

Các hệ thống thanh toán thông dụng

Phiên bản 1.0 | 07/ 2016



Các hệ thống thanh toán và phương thức bảo mật



CÁC HỆ THỐNG THANH TOÁN

Để bảo vệ doanh nghiệp của bạn trước các hành vi trộm cắp dữ liệu thanh toán, trước hết bạn cần phải hiểu về cách thức ứng dụng thanh toán điện tử trên website, gian hàng, cửa tiệm của mình. Bạn sẽ phải đầu tư những trang thiết bị gì, ngân hàng và đối tác công nghệ của bạn là ai và những yếu tố này liên kết với nhau như thế nào?

Tài liệu này sẽ cung cấp những hình ảnh trực quan nhằm giúp bạn xác định được hệ thống thanh toán cần sử dụng, các rủi ro của hệ thống và những biện pháp bảo mật cần thiết cần tiến hành để bảo mật cho hệ thống.

Điểm qua các hệ thống thanh toán

Loại	Mô tả hệ thống thanh toán
1	Thiết bị đầu cuối thanh toán dial up. Dữ liệu thanh toán truyền qua đường thoại.
2	Thiết bị đầu cuối thanh toán dial up và máy tính tiền điện tử kết nối Internet. Dữ liệu truyền qua đường thoại
3	Thiết bị đầu cuối thanh toán có kết nối với máy tính tiền điện tử. Dữ liệu truyền qua Internet bằng máy tính tiền.
4	Thiết bị đầu cuối thanh toán có chức năng mã hoá kết nối với máy tính tiền điện tử. Dữ liệu truyền qua Internet bằng máy tính tiền điện tử
5	Thiết bị đầu cuối thanh toán có chức năng mã hoá và máy tính tiền điện tử kết nối với Internet. Dữ liệu truyền qua Internet
6	Thiết bị đầu cuối thanh toán có chức năng mã hoá và máy tính tiền điện tử chia sẻ dữ liệu không phải thẻ (bán tích hợp). Dữ liệu truyền qua Internet thông qua thiết bị đầu cuối thanh toán.
7	Thiết bị đầu cuối thanh toán tích hợp và phần mềm trung gian (middleware) thanh toán chia sẻ dữ liệu thẻ. Dữ liệu truyền qua Internet.
8	Thiết bị đầu cuối thanh toán không dây có chức năng mã hoá (“Thanh toán tại bàn”) với thiết bị đầu cuối thanh toán được tích hợp và phần mềm trung gian (middleware). Dữ liệu truyền qua Internet.
9	Thiết bị đầu cuối thanh toán kết nối với máy tính tiền điện tử, kèm với thiết bị kết nối bổ sung. Dữ liệu truyền qua Internet.
10	Merchant TMĐT với trang thanh toán hoàn toàn thuê ngoài. Dữ liệu truyền qua Internet bởi bên cung cấp thứ ba.
11	Merchant TMĐT chấp nhận thanh toán trên trang thanh toán của chính mình và tự quản lý website. Dữ liệu truyền qua Internet bởi chính merchant.
12	Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động
13	Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu truyền qua sóng di động hoặc Wi-Fi.
14	Thiết bị đầu cuối thanh toán ảo được truy cập thông qua trình duyệt Internet của merchant. Dữ liệu truyền qua Internet.

Gợi ý cách sử dụng tài liệu

XÁC ĐỊNH MÔ HÌNH GIỐNG VỚI HỆ THỐNG THANH TOÁN CỦA BẠN NHẤT:

- Tài liệu này, được dùng để bổ sung cho [Guide to Safe Payment](#), sẽ mô tả mô hình các hệ thống thanh toán phổ biến nhất, bắt đầu từ rất đơn giản đến phức tạp
- Mỗi mô hình thanh toán sẽ đề cập 4 nội dung:
 - 1) Tổng quan
 - 2) Rủi ro - những khả năng dữ liệu thẻ bị lộ
 - 3) Hiểm họa - cách tội phạm mạng chiếm dữ liệu thẻ
 - 4) Phòng chống - phương án đề xuất để bảo vệ dữ liệu thẻ.
- Xác định mô hình giống với hệ thống của bạn nhất.



TÌM HIỂU VỀ RỦI RO VÀ HIỂM HOA CỦA BẠN:

- Khi tìm được hệ thống thanh toán gần giống với hệ thống của bạn nhất, hãy xem hai hình kế tiếp để xác định dữ liệu thẻ của bạn rủi ro ở đâu và các khả năng doanh nghiệp của bạn bị tổn thương trước các cuộc tấn công mạng.

BẢO VỆ DỮ LIỆU THẺ VÀ DOANH NGHIỆP BẰNG CÁC BIỆN PHÁP AN NINH CƠ BẢN:

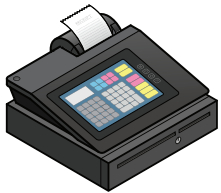
- Cuối cùng, hãy xem hình thứ tư của hệ thống với các đề xuất biện pháp an ninh cơ bản nhằm giúp bạn bảo vệ doanh nghiệp của mình.

Ý nghĩa của thuật ngữ

Tùy thuộc vào nơi bạn sống, các thiết bị thanh toán điện tử có thể được đặt tên khác nhau. Các thuật ngữ sau đây sẽ được sử dụng để mô tả các thiết bị sau.



