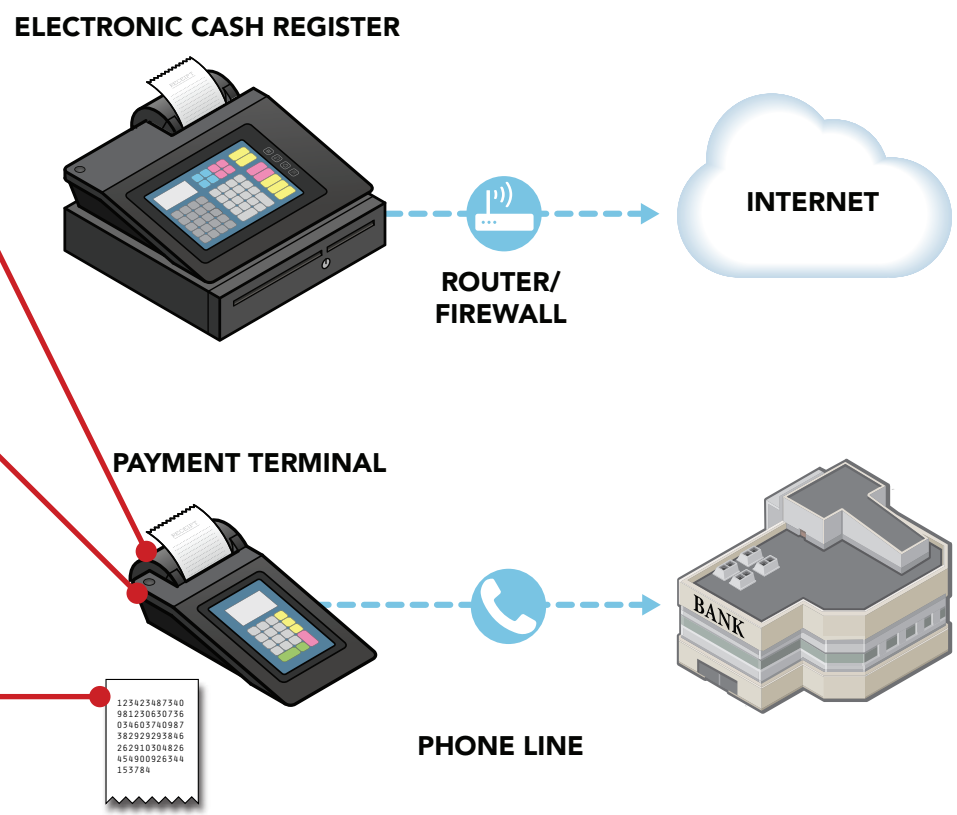
Mag Stripe: LOWER

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.

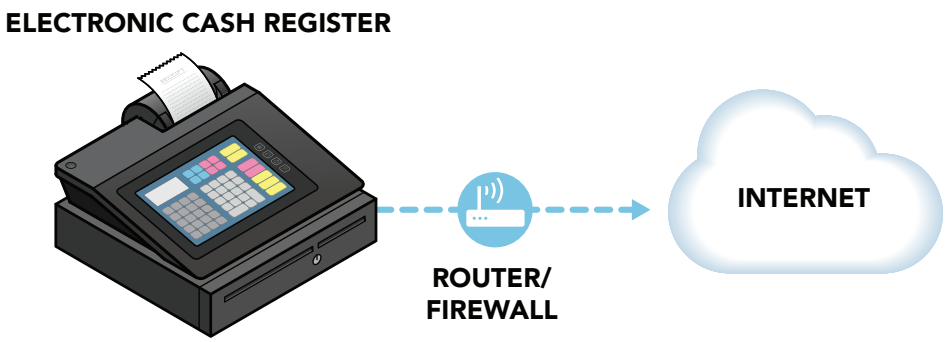
RISK PROFILE

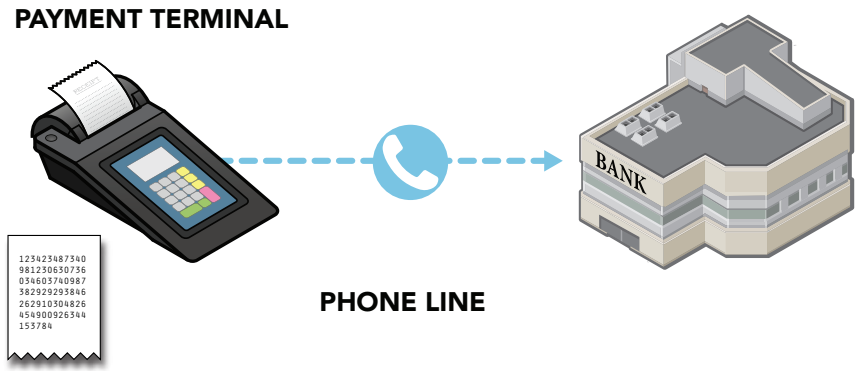
Chip: LOWER

Mag Stripe: 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





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

TYPE 3

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

RISK PROFILE

Chip: MODERATE

Mag Stripe: HIGHER

YES
This IS my setup.
Show me the details.

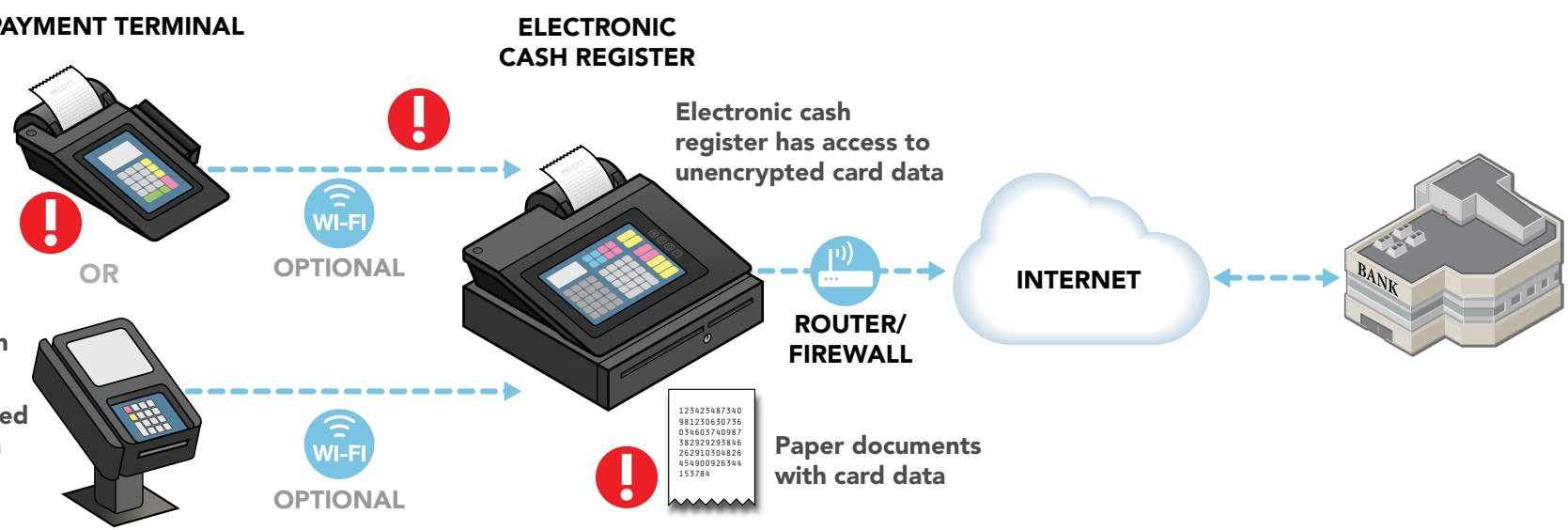
NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

Payment terminal captures customers' card data

Has access to unencrypted card data, and may encrypt card data before transmission

No other equipment connected to merchant payment system



Card data sent to electronic cash register

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

TYPE 3

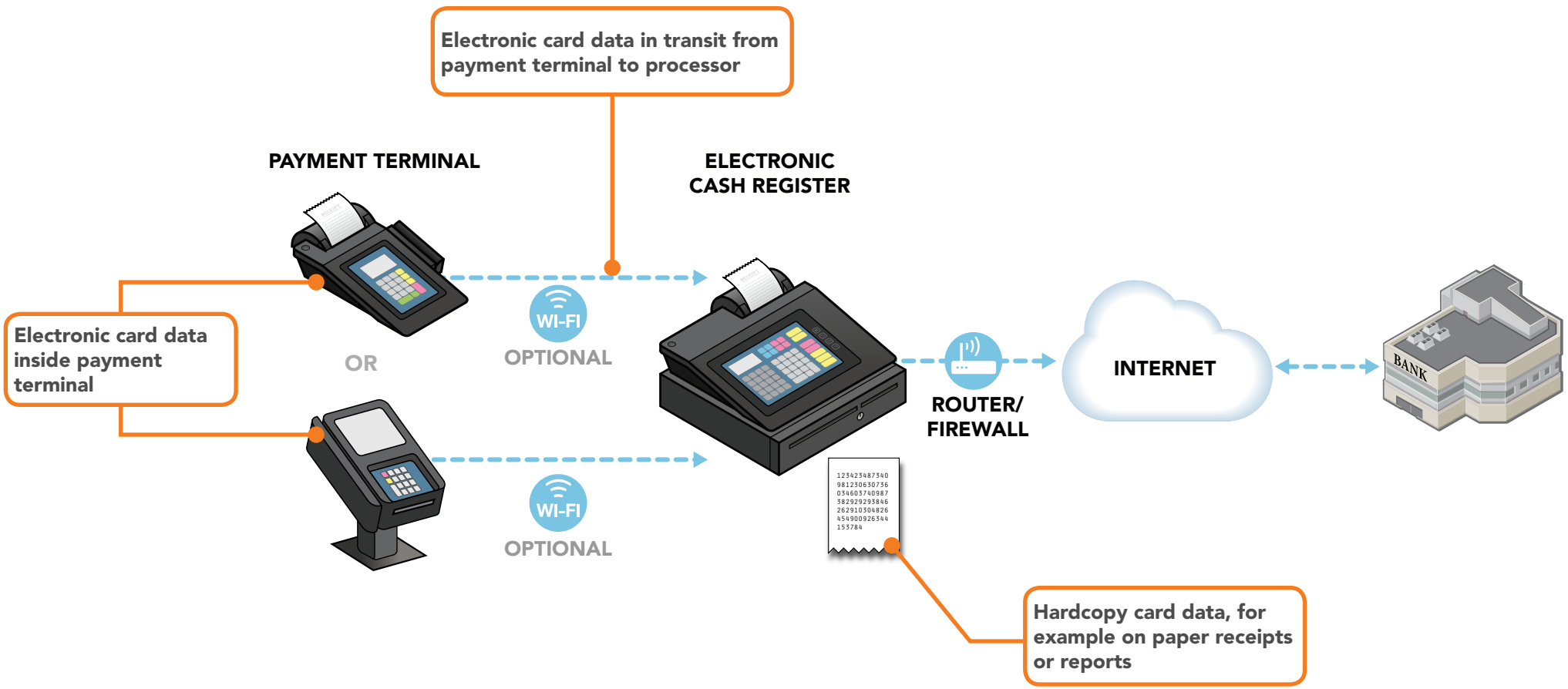
Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

RISK PROFILE

Chip: MODERATE

Mag Stripe: HIGHER

Where is your card data at risk?



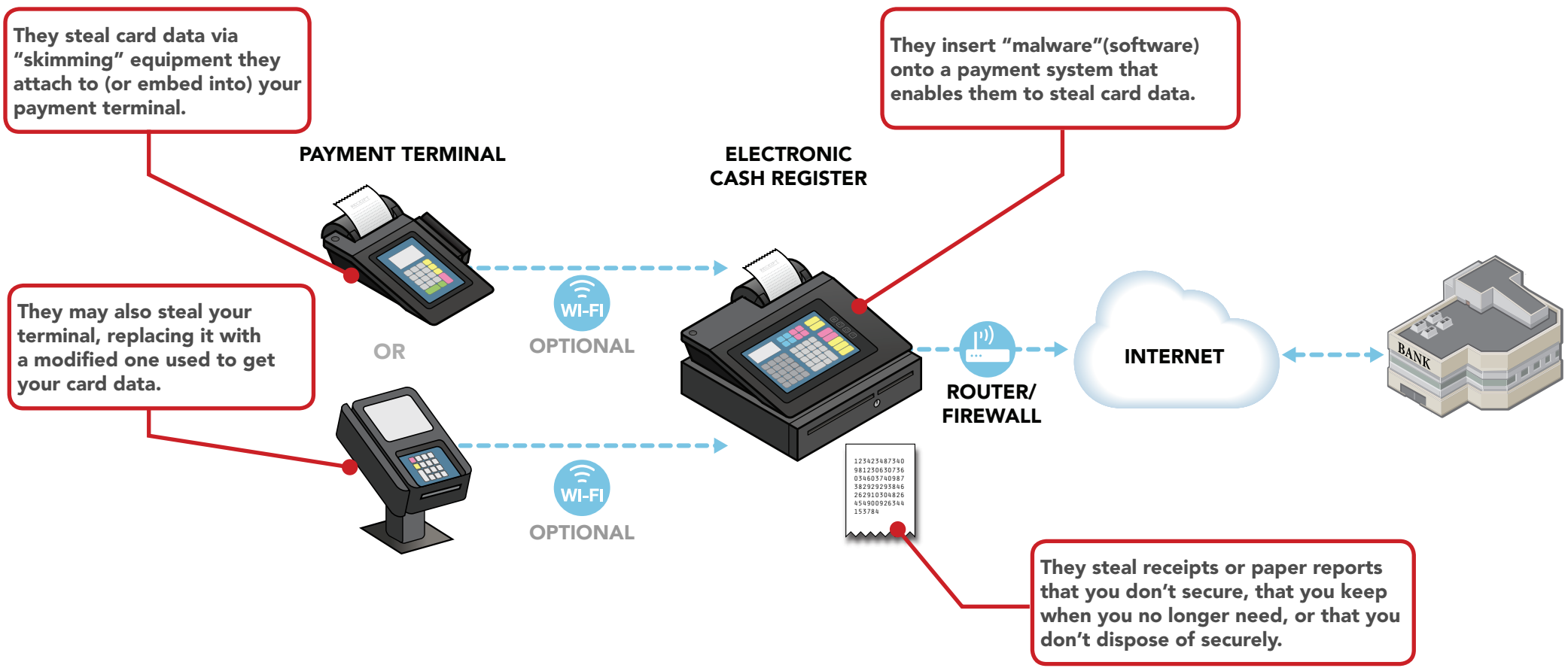
Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

RISK PROFILE

Chip: MODERATE

Mag Stripe: HIGHER

How do criminals get your card data?



TYPE 3

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

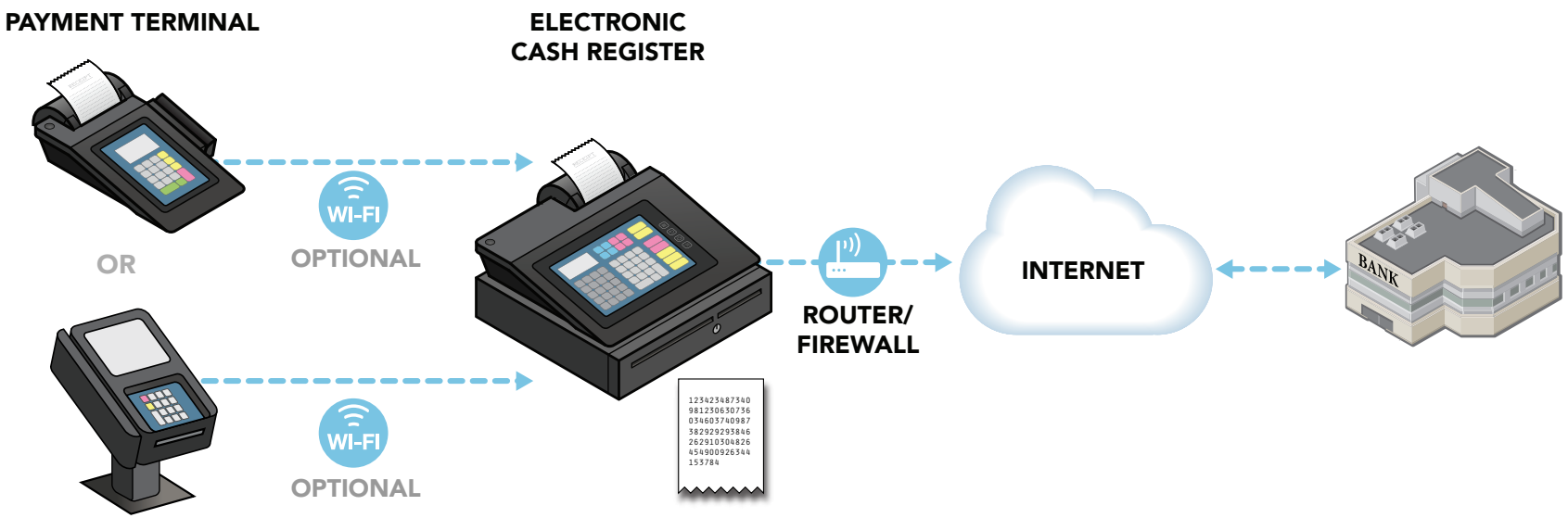
RISK PROFILE

Chip: MODERATE

Mag Stripe: HIGHER

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
- Limit in-house access to your card data
- Get regular vulnerability scanning
- Use a secure payment terminal
- 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.

PCI Security Standards Council

TYPE 4

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

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

YES
This IS my setup.
Show me the details.