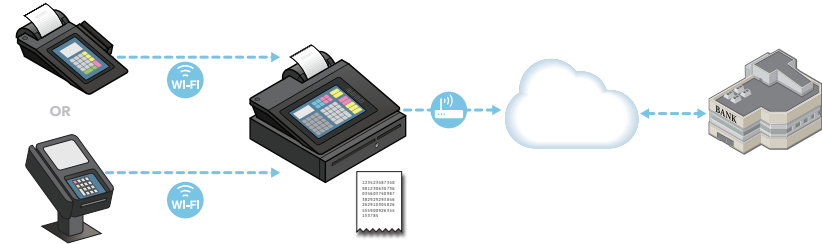
Một **THIẾT BỊ ĐẦU CUỐI THANH TOÁN** là thiết bị được sử dụng để chấp nhận thanh toán qua thẻ bằng cách quẹt, cắm hoặc nhập số thẻ vào thiết bị. POS, máy đọc thẻ tín dụng, thiết bị đầu cuối PDQ, thiết bị đầu cuối cho thẻ chip/ EMV đều được coi là thiết bị đầu cuối thanh toán



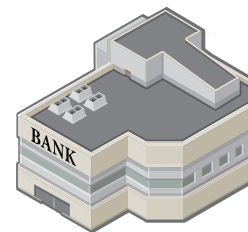
Một **MÁY TÍNH TIỀN ĐIỆN TỬ** có khả năng tính giá trị của giao dịch, có thể in hoá đơn, nhưng không chấp nhận thanh toán thẻ tín dụng.



Một **THIẾT BỊ ĐẦU CUỐI THANH TOÁN TÍCH HỢP** là một thiết bị đầu cuối thanh toán kèm máy tính tiền điện tử, với các tính năng tính giá trị giao dịch, in hoá đơn và chấp nhận thanh toán bằng thẻ tín dụng



Một **HỆ THỐNG THANH TOÁN** bao gồm toàn bộ quá trình chấp nhận thẻ thanh toán tại một điểm bán lẻ (bao gồm gian hàng, cửa hàng, website TMĐT) và có thể bao gồm thiết bị đầu cuối thanh toán, máy tính tiền điện tử, các thiết bị và hệ thống khác kết nối với thiết bị đầu cuối thanh toán (ví dụ, thiết bị phát Wi-Fi hay máy tính kiểm soát hàng tồn kho), máy chủ với các thành phần thương mại điện tử như trang thanh toán, đường kết nối đến ngân hàng của merchant.



Một **NGÂN HÀNG CỦA MERCHANT** là một ngân hàng hoặc một tổ chức tín dụng xử lý các giao dịch bằng thẻ tín dụng hoặc thẻ ghi nợ thay mặt cho merchant. Các thuật ngữ **Acquirer**, **acquiring bank**, và **card** hoặc **payment processor** cũng có ý nghĩa tương tự.

Thiết bị đầu cuối thanh toán dial up. Dữ liệu thanh toán truyền qua đường thoại.



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.

THIẾT BỊ ĐẦU CUỐI THANH TOÁN DIAL UP

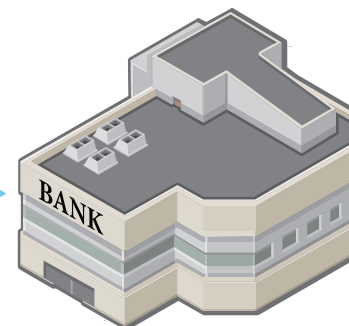
Thiết bị đầu cuối thanh toán dial up cho thấy nó quay số cho mỗi giao dịch



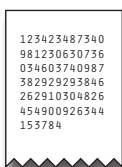
Thiết bị đầu cuối thanh toán được kết nối với ngân hàng thông qua đường truyền dial up



PHONE LINE



Sao kê với dữ liệu thẻ



Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán dial up. Dữ liệu thanh toán truyền qua đường thoại.