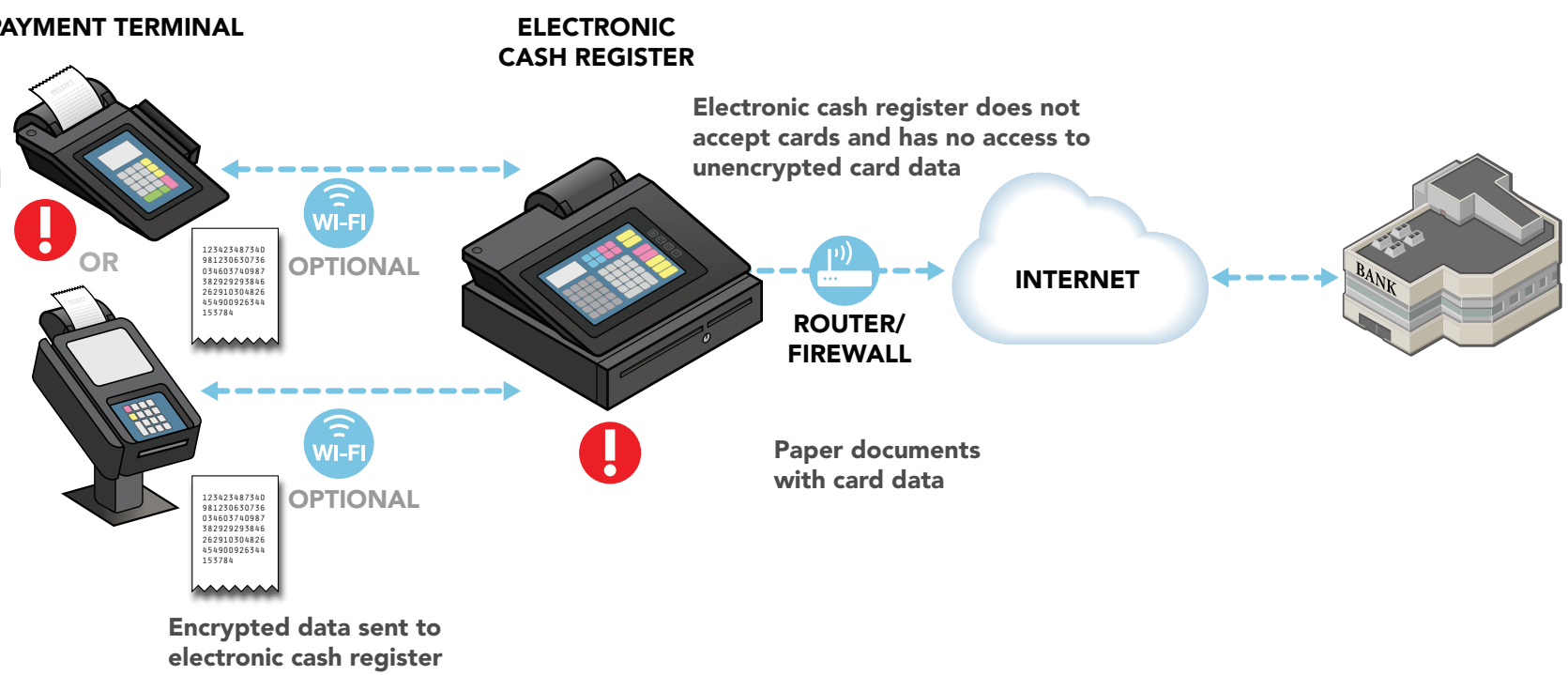
NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

Payment terminal encrypts card data (for example, using PCI's Secure Reading & Exchange of Data – SRED)

Merchant has no access to unencrypted data

No other equipment connected to merchant payment systems



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

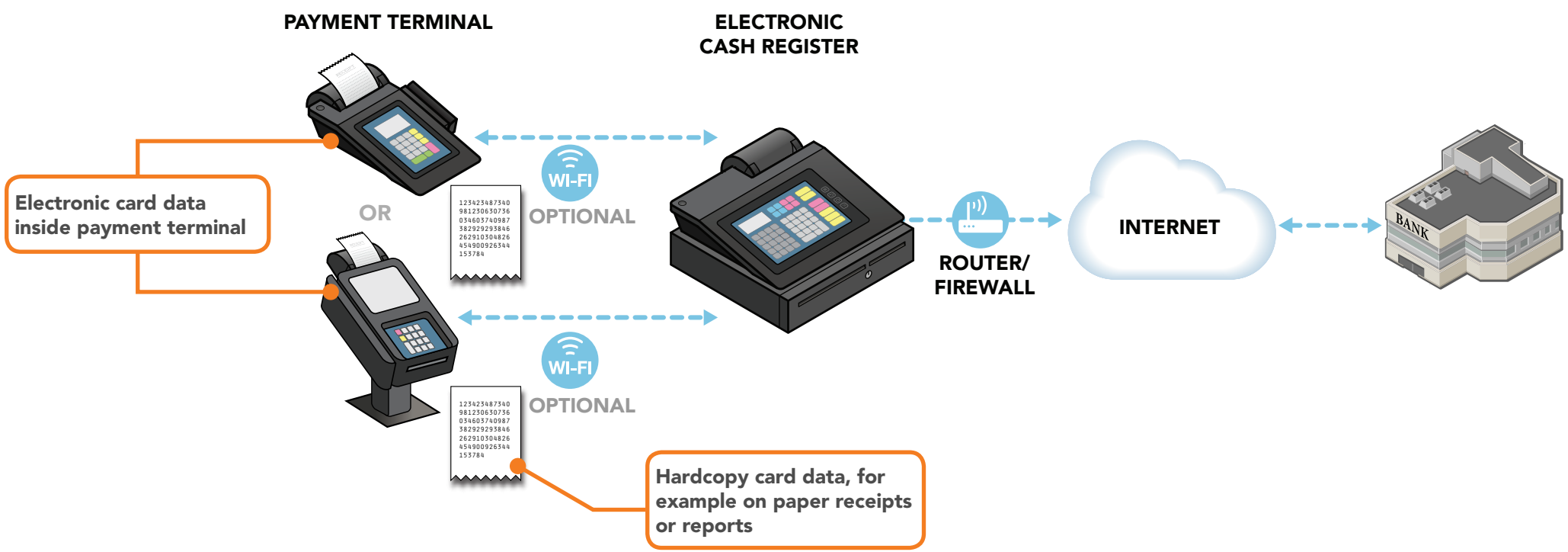
Encrypting payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

Where is your card data at risk?



TYPE 4

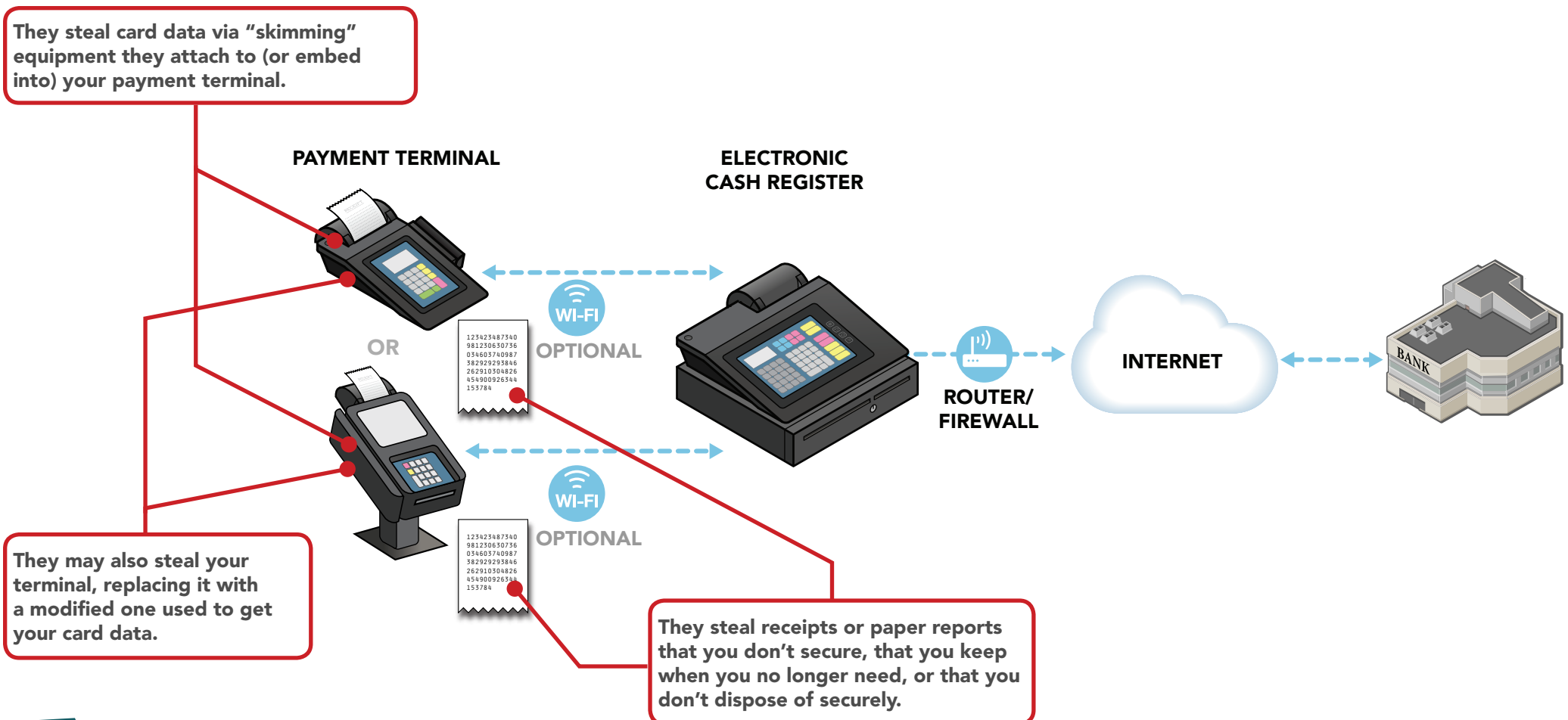
Encrypting payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

How do criminals get your card data?



PCI Security Standards Council

TYPE 4

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

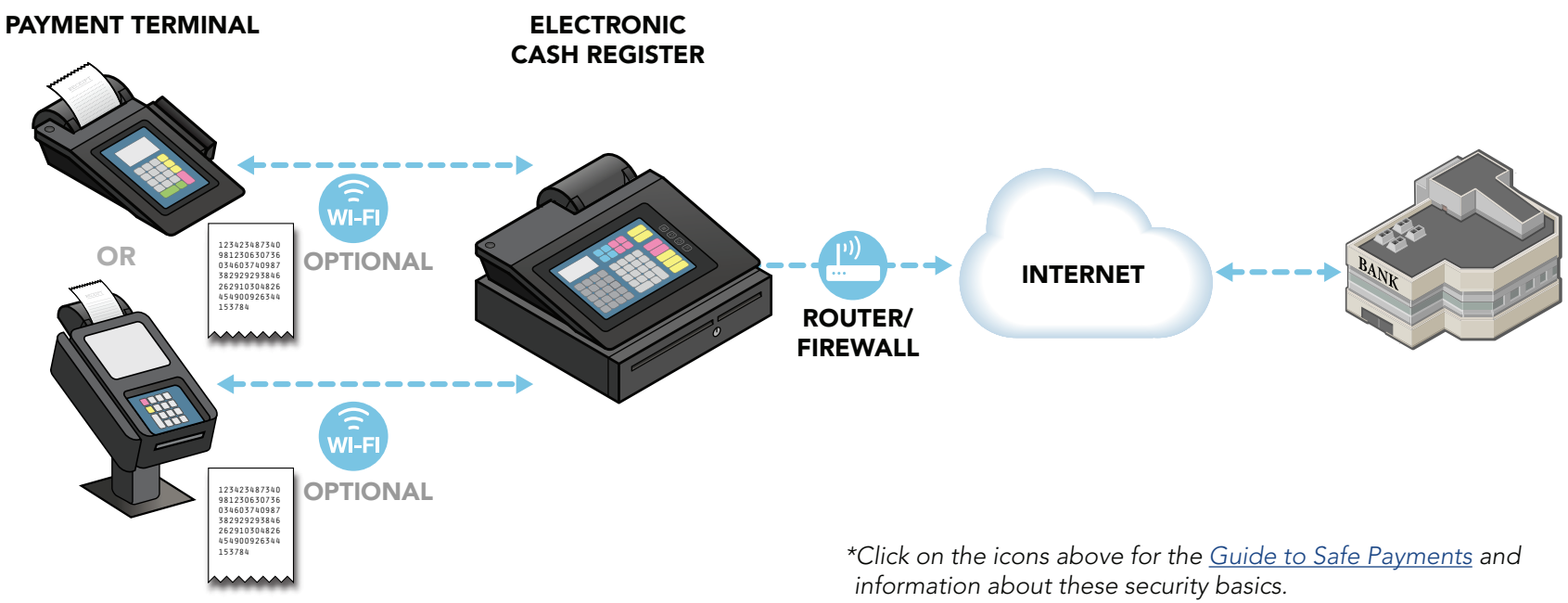
RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

How do you start to protect card data today?*

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



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

TYPE 5

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

RISK PROFILE

Chip: LOWER

Mag Stripe: LOWER

TYPE 5 OVERVIEW | TYPE 5 RISKS | TYPE 5 THREATS | TYPE 5 PROTECTIONS

YES
This IS my setup.
Show me the details.

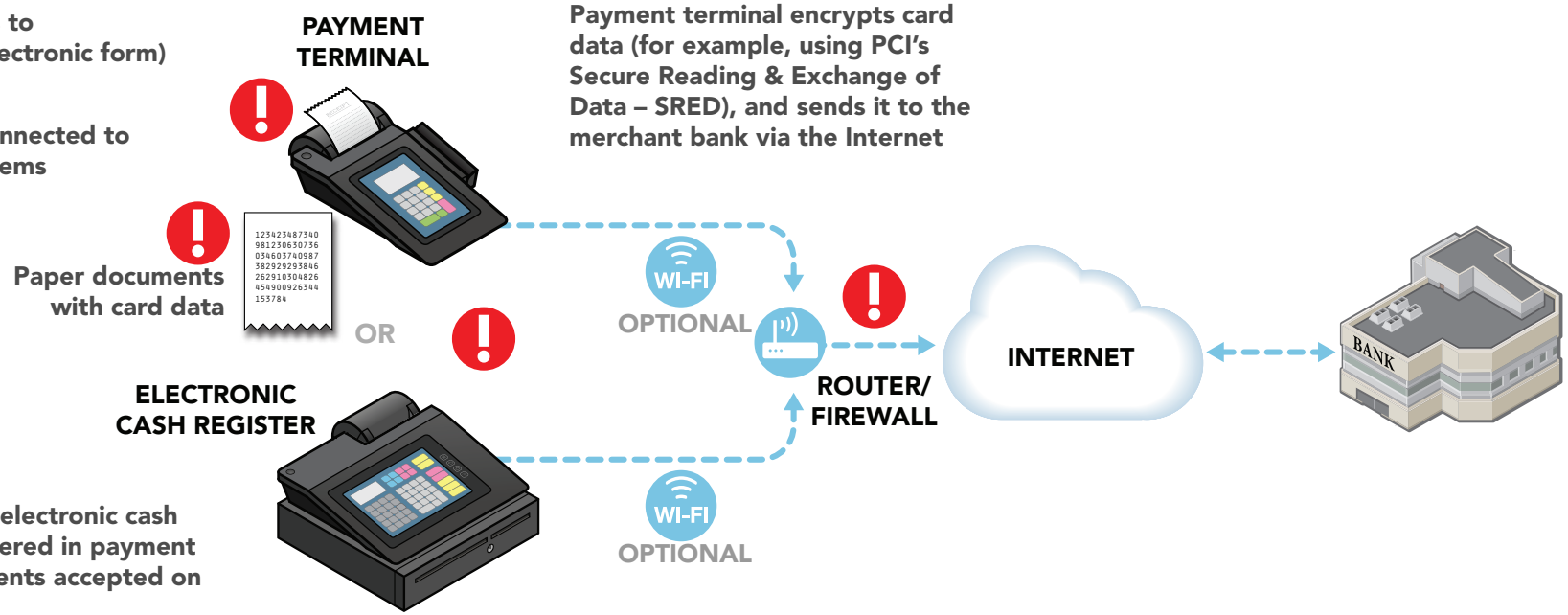
NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

Merchant has no access to unencrypted data (in electronic form)

No other equipment connected to merchant payment systems

Payment terminal encrypts card data (for example, using PCI's Secure Reading & Exchange of Data – SRED), and sends it to the merchant bank via the Internet



Total sale amount from electronic cash register is manually entered in payment terminal; no card payments accepted on electronic cash register

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

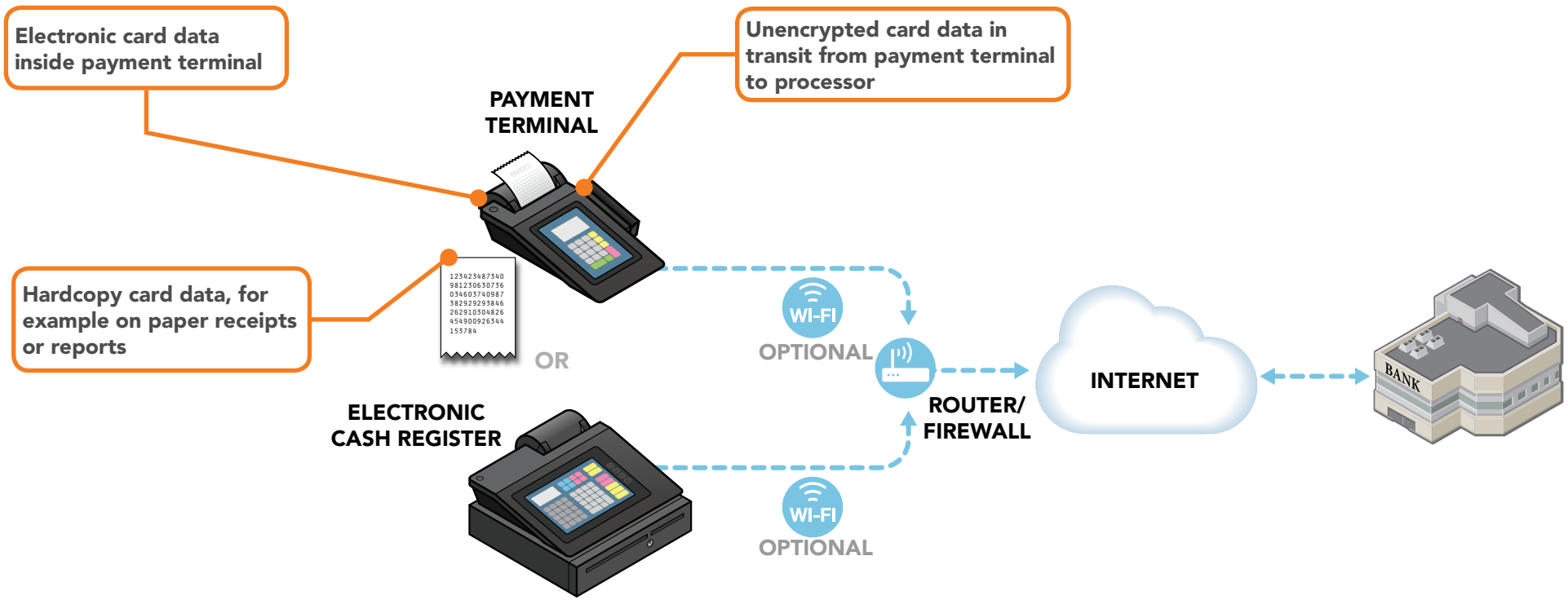
Encrypting payment terminal and electronic cash register connected to the Internet. Payments sent via Internet by payment terminal.

RISK PROFILE

Chip: LOWER

Mag Stripe: LOWER

Where is your card data at risk?