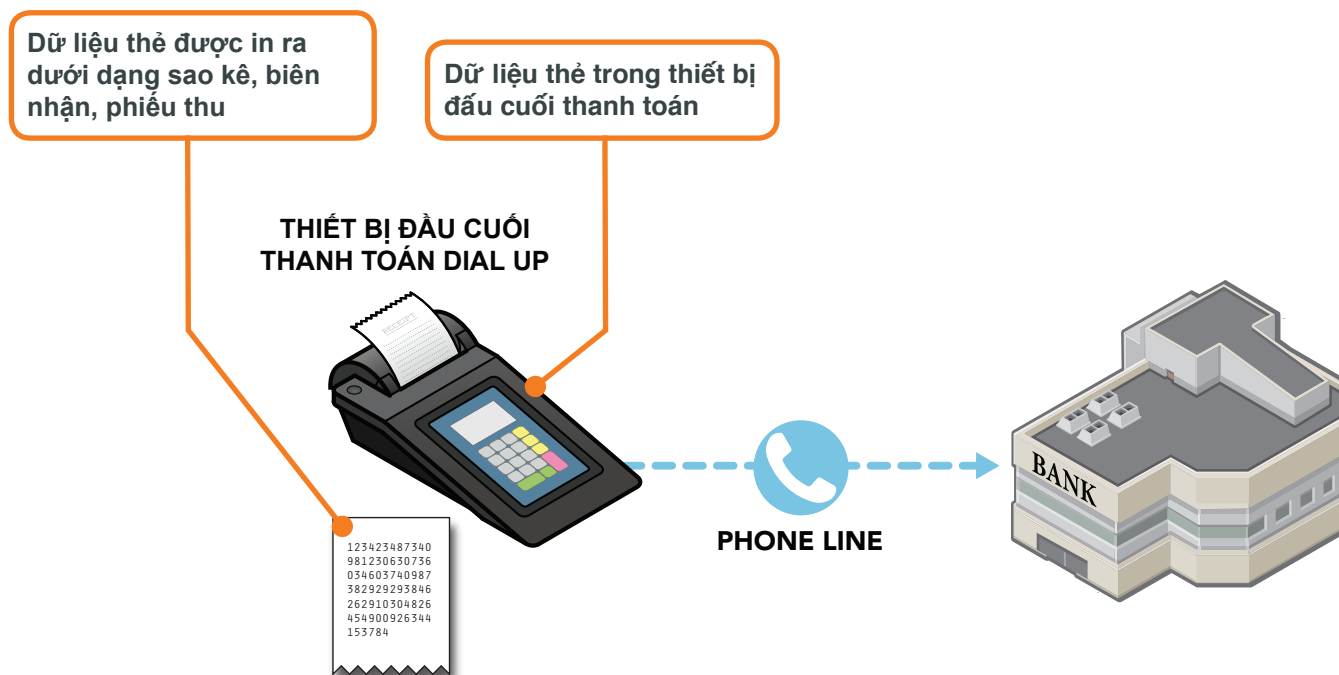
TYPE 1 OVERVIEW

TYPE 1 RISKS

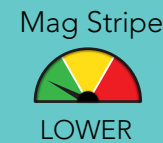
TYPE 1 THREATS

TYPE 1 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối thanh toán dial up. Dữ liệu thanh toán truyền qua đường thoại.



TYPE 1 OVERVIEW

TYPE 1 RISKS

TYPE 1 THREATS

TYPE 1 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?

Chúng ăn cắp các phiếu thu, sao kê, hoá đơn được in ra mà không được bạn bảo mật, vẫn còn giữ khi không cần hoặc vứt bỏ cầu thả.

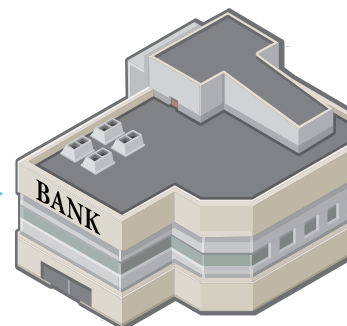
Chúng ăn cắp dữ liệu thẻ bằng các thiết bị “gián điệp” gắn/ nhúng vào thiết bị đầu cuối thanh toán của bạn

Chúng đánh cắp thiết bị đầu cuối của bạn rồi thay thế chúng bằng một thiết bị khác nhằm chiếm đoạt dữ liệu thẻ

THIẾT BỊ ĐẦU CUỐI
THANH TOÁN DIAL UP



123423487340
981230630736
034603740987
38292939846
262910304826
454900926344
153784



Thiết bị đầu cuối thanh toán dial up. Dữ liệu thanh toán truyền qua đường thoại.



Bạn cần làm gì để bảo mật dữ liệu thẻ?



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết

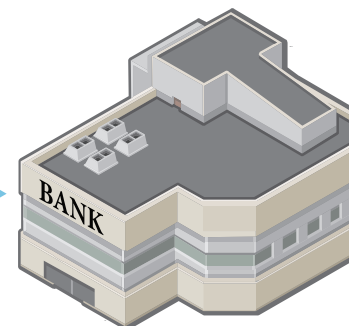
THIẾT BỊ ĐẦU CUỐI THANH TOÁN DIAL UP



123423487340
981230630736
034603740987
382929293846
262910304826
454900926344
153784



PHONE LINE



Thiết bị đầu cuối thanh toán dial up và máy tính tiền điện tử kết nối Internet. Dữ liệu thanh toán truyền qua đường thoại.

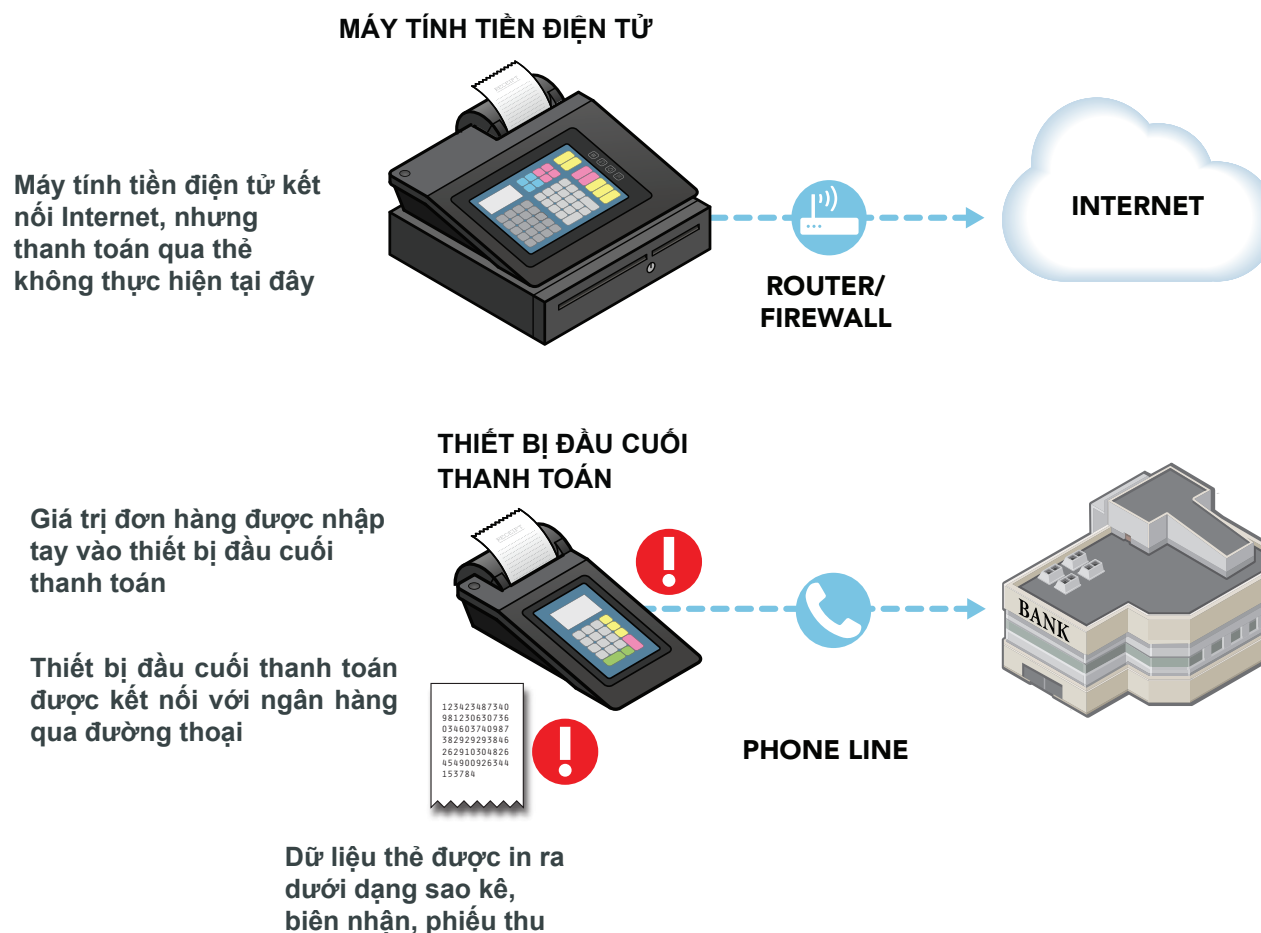


TYPE 2 OVERVIEW

TYPE 2 RISKS

TYPE 2 THREATS

TYPE 2 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.

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán dial up và máy tính tiền điện tử kết nối Internet. Dữ liệu thanh toán truyền qua đường thoại.



TYPE 2 OVERVIEW

TYPE 2 RISKS

TYPE 2 THREATS

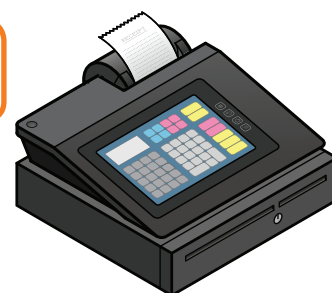
TYPE 2 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?

MÁY TÍNH TIỀN ĐIỆN TỬ

Dữ liệu thẻ trong thiết bị đầu cuối thanh toán

Dữ liệu thẻ được in ra dưới dạng sao kê, biên nhận, phiếu thu



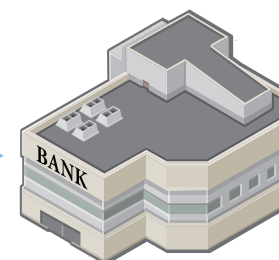
ROUTER/
FIREWALL

INTERNET

THIẾT BỊ ĐẦU CÚI THANH TOÁN



PHONE LINE



Thiết bị đầu cuối thanh toán dial up và máy tính tiền điện tử kết nối Internet. Dữ liệu thanh toán truyền qua đường thoại.



TYPE 2 OVERVIEW

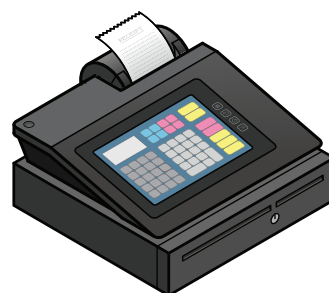
TYPE 2 RISKS

TYPE 2 THREATS

TYPE 2 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?

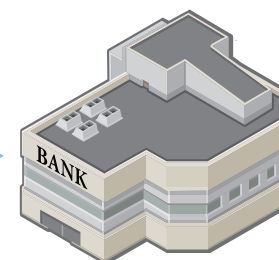
MÁY TÍNH TIỀN ĐIỆN TỬ

ROUTER/
FIREWALL

INTERNET

THIẾT BỊ ĐẦU CUỐI
THANH TOÁN

PHONE LINE



Chúng ăn cắp dữ liệu thẻ bằng các thiết bị “gián điệp” gắn/ nhúng vào thiết bị đầu cuối thanh toán của bạn

Chúng đánh cắp thiết bị đầu cuối của bạn rồi thay thế chúng bằng một thiết bị khác nhằm chiếm đoạt dữ liệu thẻ

Chúng ăn cắp các phiếu thu, sao kê, hoá đơn được in ra mà không được bạn bảo mật, vẫn còn giữ khi không cần hoặc vứt bỏ cầu thả.