TYPE 5

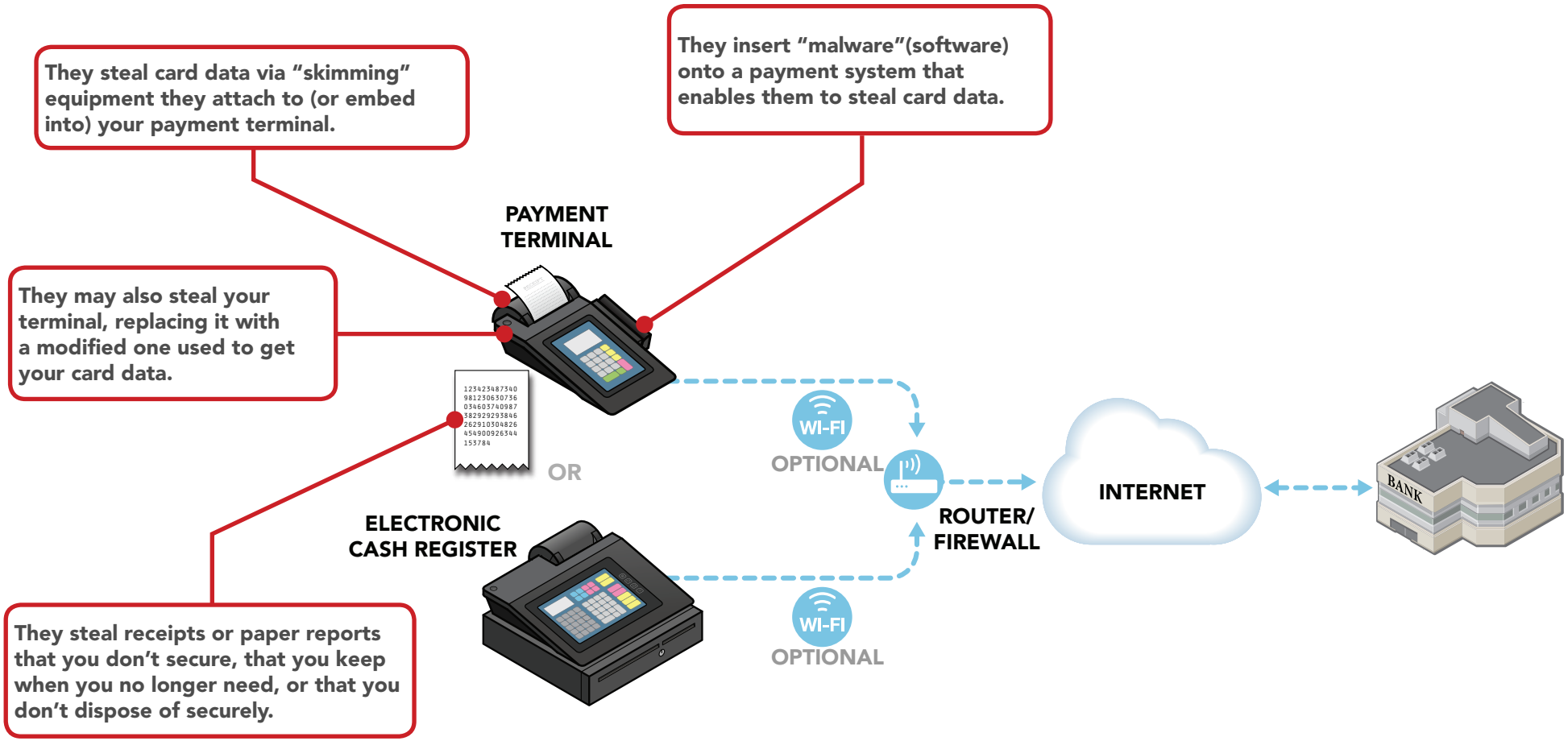
Encrypting payment terminal and electronic cash register connected to the Internet. Payments sent via Internet by payment terminal.

RISK PROFILE

Chip: LOWER

Mag Stripe: LOWER

How do criminals get your card data?



TYPE 5

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

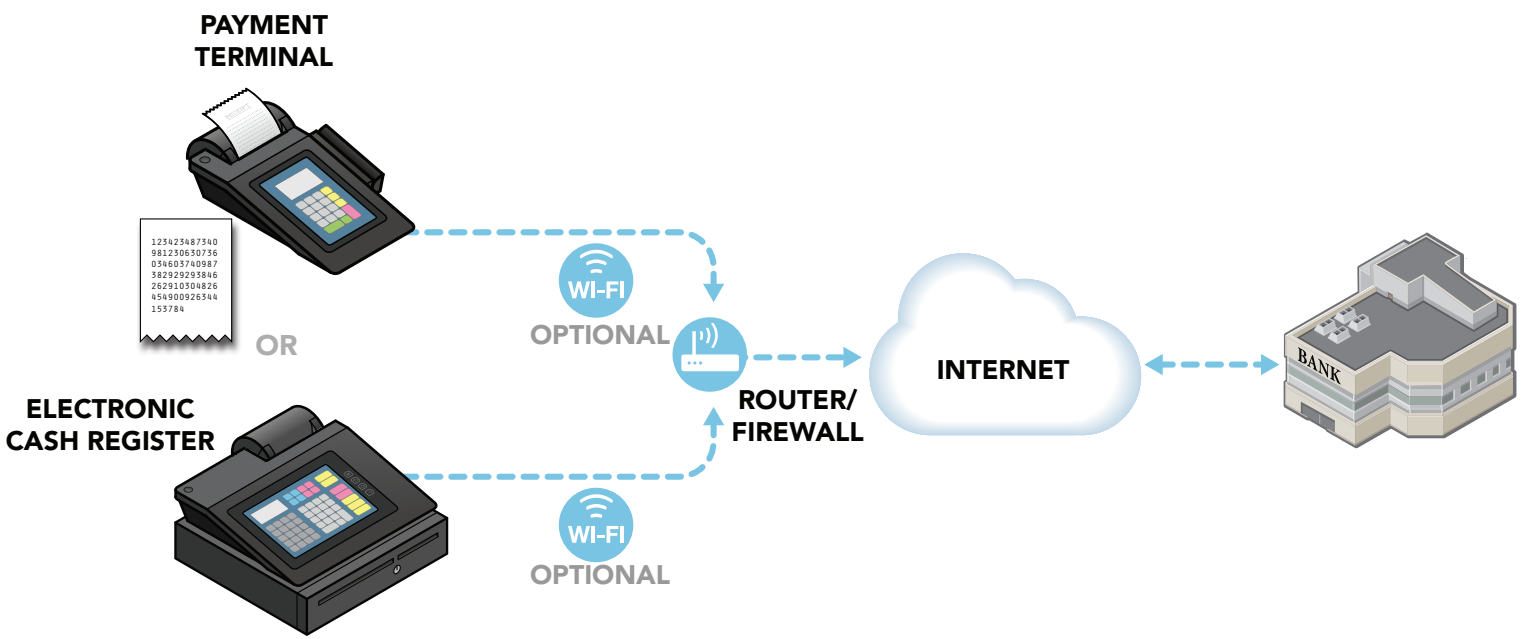
RISK PROFILE

Chip: LOWER

Mag Stripe: LOWER

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
- 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 a secure payment terminal
- Protect your business from the Internet



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

TYPE 6

Encrypting payment terminal and electronic cash register share non-card data (semi-integrated). Payment sent via Internet by payment terminal.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

TYPE 6 OVERVIEW | TYPE 6 RISKS | TYPE 6 THREATS | TYPE 6 PROTECTIONS

YES
This IS my setup.
Show me the details.

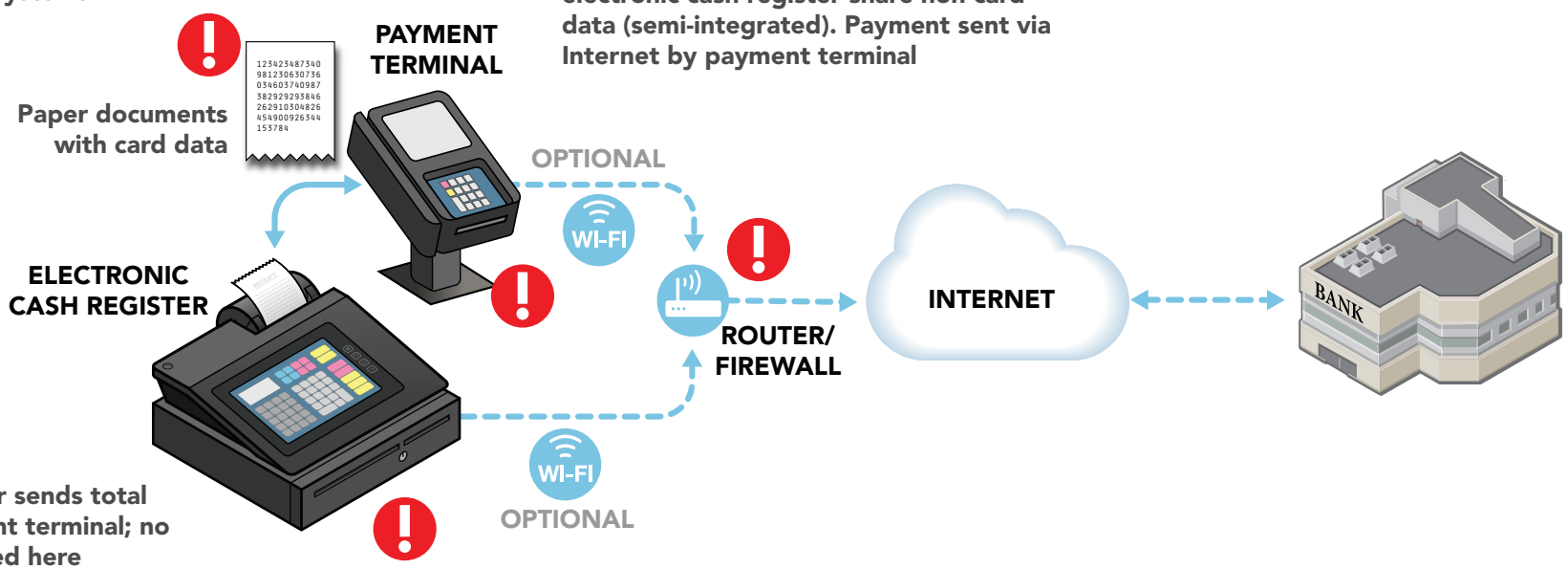
NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

No card data shared between electronic cash register and payment terminal

No other equipment connected to merchant payment systems

Encrypting payment terminal and electronic cash register share non-card data (semi-integrated). Payment sent via Internet by payment terminal



Electronic cash register sends total sale amount to payment terminal; no card payments accepted here

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

PCI Security Standards Council

TYPE 6

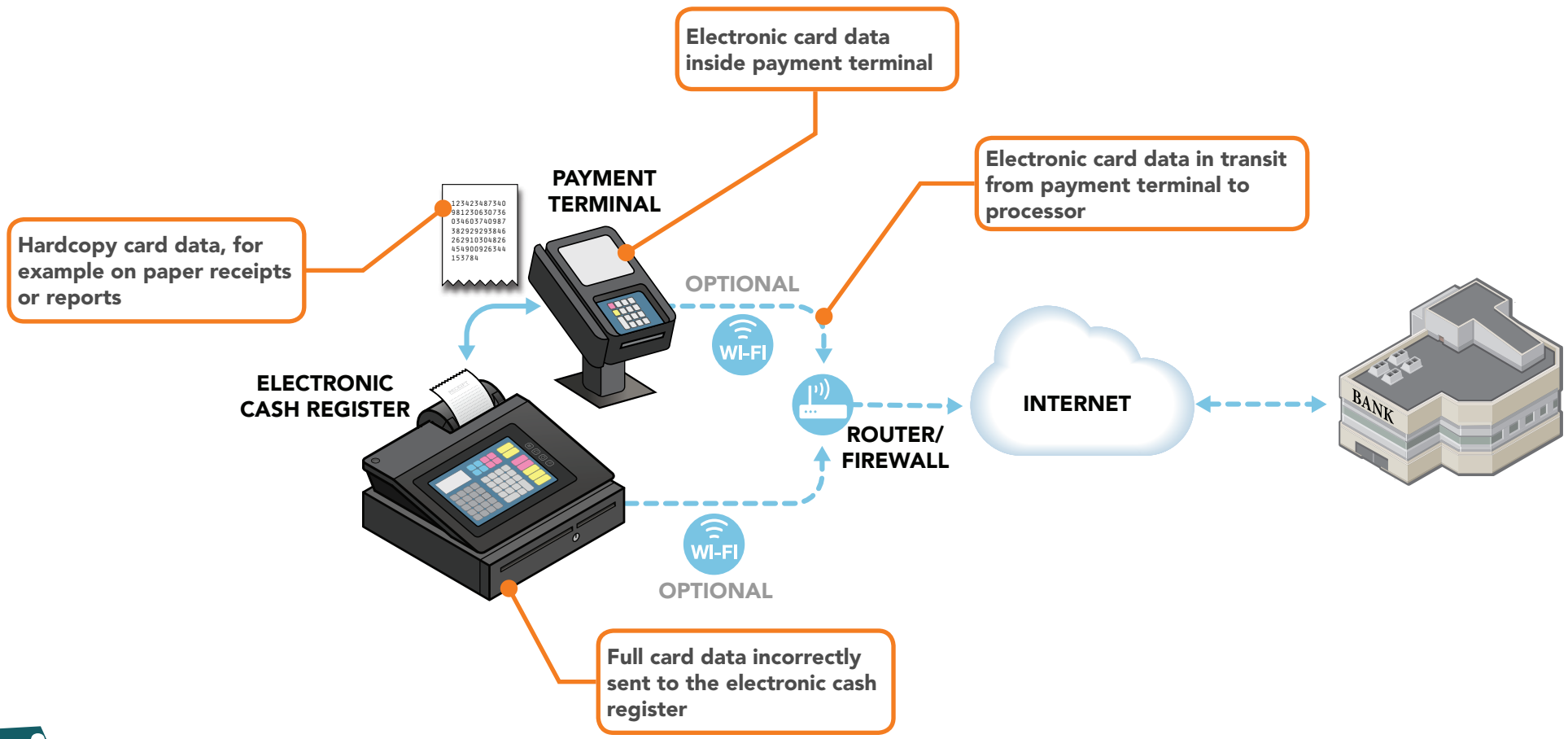
Encrypting payment terminal and electronic cash register share non-card data (semi-integrated). Payment sent via Internet by payment terminal.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

Where is your card data at risk?



PCI Security Standards Council

Encrypting payment terminal and electronic cash register share non-card data (semi-integrated). Payment sent via Internet by payment terminal.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

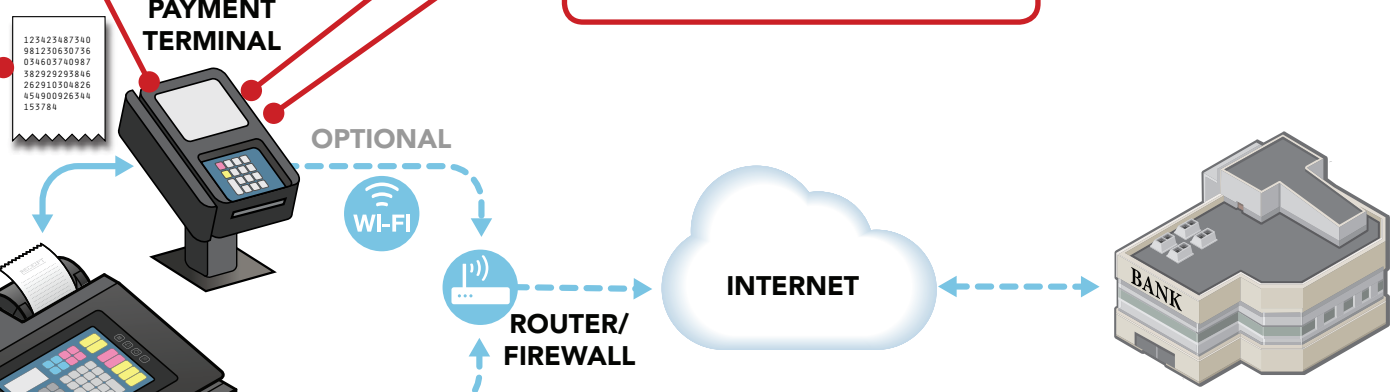
How do criminals get your card data?

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

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



They are able to steal card data incorrectly sent by payment terminal to electronic cash register due to incorrect integration between the devices. For example, for receipt printing, payment terminal should only send truncated card data to electronic cash register.

TYPE 6

Encrypting payment terminal and electronic cash register share non-card data (semi-integrated). Payment sent via Internet by payment terminal.

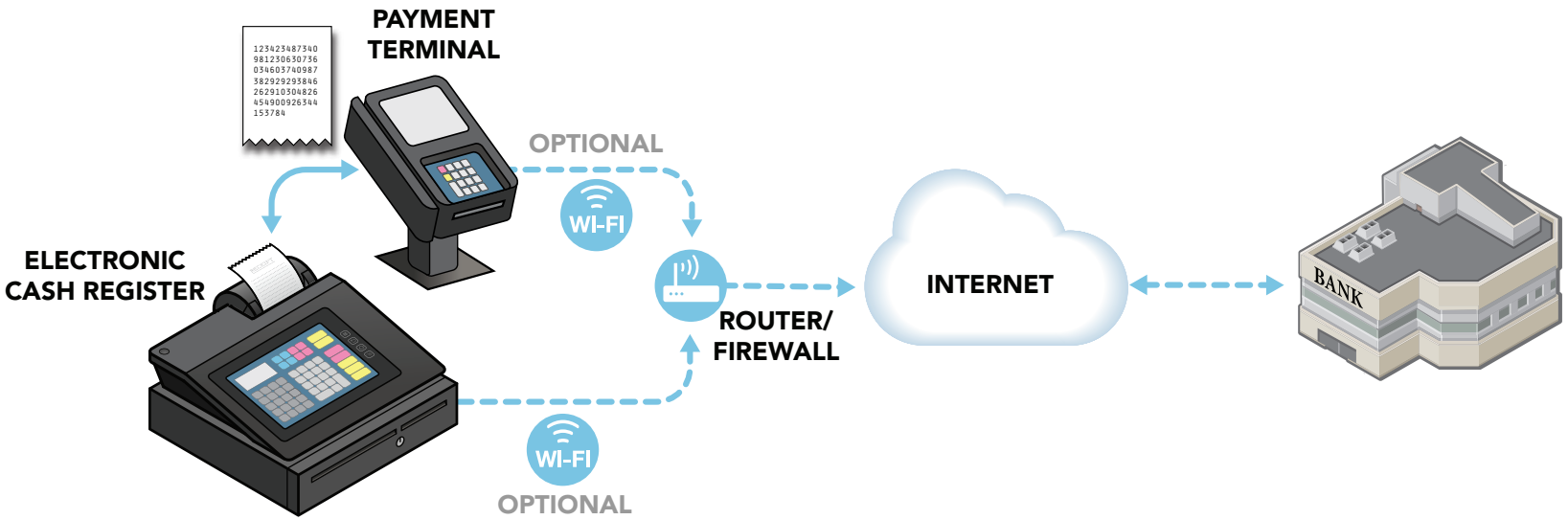
RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

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
- 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 a secure payment terminal
- Protect your business from the Internet



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

TYPE 7

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

RISK PROFILE

Chip

Mag Stripe

HIGHER

TYPE 7 OVERVIEW | TYPE 7 RISKS | TYPE 7 THREATS | TYPE 7 PROTECTIONS

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.

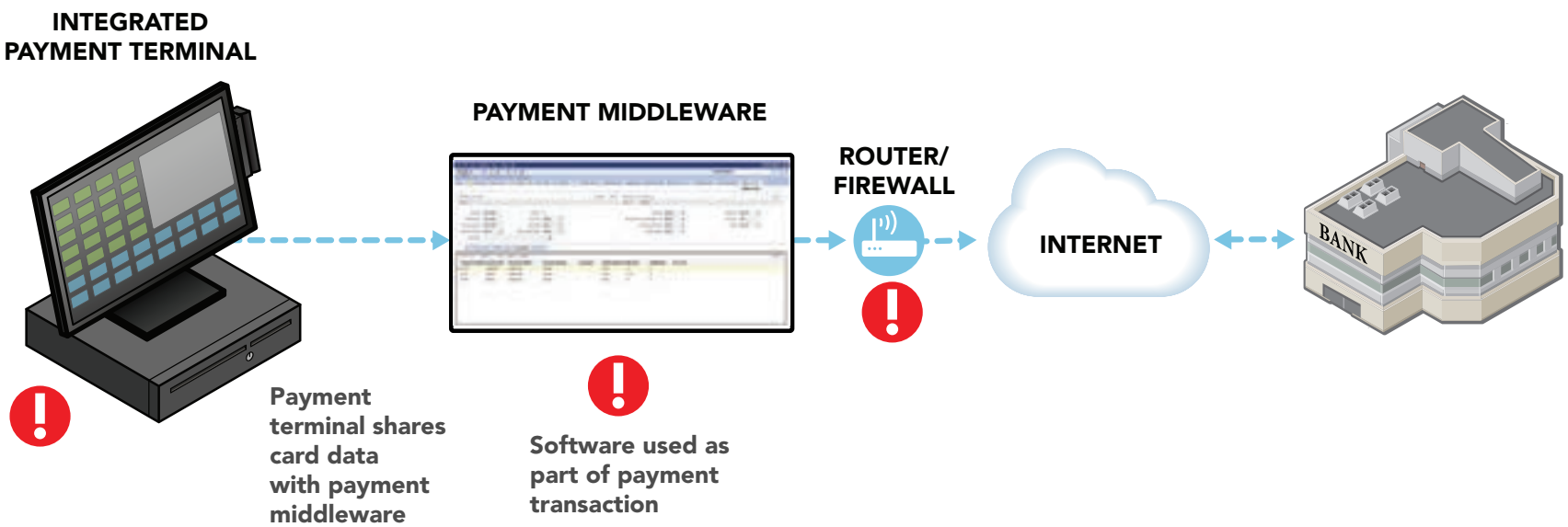
BACK
to previous diagram.