123425487340
981250650736
034605740987
582929293846
262910304826
454000926344
153784

Thiết bị đầu cuối thanh toán dial up và máy tính tiền điện tử kết nối Internet. Dữ liệu thanh toán truyền qua đường thoại.



TYPE 2 OVERVIEW

TYPE 2 RISKS

TYPE 2 THREATS

TYPE 2 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần

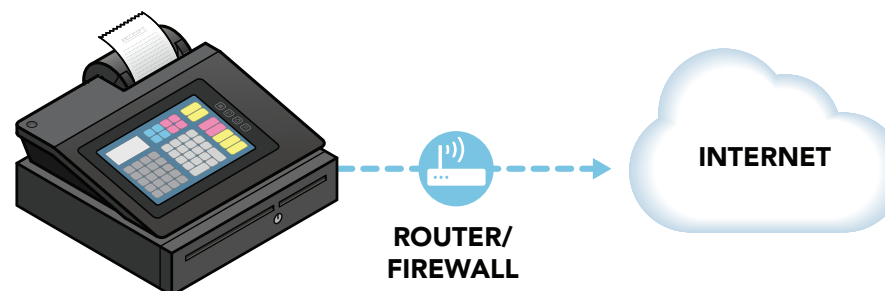


Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán

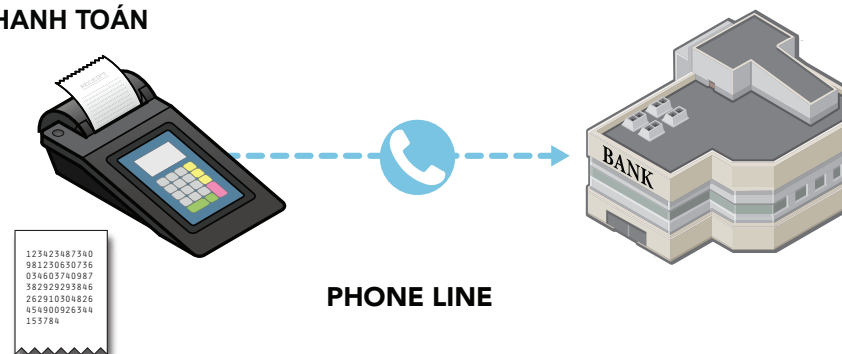


Yêu cầu nhà cung cấp hỗ trợ khi cần thiết

MÁY TÍNH TIỀN ĐIỆN TỬ



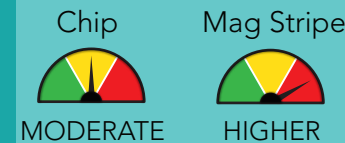
THIẾT BỊ ĐẦU CUỐI THANH TOÁN



123425487340
981250650736
034605740987
582929293846
262910304826
454900926344
153784

Thiết bị đầu cuối thanh toán có kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền.