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



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

PCI Security Standards Council

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

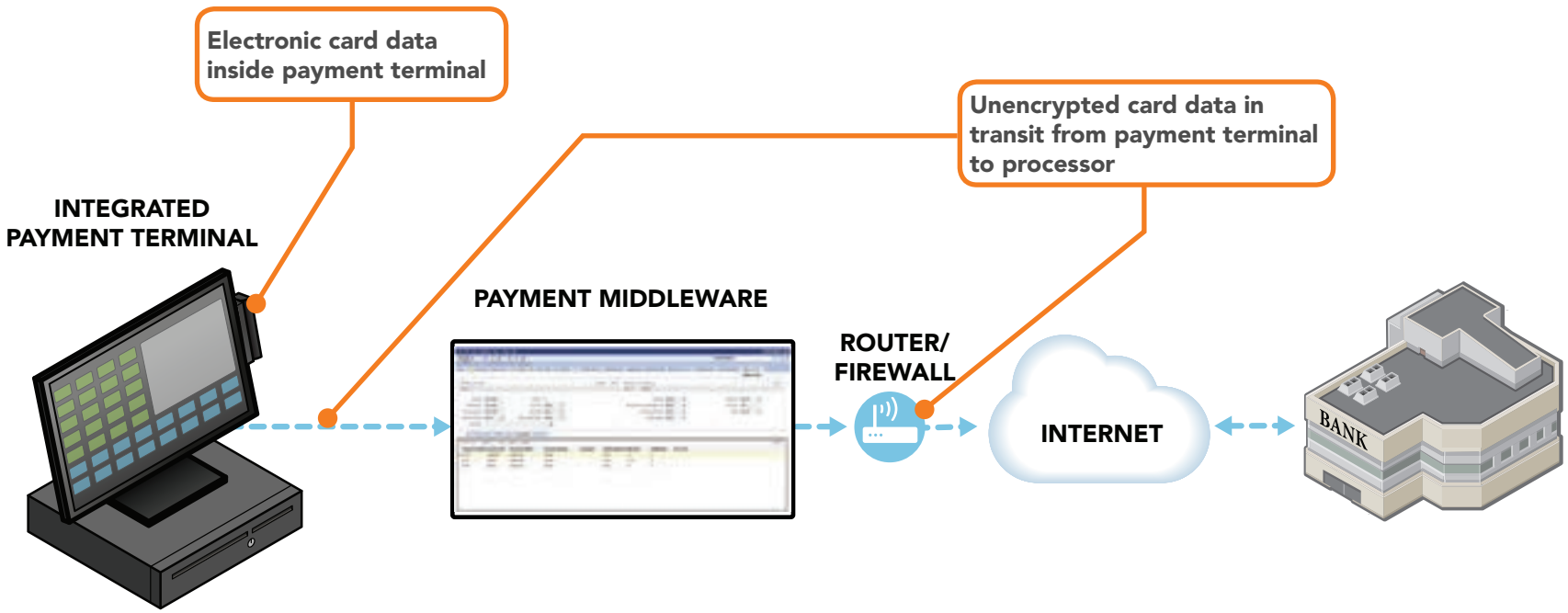
RISK PROFILE

Chip

Mag Stripe

HIGHER

Where is your card data at risk?



TYPE 7

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

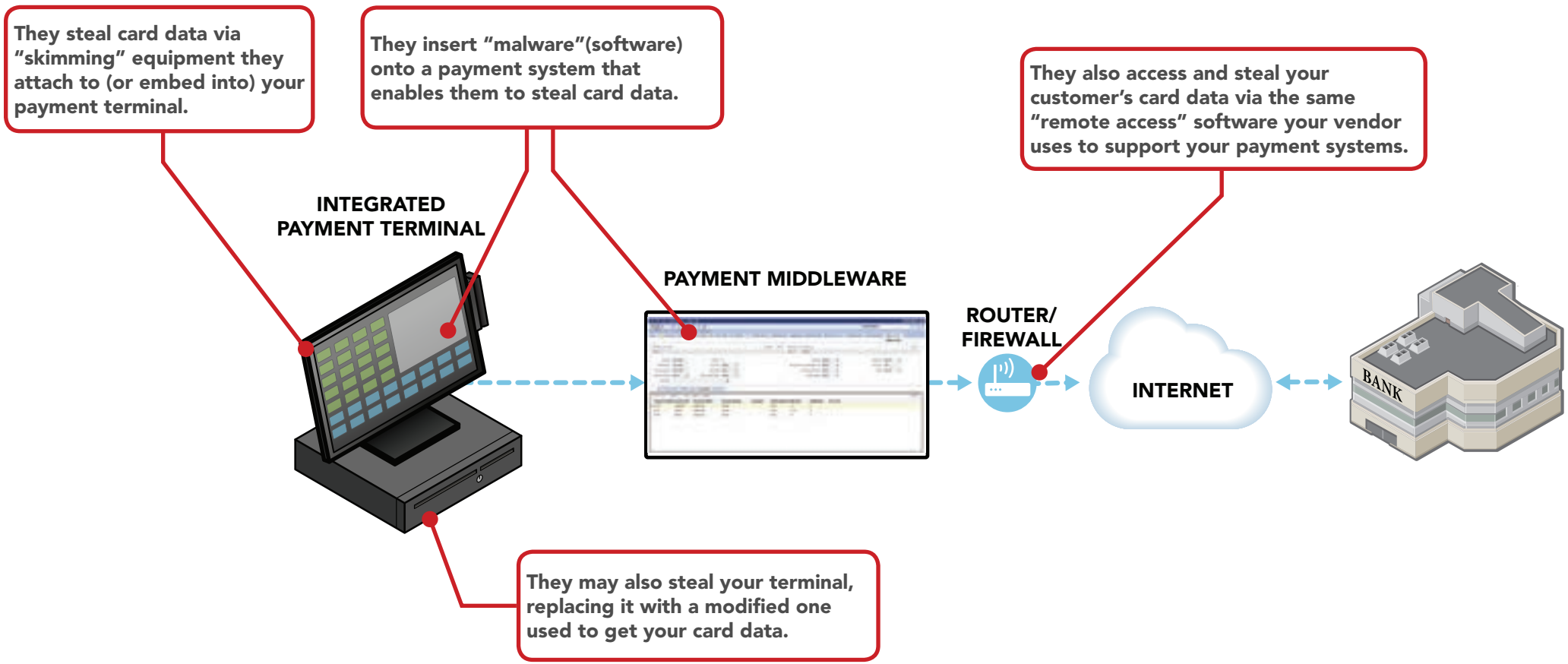
RISK PROFILE

Chip

Mag Stripe

HIGHER

How do criminals get your card data?



TYPE 7

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

RISK PROFILE

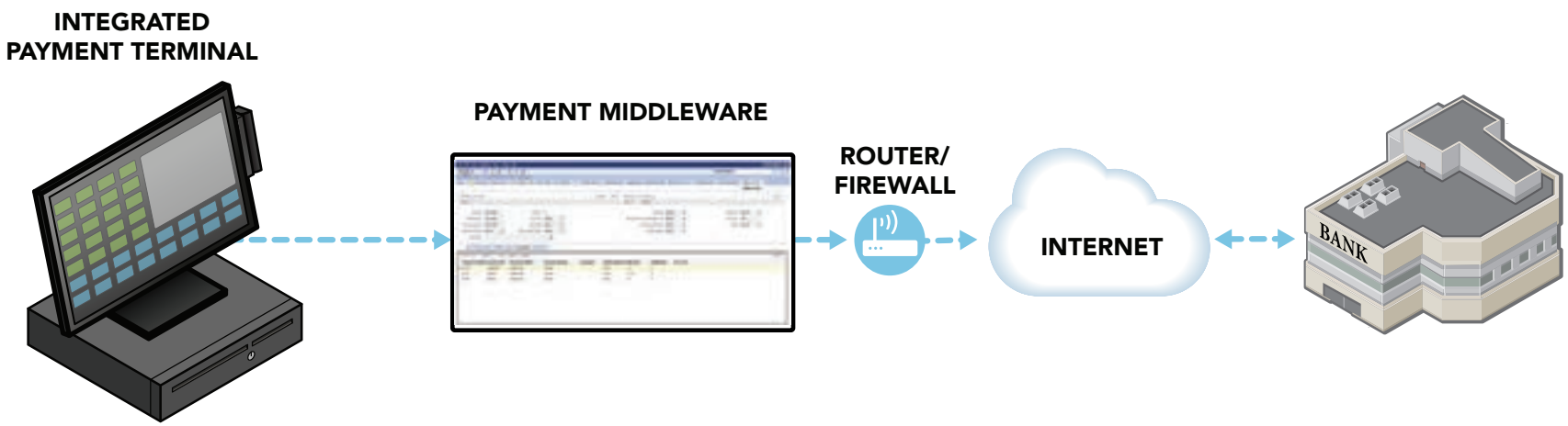
Chip

Mag Stripe

HIGHER

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
- 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 a secure payment terminal
- 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.

TYPE 8

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

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

YES
This IS my setup.
Show me the details.

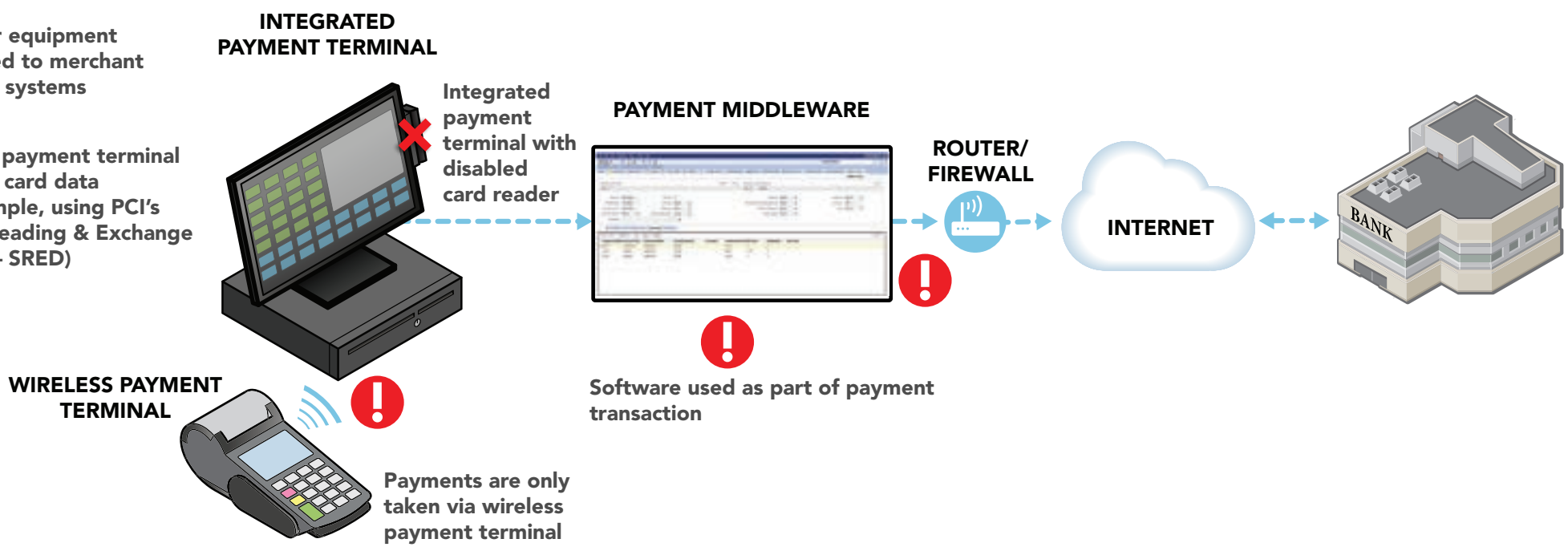
NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

Encrypted card data shared with terminal and middleware

No other equipment connected to merchant payment systems

Wireless payment terminal encrypts card data (for example, using PCI's Secure Reading & Exchange of Data – SRED)



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

PCI Security Standards Council

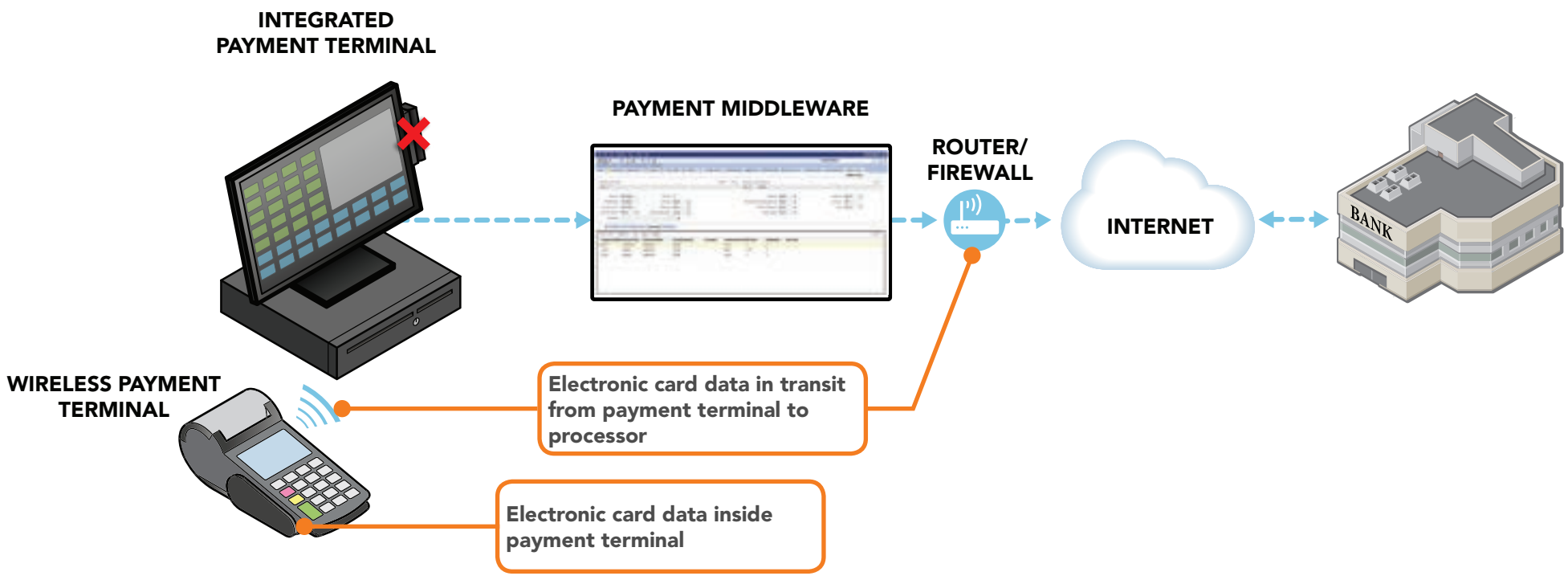
Encrypting wireless payment terminal ("pay-at-table") with integrated payment terminal and middleware. Payments sent via Internet.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

Where is your card data at risk?



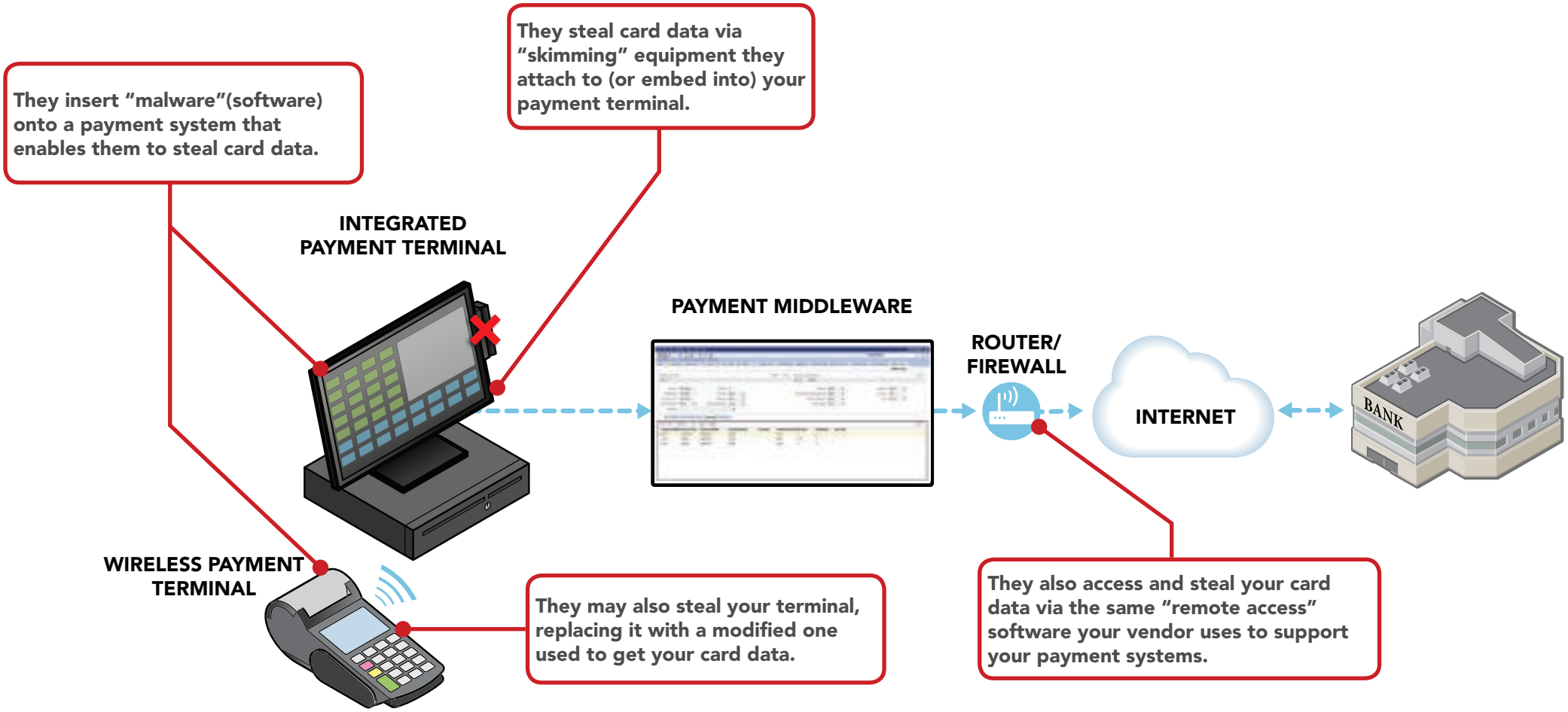
Encrypting wireless payment terminal ("pay-at-table") with integrated payment terminal and middleware. Payments sent via Internet.

RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

How do criminals get your card data?



TYPE 8

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

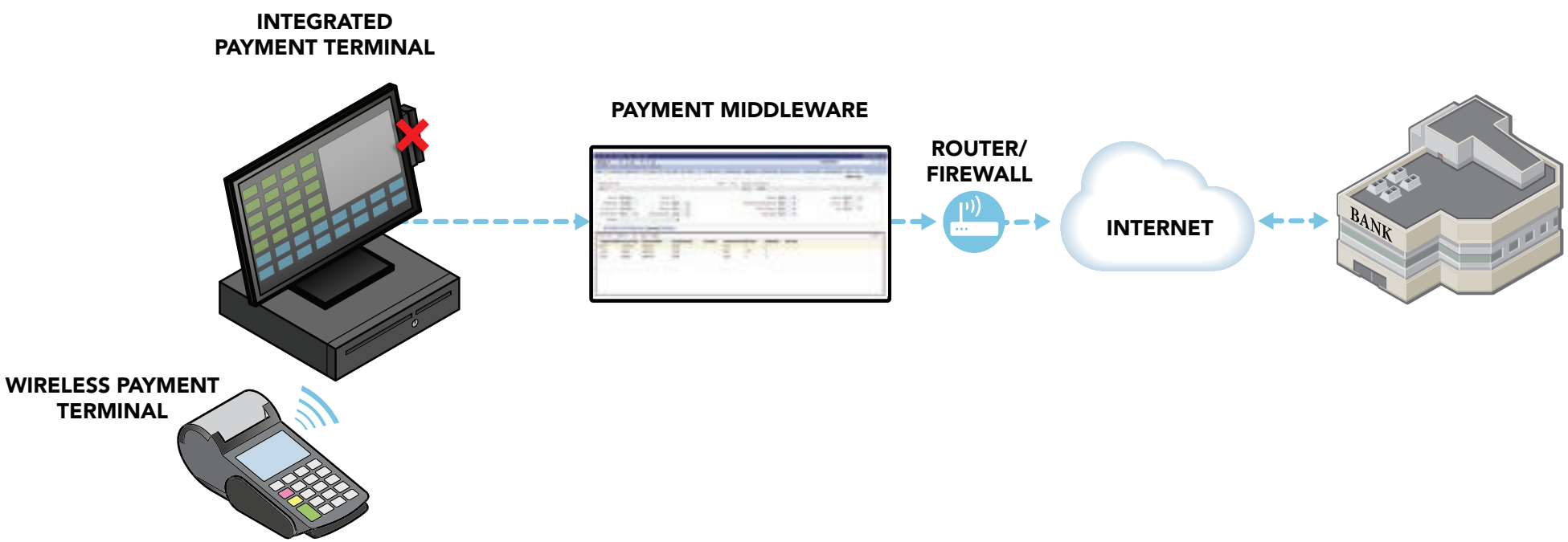
RISK PROFILE

Chip: LOWER

Mag Stripe: MODERATE

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
- 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 a secure payment terminal
- 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.

PCI Security Standards Council

TYPE 9

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

RISK PROFILE

HIGHER

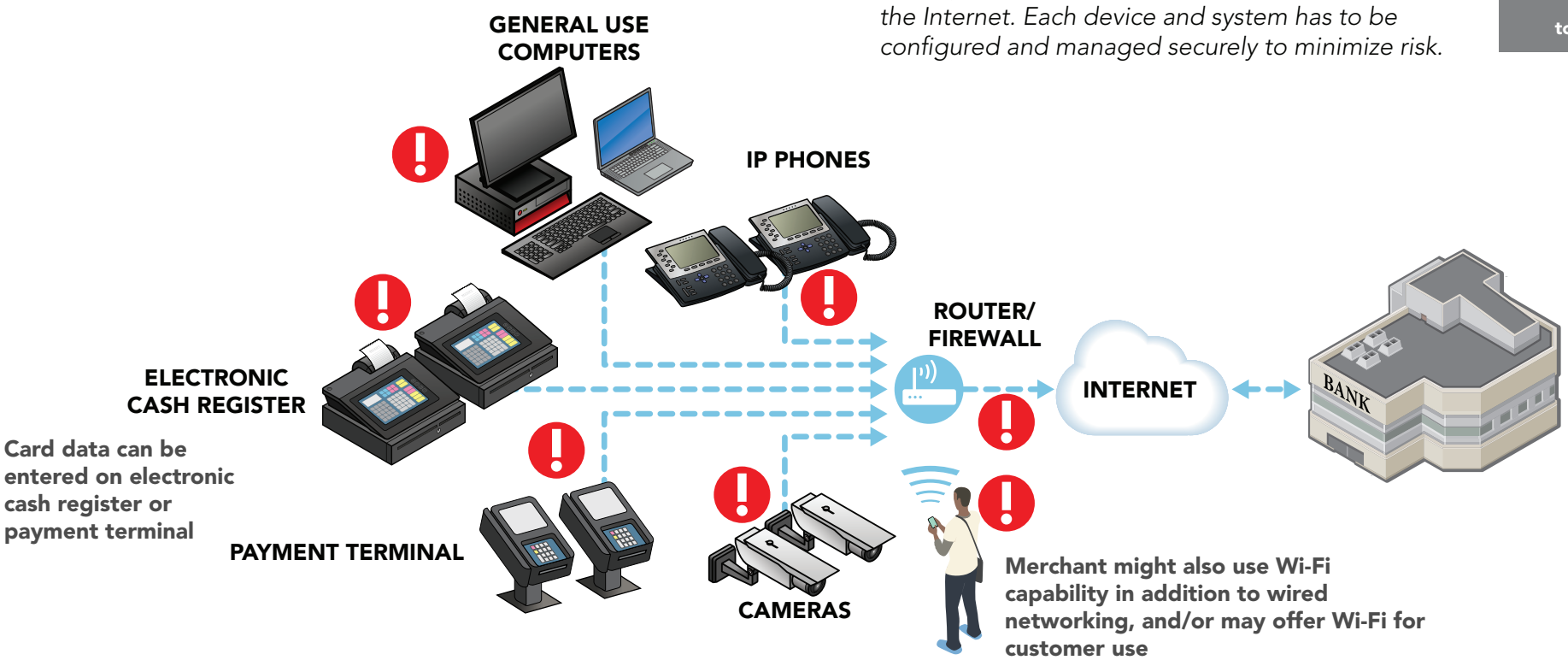
TYPE 9 OVERVIEW | TYPE 9 RISKS | TYPE 9 THREATS | TYPE 9 PROTECTIONS

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

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



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

PCI Security Standards Council

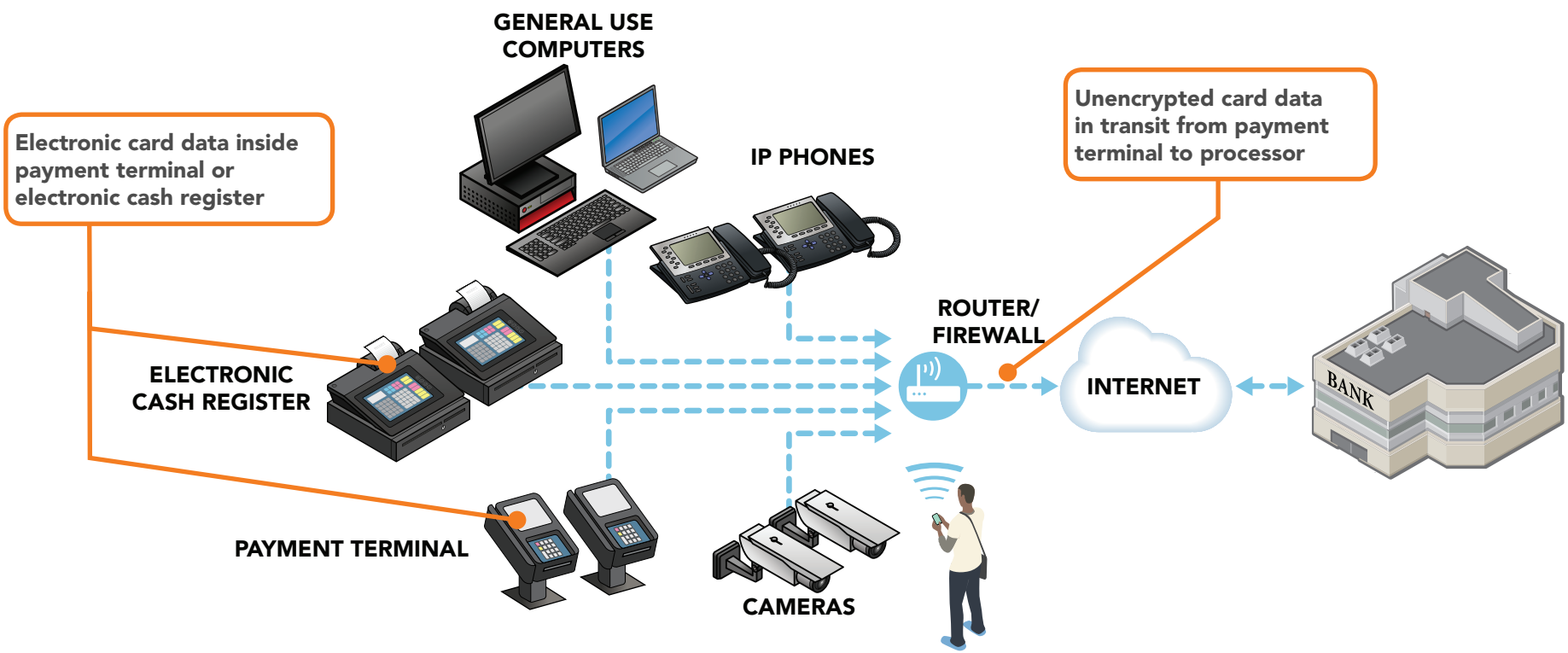
TYPE 9

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

RISK PROFILE

HIGHER

Where is your card data at risk?



TYPE 9

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

RISK PROFILE

HIGHER

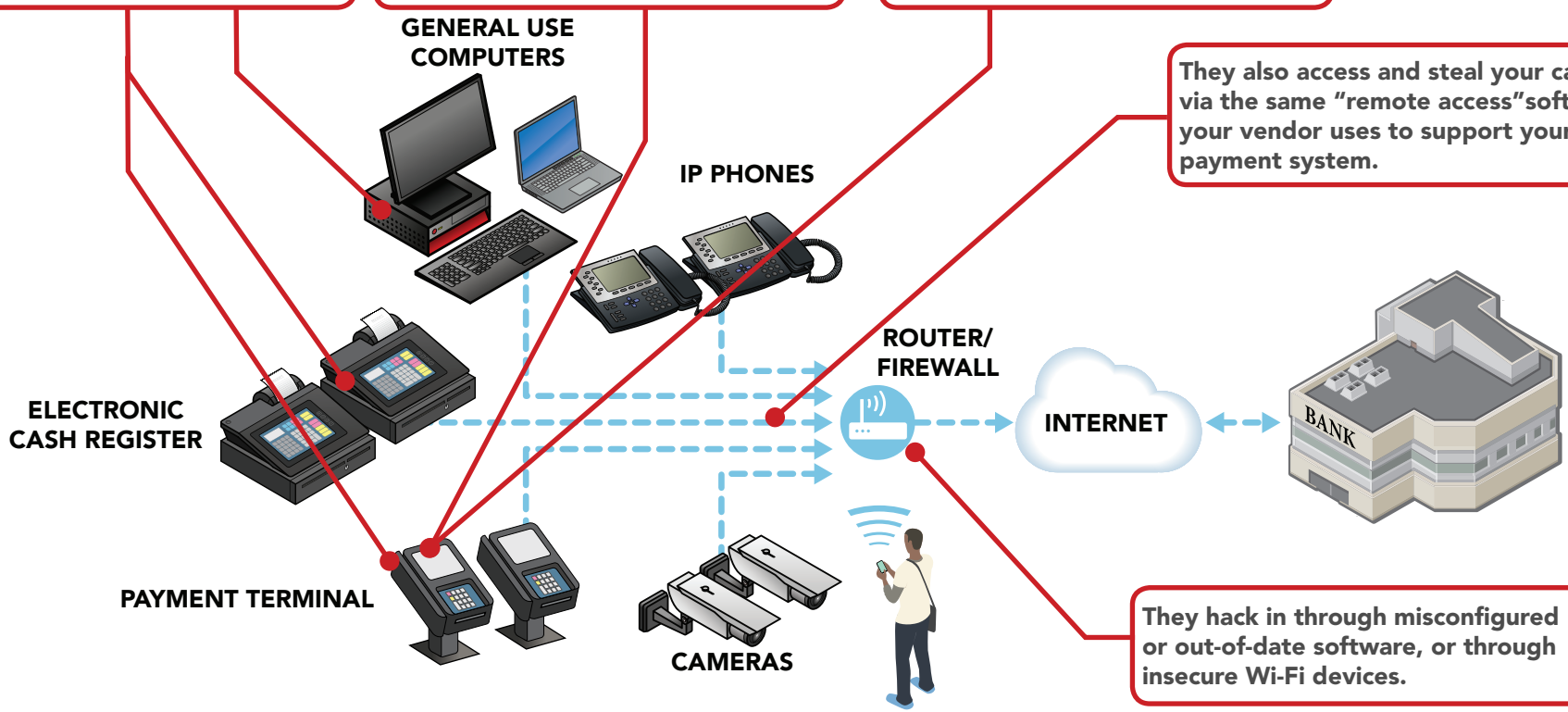
How do criminals get your card data?

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

They also access and steal your card data via the same "remote access"software your vendor uses to support your payment system.



They hack in through misconfigured or out-of-date software, or through insecure Wi-Fi devices.

TYPE 9

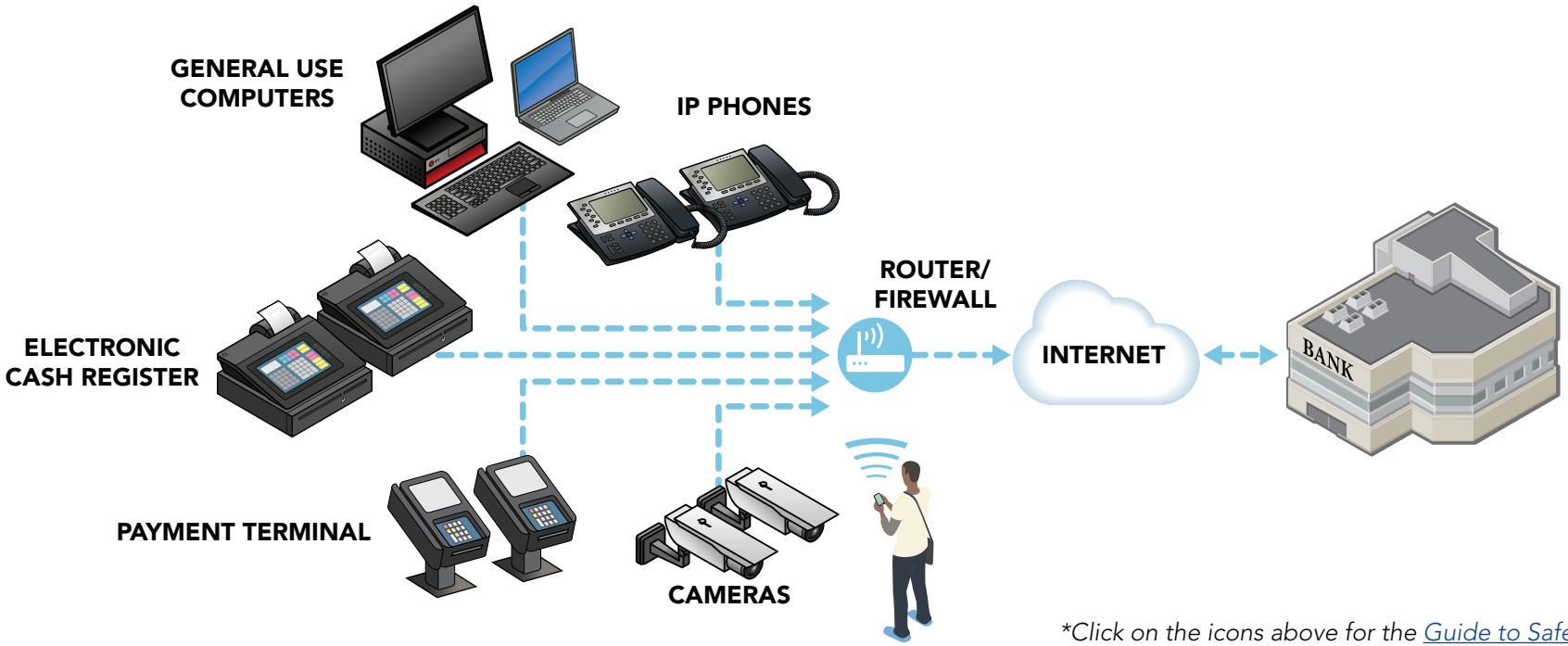
Payment terminal connects to electronic cash register with additional connected equipment. Payments sent via Internet.

RISK PROFILE

HIGHER

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
- 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 a secure payment terminal
- 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.

PCI Security Standards Council

TYPE 10

E-commerce merchant with fully-outsourced payment page. Payments sent via Internet by third-party provider.

RISK PROFILE

LOWER

YES
This IS my setup.
Show me the details.