RISK PROFILE



TYPE 3 OVERVIEW

TYPE 3 RISKS

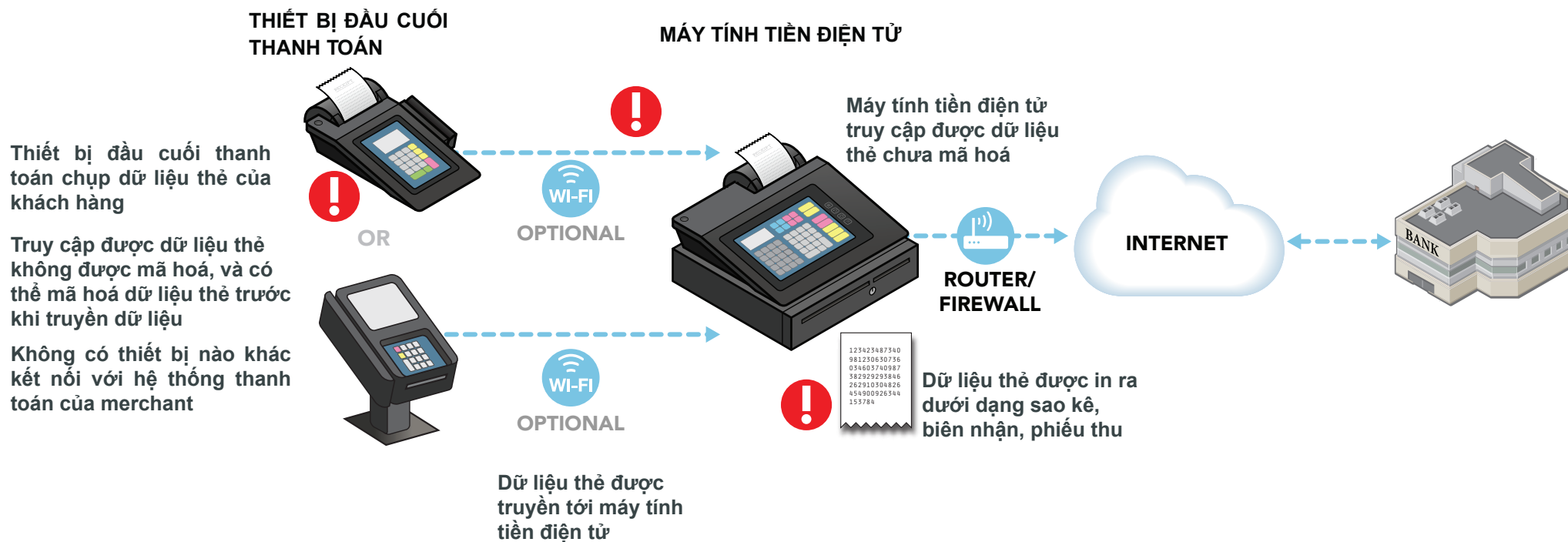
TYPE 3 THREATS

TYPE 3 PROTECTIONS

YES
This IS my setup.
Show me the details.

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

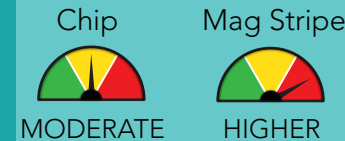
BACK
to previous diagram.



Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán có kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền.

RISK PROFILE



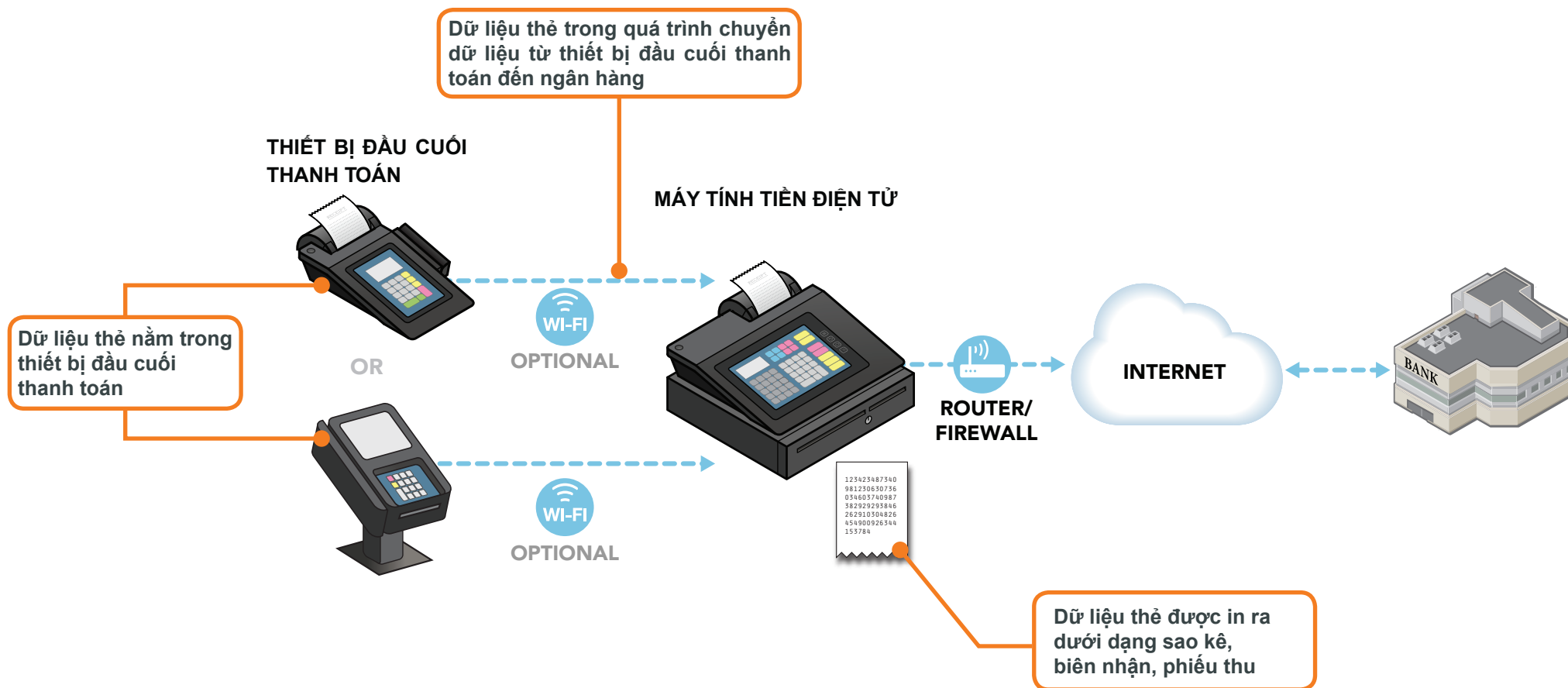
TYPE 3 OVERVIEW

TYPE 3 RISKS

TYPE 3 THREATS

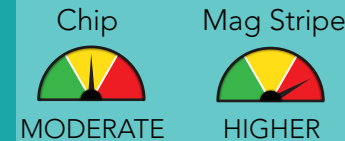
TYPE 3 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối thanh toán có kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền.

RISK PROFILE



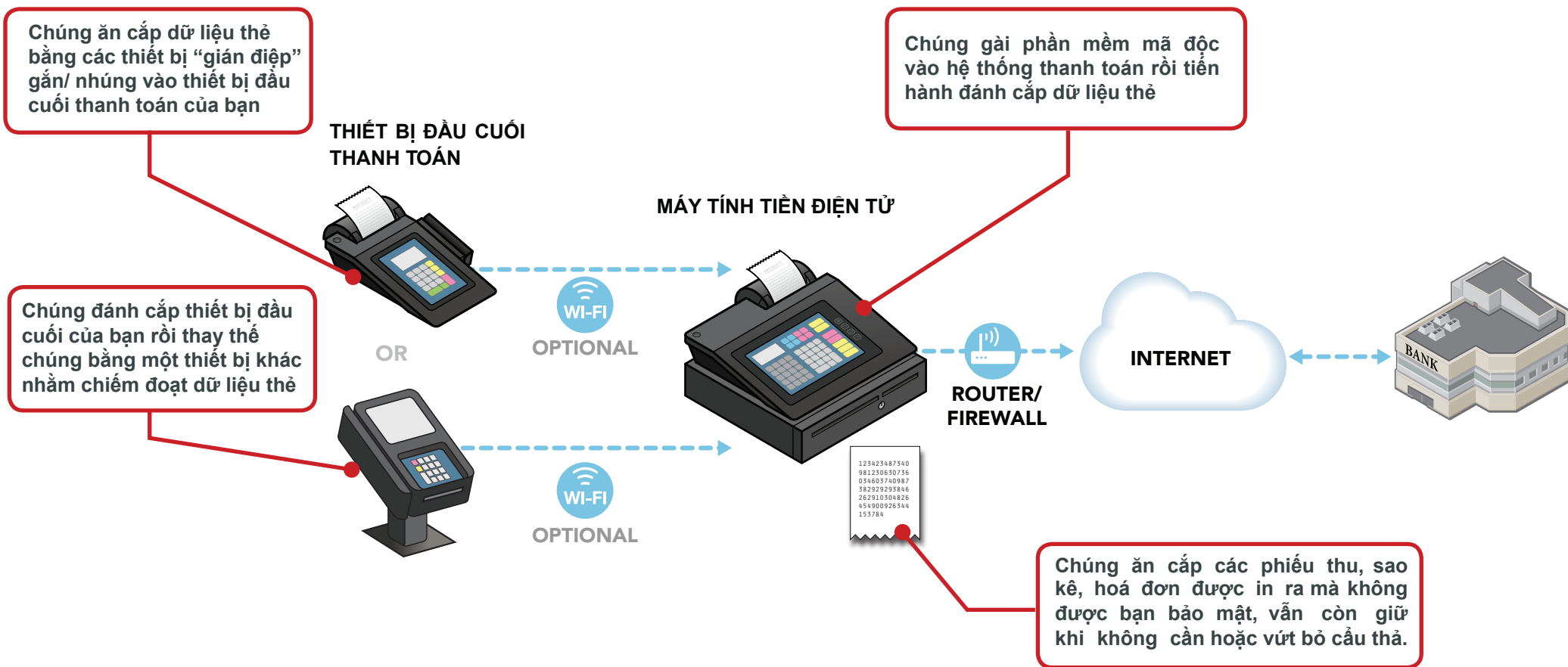
TYPE 3 OVERVIEW

TYPE 3 RISKS

TYPE 3 THREATS

TYPE 3 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối thanh toán có kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền.

RISK PROFILE

Chip

MODERATE

Mag Stripe

HIGHER

TYPE 3 OVERVIEW

TYPE 3 RISKS

TYPE 3 THREATS

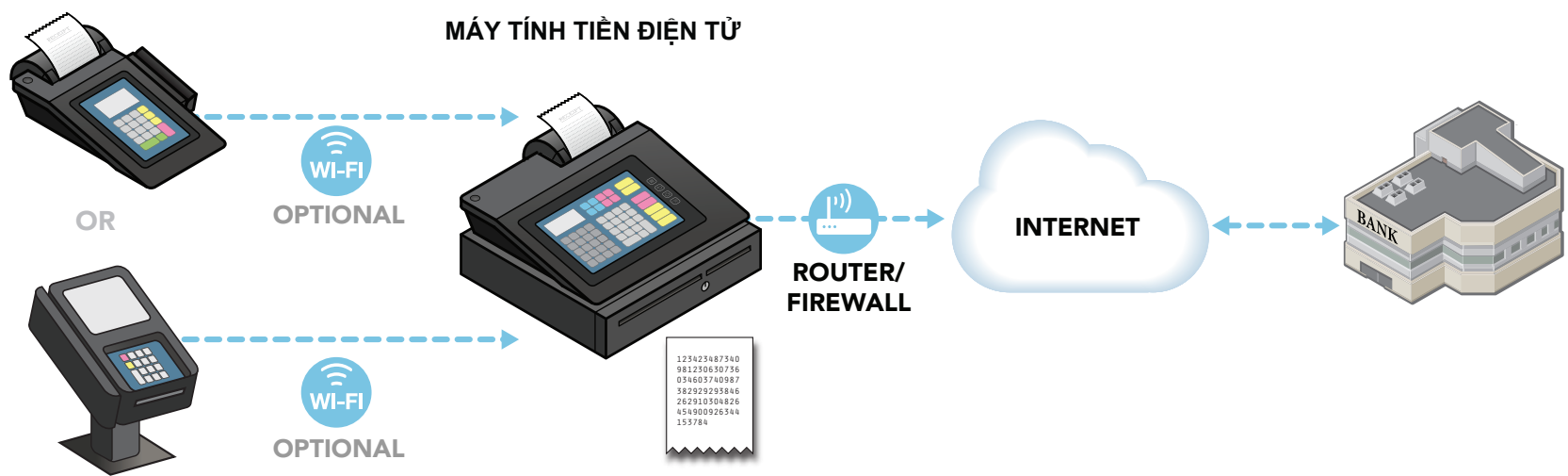
TYPE 3 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?