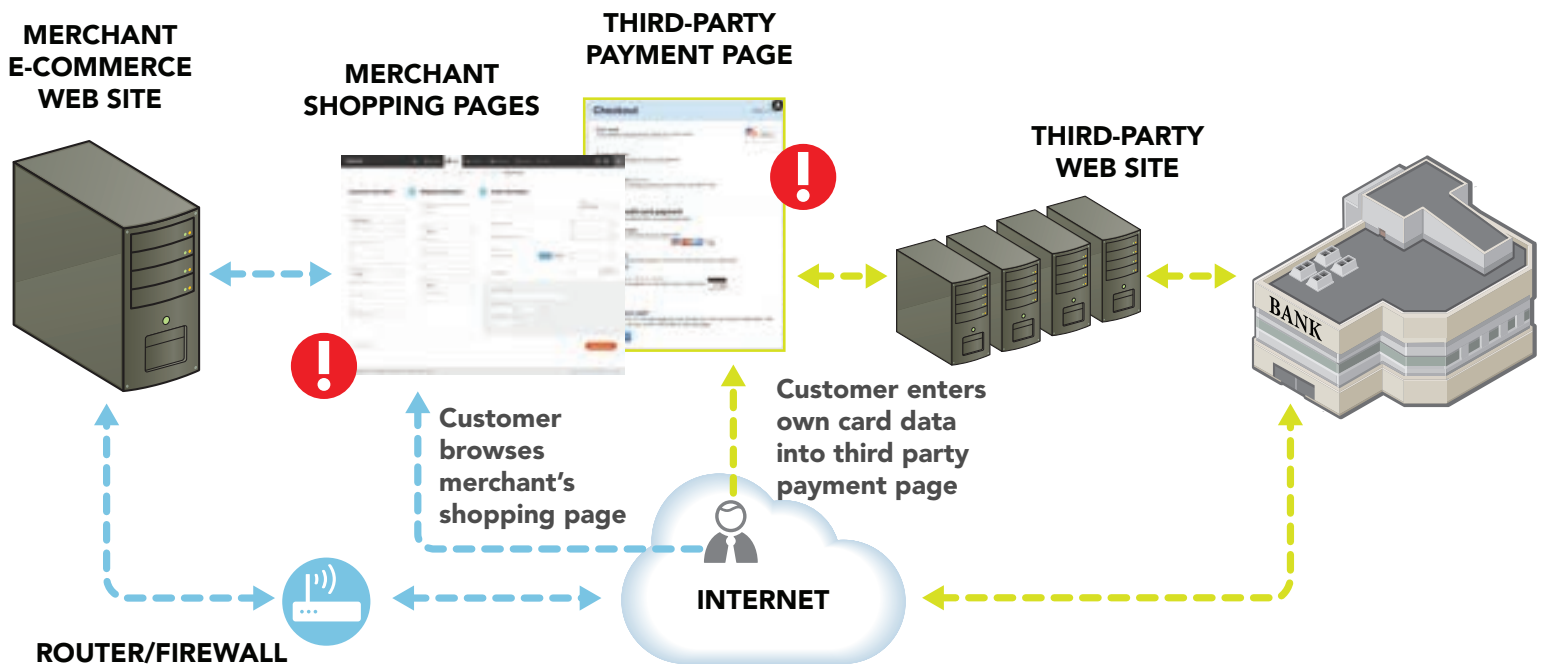
NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

Merchant's entire payment page is outsourced to a PCI DSS compliant third party

Merchant manages own website, but has no access to the payment page

Merchant has only product info (shopping pages, etc.) available from their website, and never has access to, or the ability to control, any card data



Shopping pages may be delivered by merchant or merchant's hosting provider

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

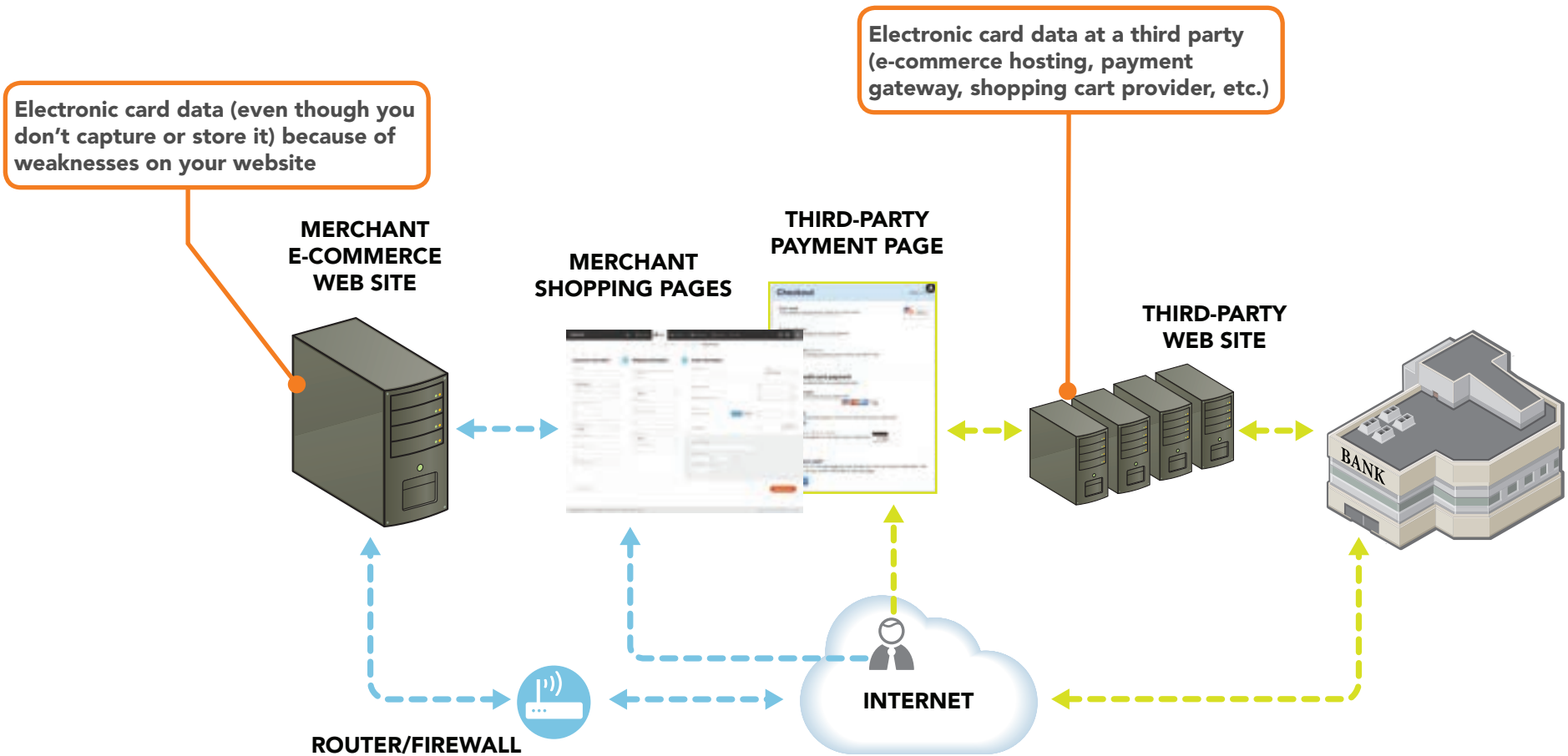
TYPE 10

E-commerce merchant with fully-outsourced payment page. Payments sent via Internet by third-party provider.

RISK PROFILE

LOWER

Where is your card data at risk?



TYPE 10

E-commerce merchant with fully-outsourced payment page. Payments sent via Internet by third-party provider.

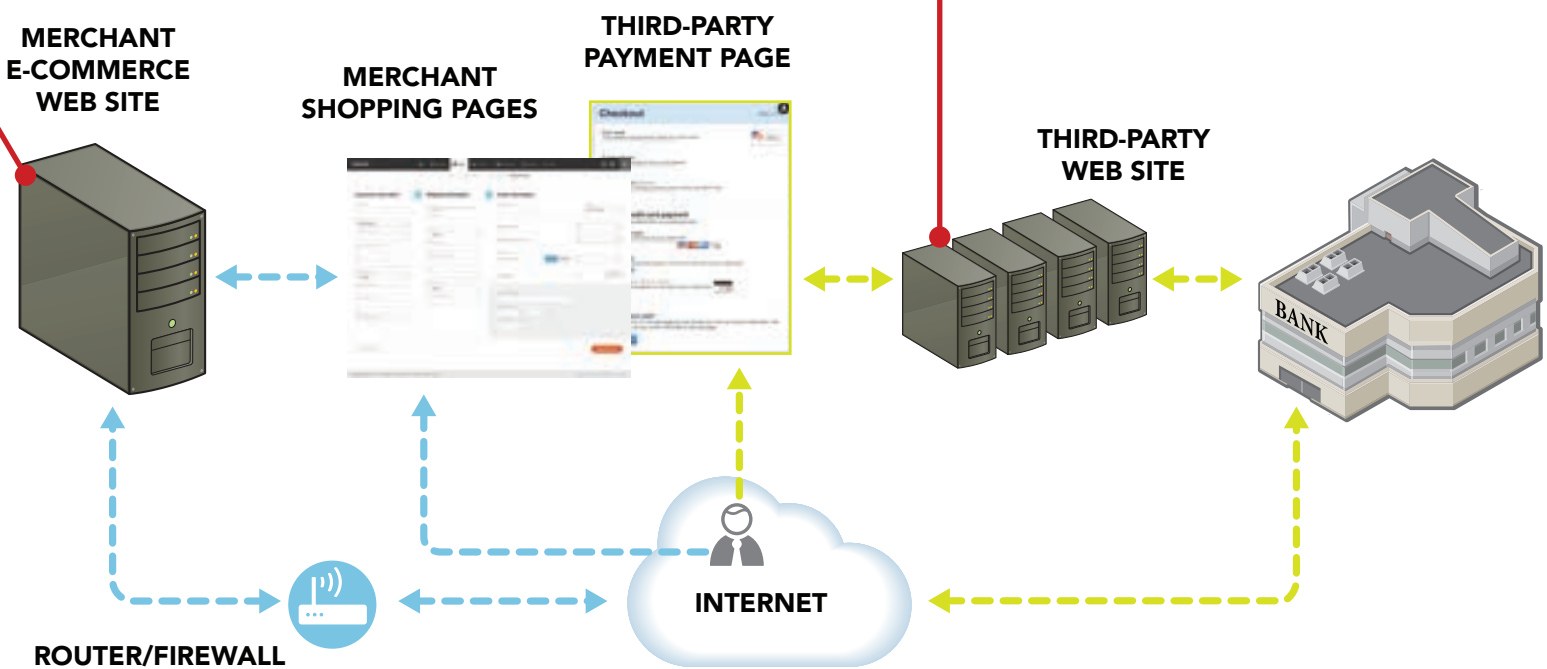
RISK PROFILE

LOWER

How do criminals get your card data?

They compromise your website due to vulnerabilities, and they intercept card data as your customers send it to your outsourced e-commerce provider.

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



TYPE 10

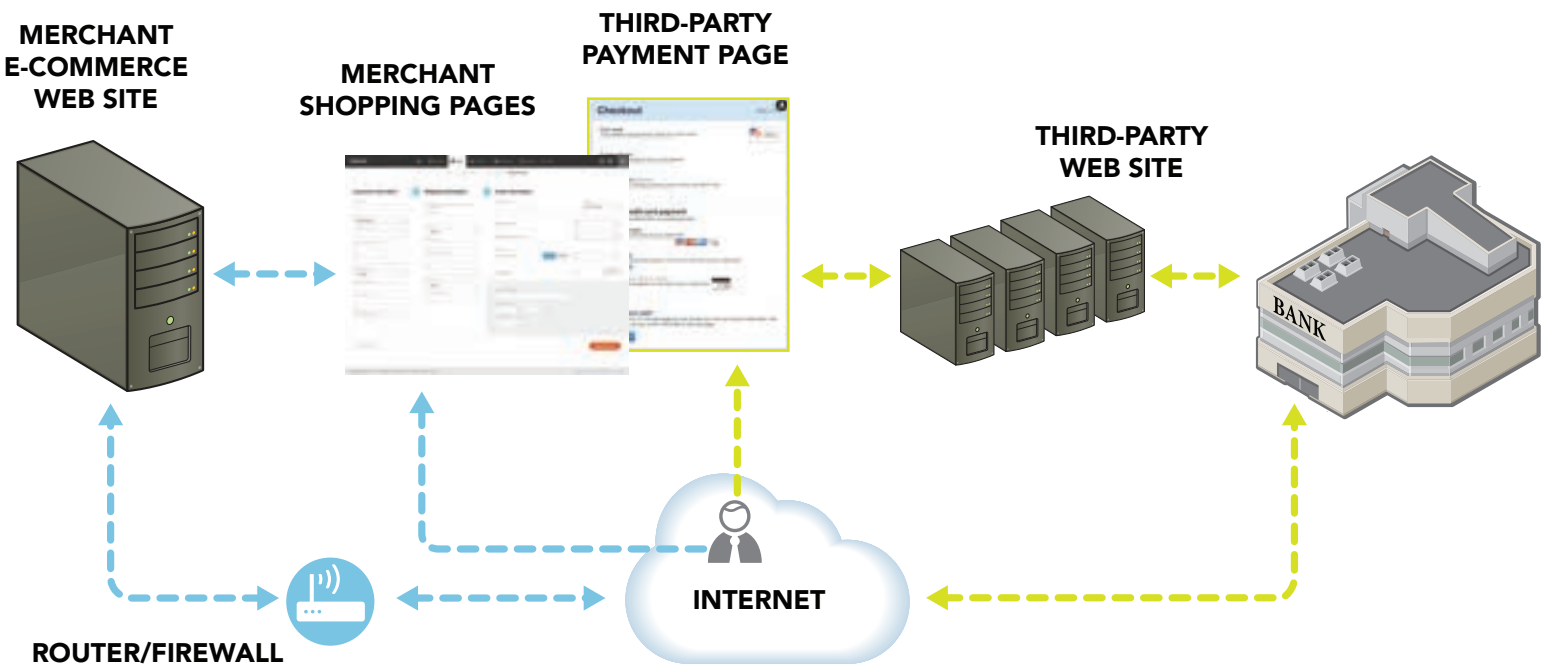
E-commerce merchant with fully-outsourced payment page. Payments sent via Internet by third-party provider.

RISK PROFILE

LOWER

How do you start to protect card data today?*

- Use strong passwords
- Install patches from your vendors
- Ask your vendor partners for help if you need it
- Protect your business from the Internet



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

TYPE 11

E-commerce merchant accepts payments on own payment page and manages own website. Payments sent via Internet by merchant.

RISK PROFILE

HIGHER

TYPE 11 OVERVIEW | TYPE 11 RISKS | TYPE 11 THREATS | TYPE 11 PROTECTIONS

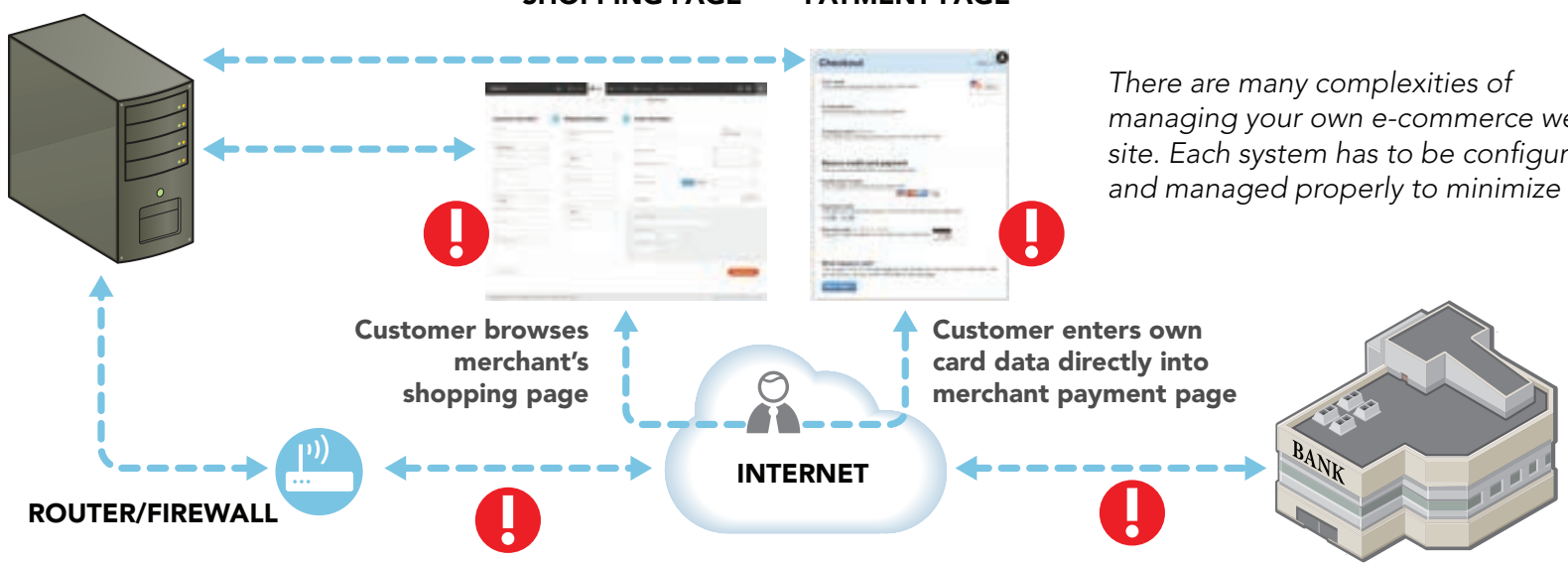
YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

Shopping pages and/or payment pages may be hosted by merchant or merchant's hosting provider

Merchant manages website, including payment page (or elements of the payment page)



There are many complexities of managing your own e-commerce web site. Each system has to be configured and managed properly to minimize risk.

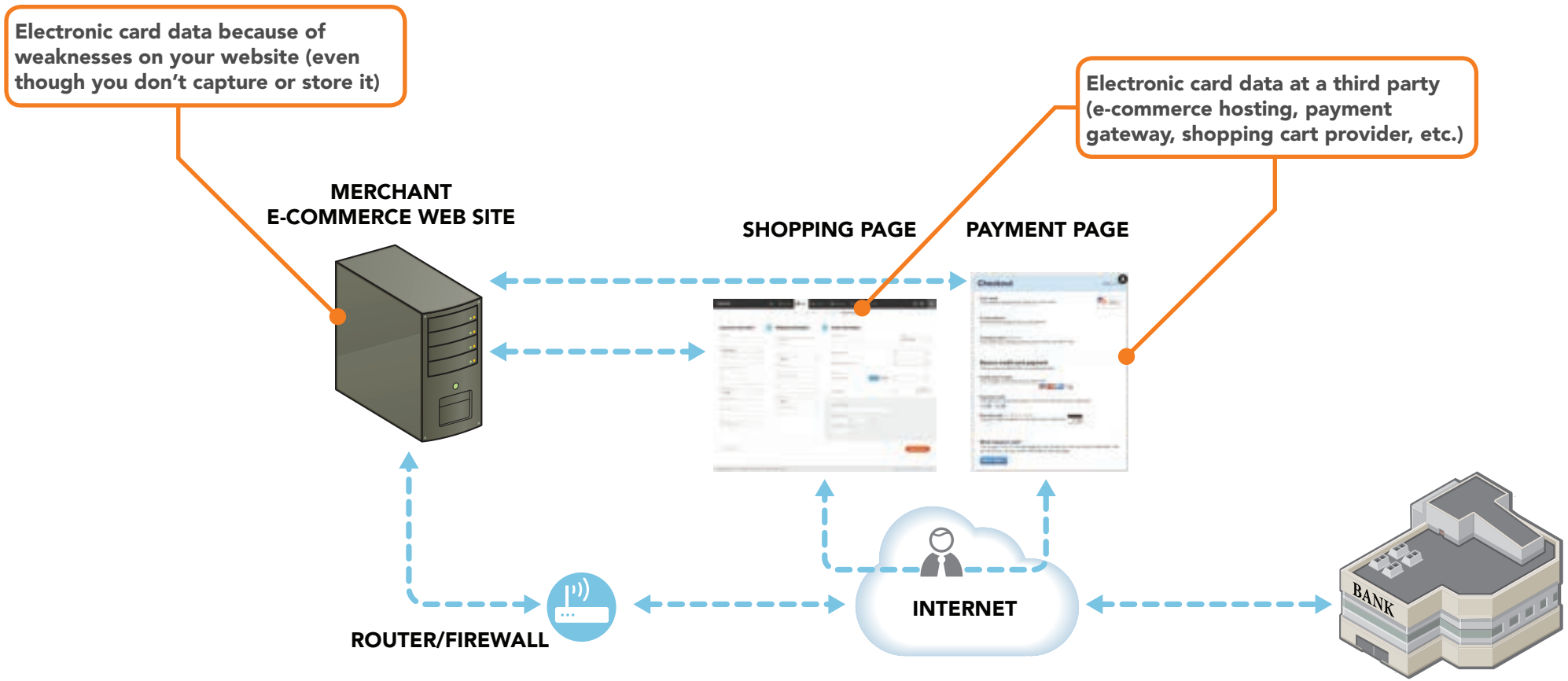
For this scenario, risks to card data are present at ❗ above. Risks explained on next page.

E-commerce merchant accepts payments on own payment page and manages own website. Payments sent via Internet by merchant.

RISK PROFILE

HIGHER

Where is your card data at risk?



E-commerce merchant accepts payments on own payment page and manages own website. Payments sent via Internet by merchant.

RISK PROFILE

HIGHER

How do criminals get your card data?

They compromise or attack your website due to vulnerabilities. For example, SQL injection is a common technique used to steal data from websites.

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

TYPE 11

E-commerce merchant accepts payments on own payment page and manages own website. Payments sent via Internet by merchant.

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 a secure payment terminal
- 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.

PCI Security Standards Council

TYPE 12

Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

RISK PROFILE

Chip: LOWER

Mag Stripe: LOWER

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.

BACK
to previous diagram.

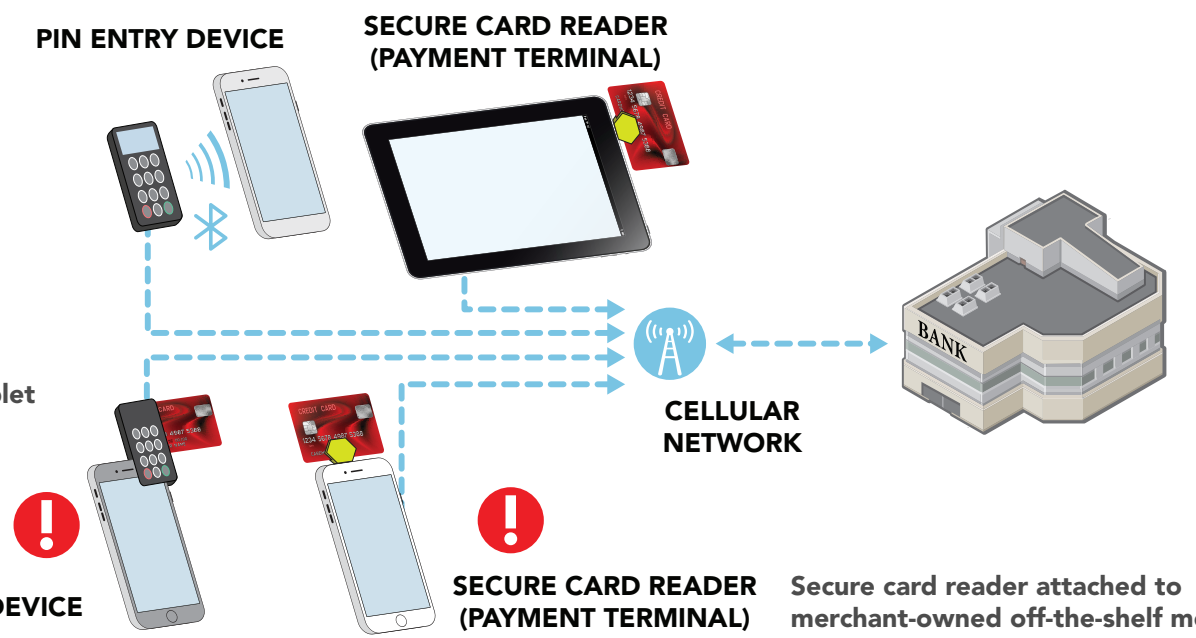
Different devices are used to read magnetic stripe card data, enter personal identification number (PIN), and read chip card data

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.)

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



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.

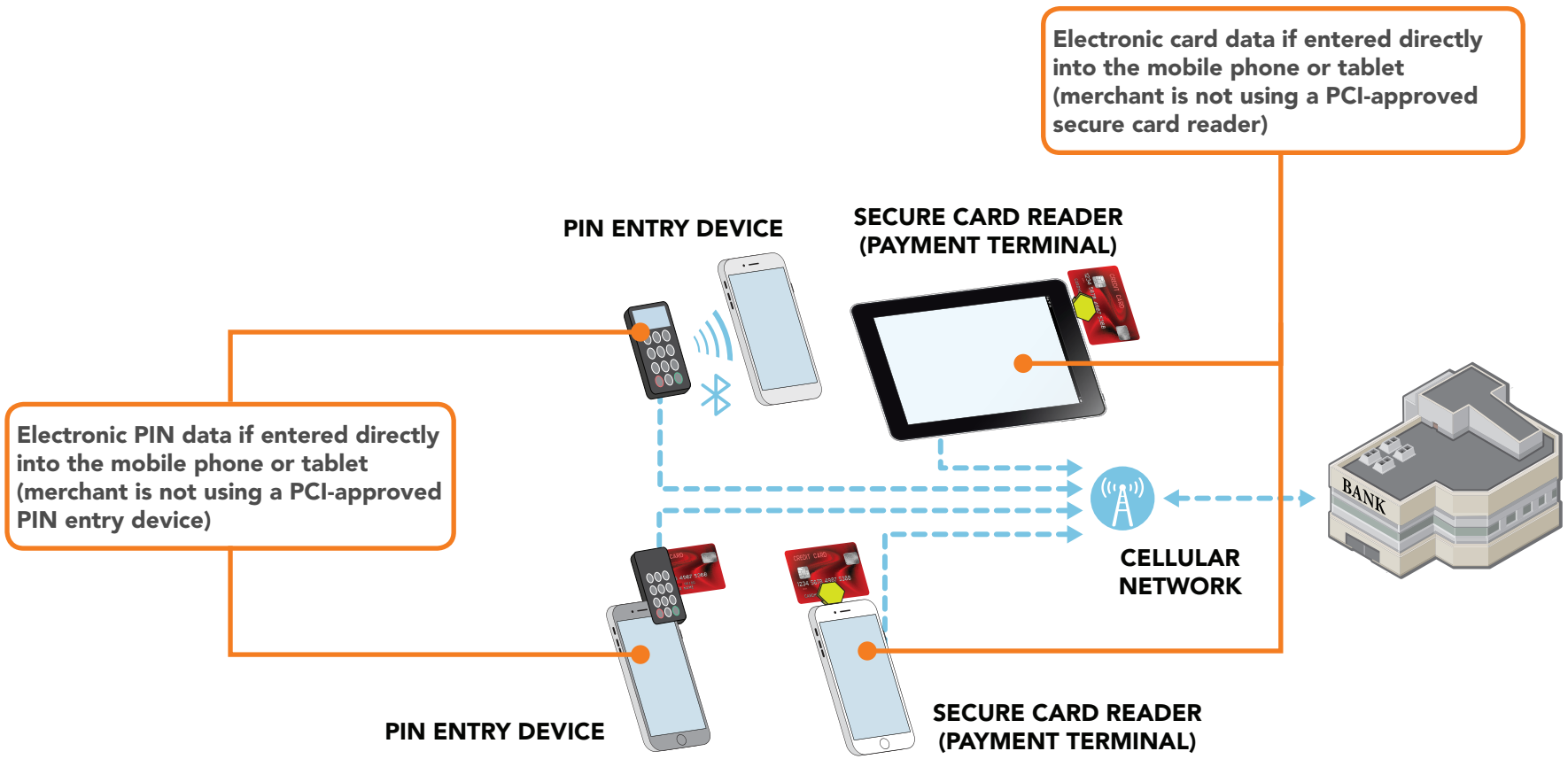
Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

RISK PROFILE

Chip: LOWER

Mag Stripe: LOWER

Where is your card data at risk?



Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

RISK PROFILE

Chip: LOWER

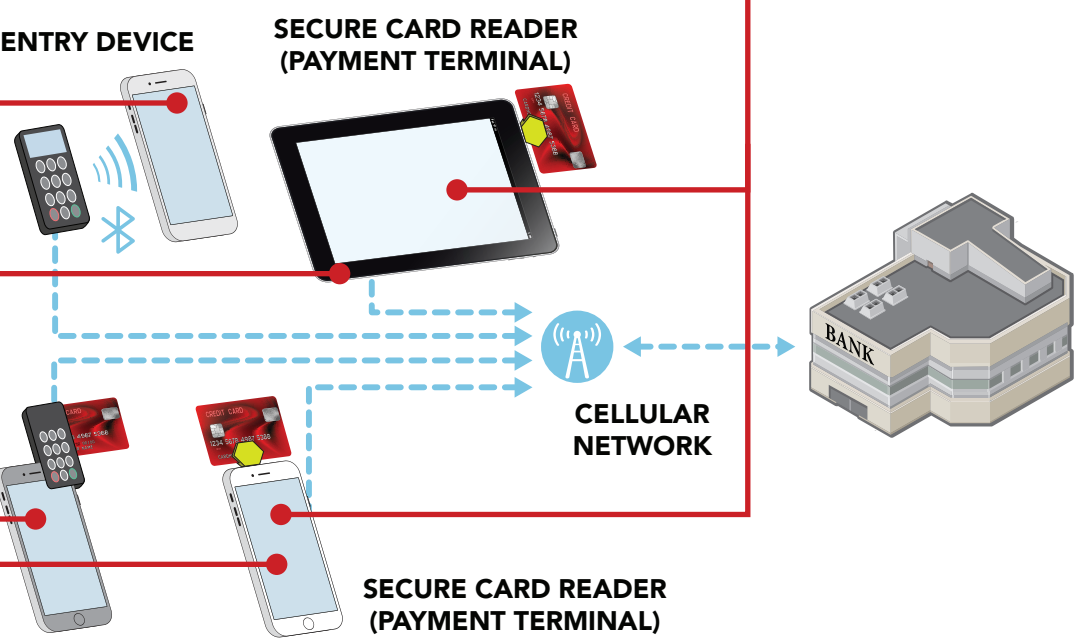
Mag Stripe: LOWER

How do criminals get your card data?

They may hack into phone/tablet and insert "malware"(software) that enables them to steal card data or PIN data on mobile phones/tablets.

They use applications in "app store" that enable them to steal card or PIN data when you download that app onto your phone/tablet.

Criminals may swap out the secure card reader for one they have modified to include a skimmer.



TYPE 12

Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network only.

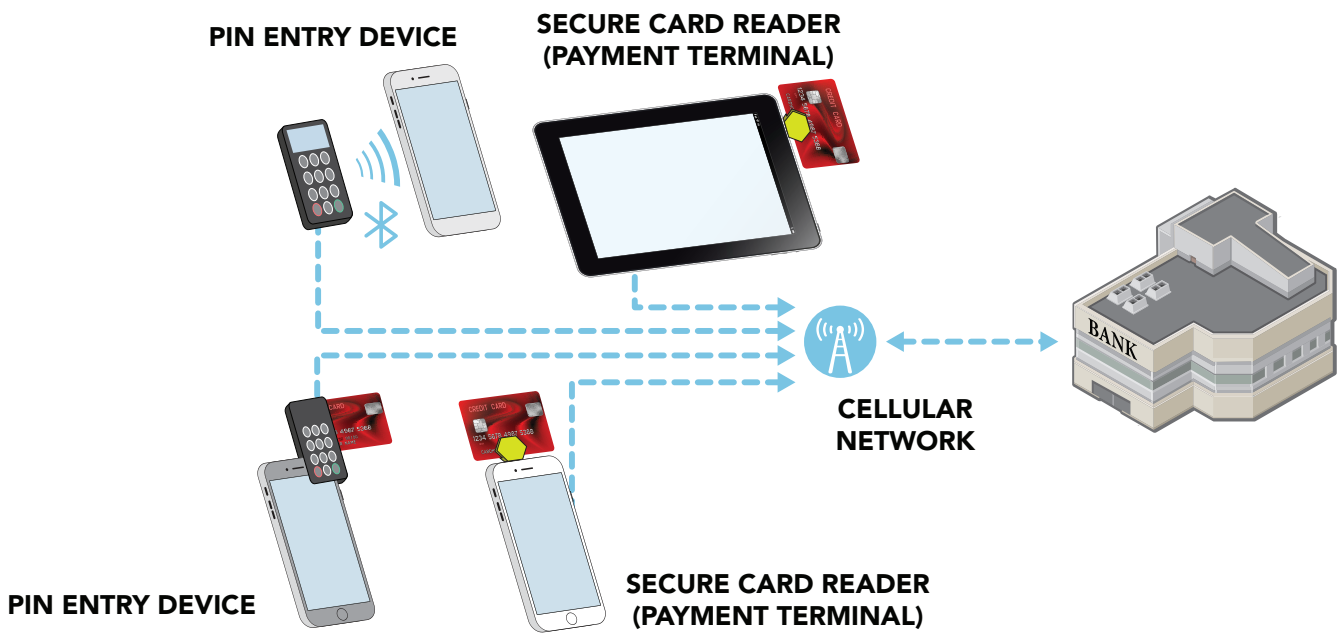
RISK PROFILE

Chip: LOWER

Mag Stripe: 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
- Use anti-virus software
- Use a secure card reader and PIN entry device
- Make your card data useless to criminals



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

TYPE 13

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

RISK PROFILE

Chip: MODERATE

Mag Stripe: MODERATE

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Show me the next setup.

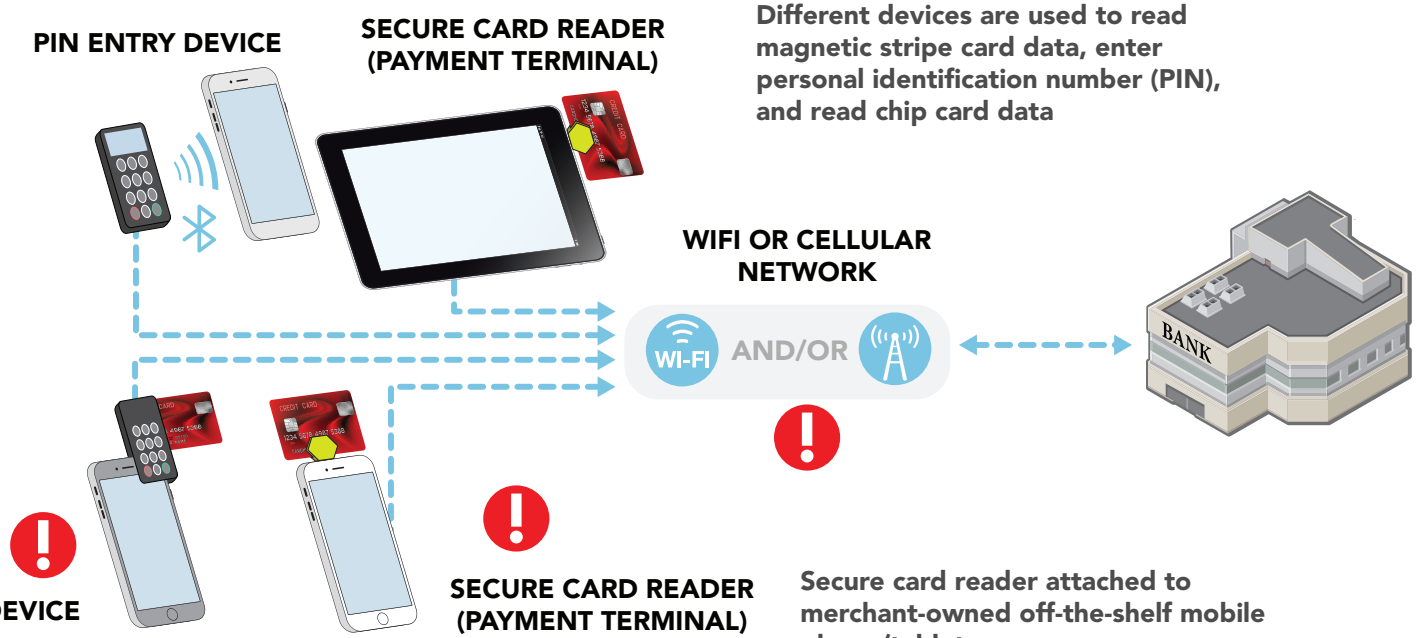
BACK
to previous diagram.

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

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

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



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.

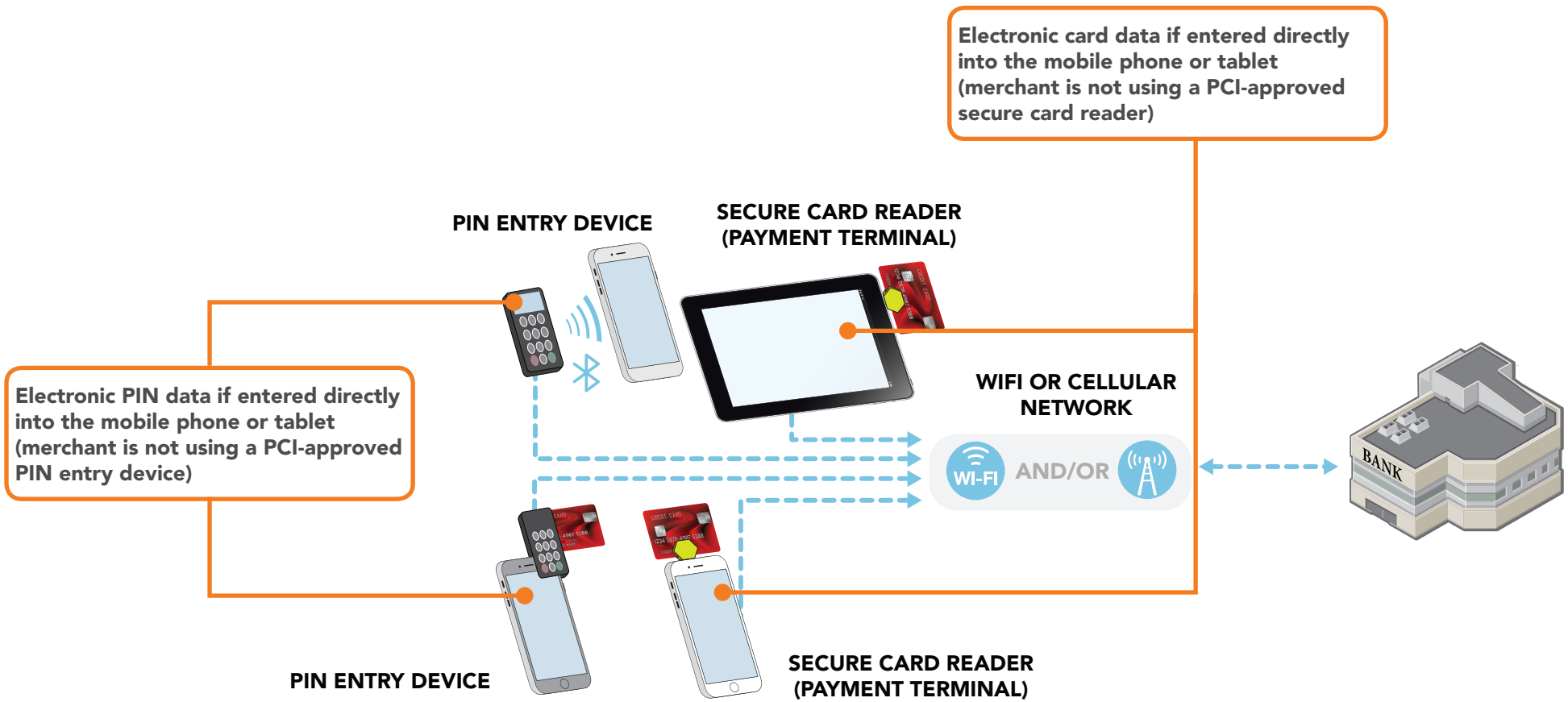
Encrypting secure card reader and mobile payment terminal. Payments sent via cellular network or Wi-Fi.

RISK PROFILE

Chip: MODERATE

Mag Stripe: MODERATE

Where is your card data at risk?