- Dùng mật khẩu mạnh
- Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần
- Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán
- Cài đặt các bản vá từ nhà cung cấp thiết bị đầu cuối thanh toán
- Yêu cầu nhà cung cấp hỗ trợ khi cần thiết
- Giới hạn quyền truy cập nội bộ vào dữ liệu thẻ
- Định kỳ rà soát lỗ hổng an ninh
- Sử dụng thiết bị đầu cuối thanh toán chính hãng
- Bảo vệ doanh nghiệp trước mặt trái của Internet
- Làm cho dữ liệu thẻ trở nên vô dụng với tội phạm mạng

THIẾT BỊ ĐẦU CUỐI THANH TOÁN

MÁY TÍNH TIỀN ĐIỆN TỬ



1234567890
9876543210
0123456789
8765432109
7654321098
6543210987
5432109876
4321098765
3210987654
2109876543
1098765432
0987654321

Thiết bị đầu cuối thanh toán có chức năng mã hoá kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền điện tử



TYPE 4 OVERVIEW

TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 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.

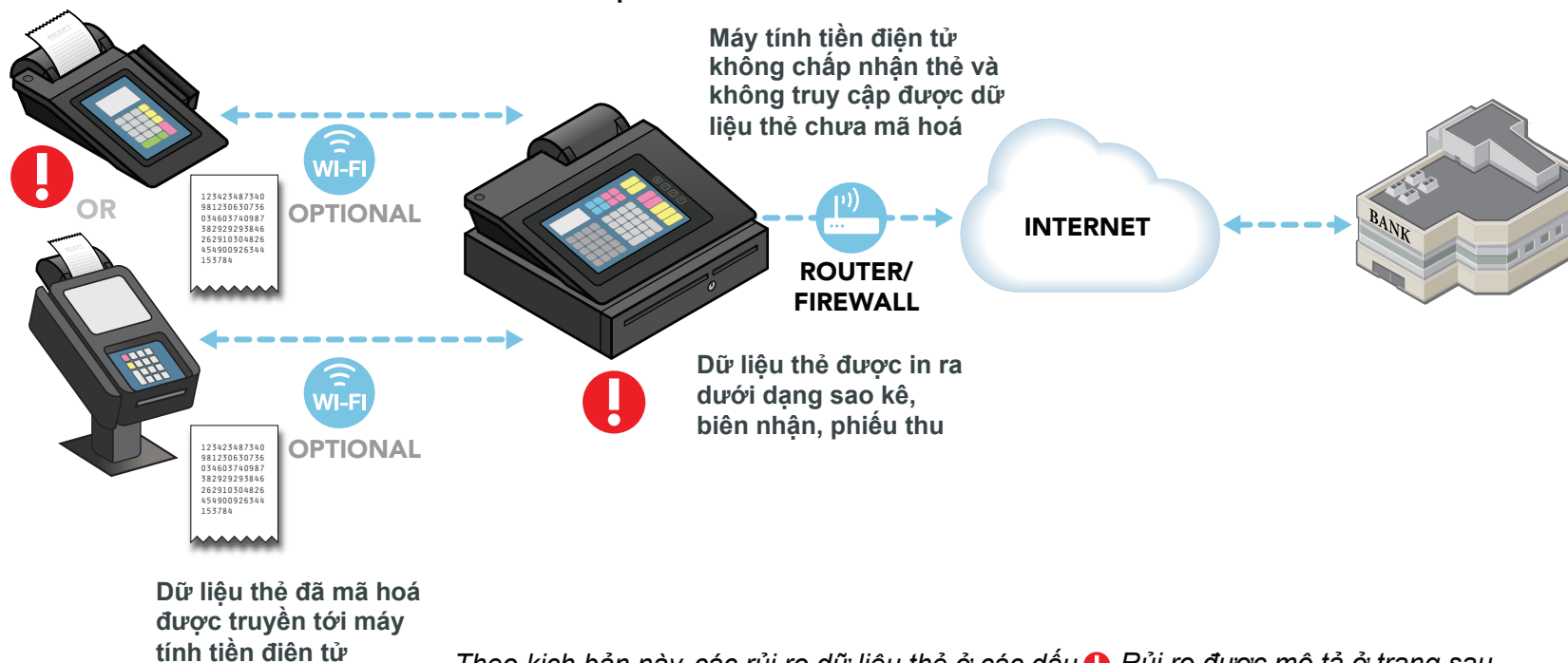
THIẾT BỊ ĐẦU CUỐI THANH TOÁN

MÁY TÍNH TIỀN ĐIỆN TỬ

Thiết bị đầu cuối thanh toán mã hoá dữ liệu thẻ (ví dụ, sử dụng giao thức đọc và trao đổi dữ liệu bảo mật PCI - PCI SRED)

Merchant không có quyền truy cập vào dữ liệu không được mã hoá

Không