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

RISK PROFILE

Chip: MODERATE

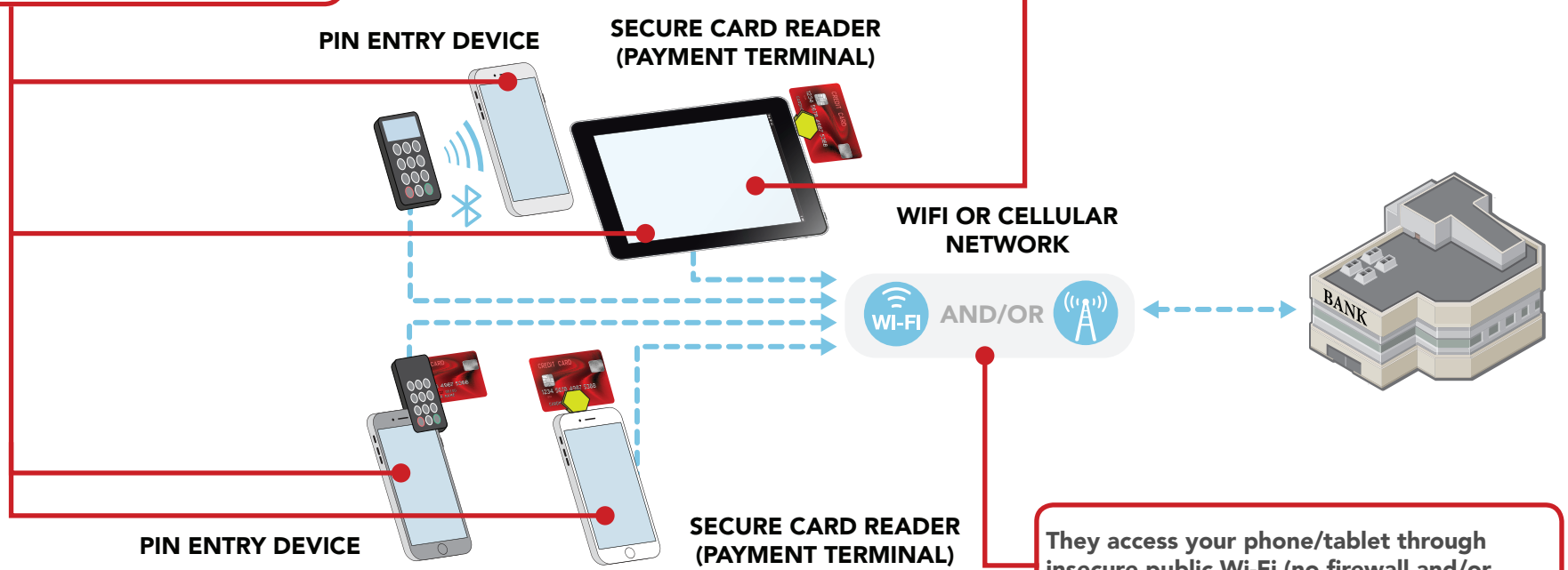
Mag Stripe: MODERATE

How do criminals get your card data?

They may hack into phone/tablet and insert "malware"(software) that enables them to steal card data or PIN data on mobile phones/tablets.

They use applications in "app store" that enable them to steal card or PIN data when you download that app onto your phone/tablet.

Criminals may swap out the secure card reader for one they have modified to include a skimmer.



They access your phone/tablet through insecure public Wi-Fi (no firewall and/or unknown security) to steal card or PIN data

TYPE 13

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

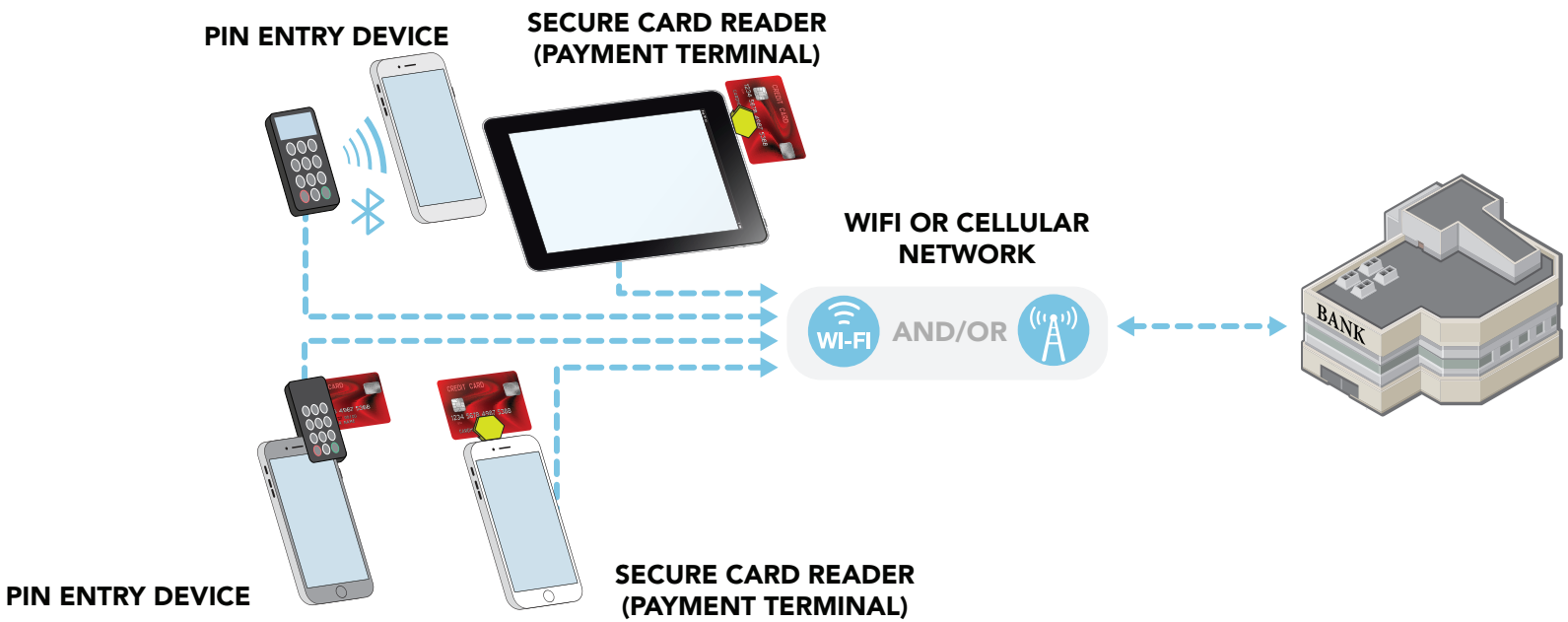
RISK PROFILE

Chip: MODERATE

Mag Stripe: MODERATE

How do you start to protect card data today?*

- Use strong passwords
- Protect in-house access to your card data
- Protect your business from the Internet
- Inspect your secure card readers and PIN entry devices for damage or changes
- Limit remote access for your vendor partners - don't give hackers easy access
- Make your card data useless to criminals
- Install patches from your payment terminal vendor
- Use anti-virus software
- 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.

PCI Security Standards Council

TYPE 14

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

RISK PROFILE

LOWER

YES
This IS my setup.
Show me the details.

NO
This IS NOT my setup.
Take me back to the beginning.

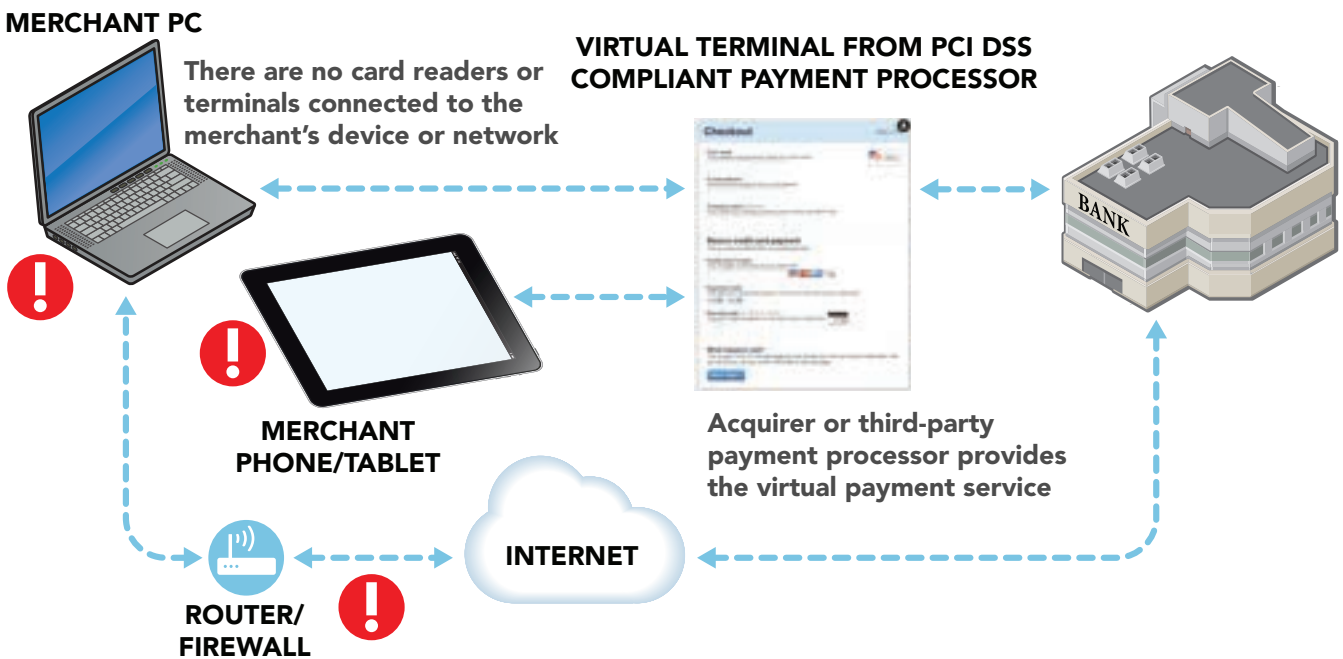
BACK
to previous diagram.

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.

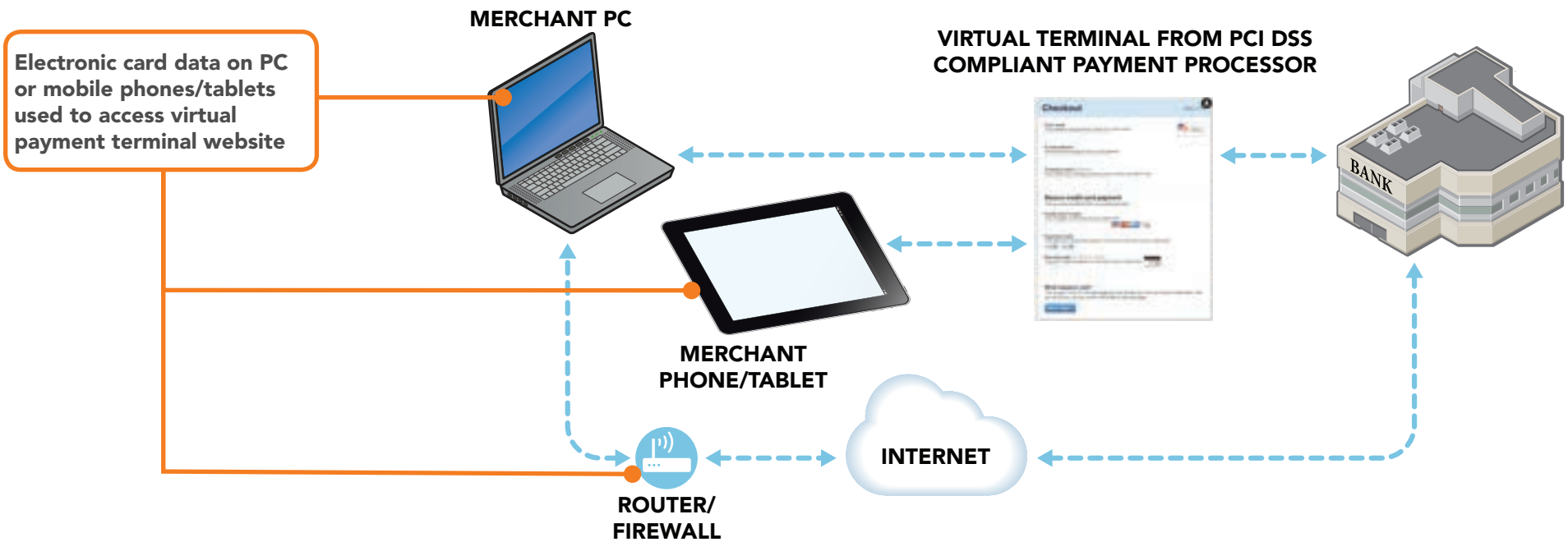
PCI Security Standards Council

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

RISK PROFILE

LOWER

Where is your card data at risk?



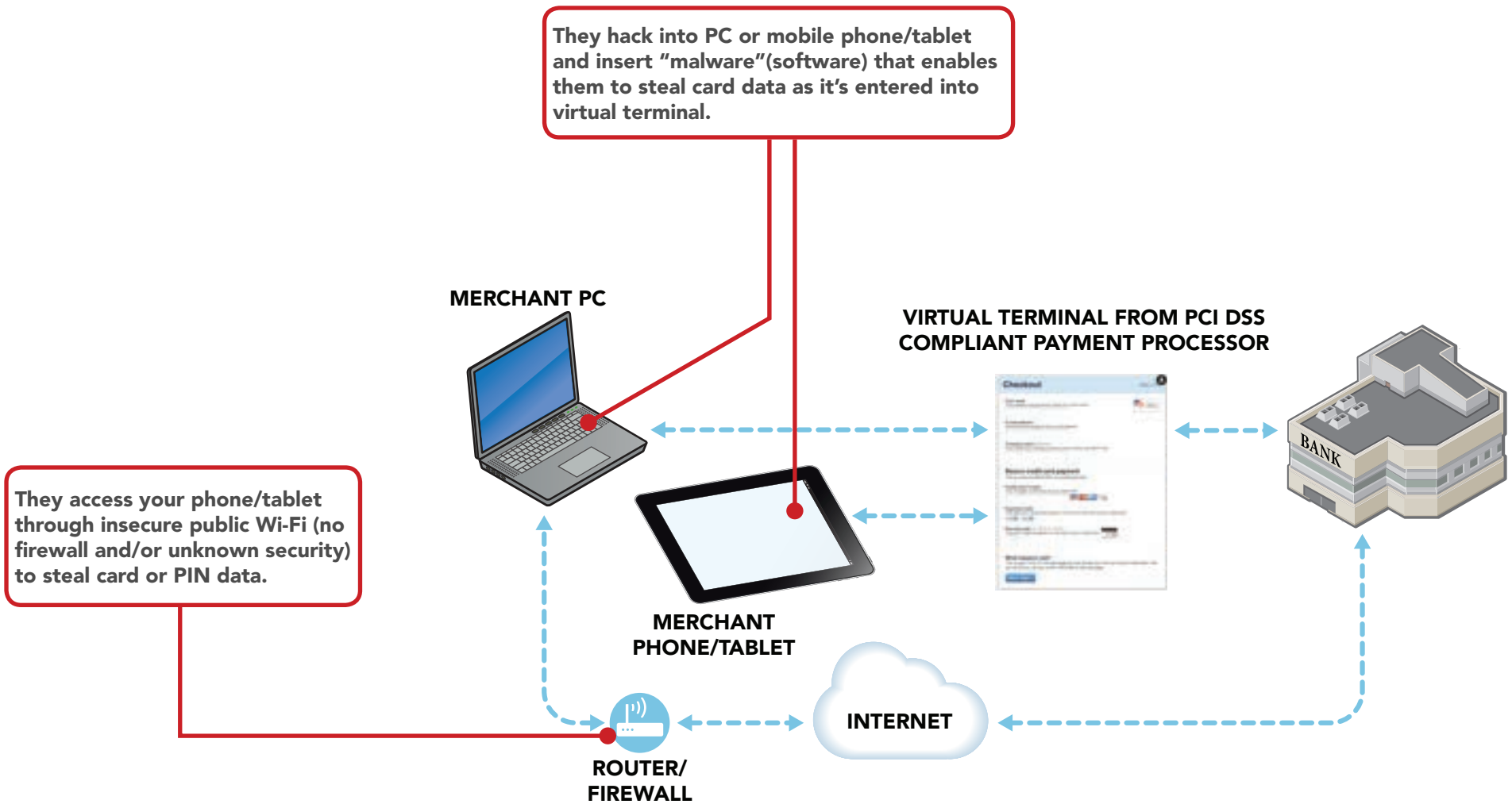
TYPE 14

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

RISK PROFILE

LOWER

How do criminals get your card data?



PCI Security Standards Council

TYPE 14

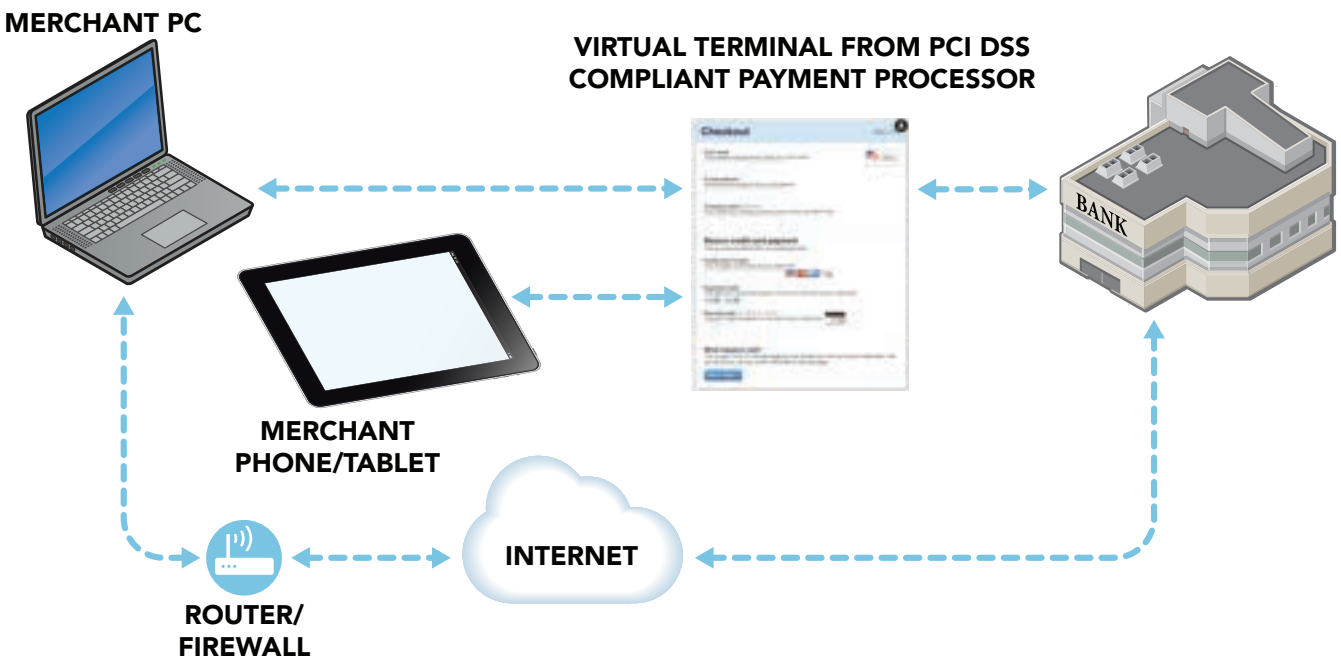
Virtual payment terminal accessed via merchant Internet browser. Payments sent via Internet.

RISK PROFILE

LOWER

How do you start to protect card data today?*

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



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

PCI Security Standards Council

Resources

PCI Small Merchant Documents

Resource	Link	URL
Guide to Safe Payments	*Guide to Safe Payments*	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf*
Small Merchant Questions for Vendors	*Small Merchant Questions for Vendors*	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf*
Small Merchant Glossary	*Small Merchant Glossary*	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf*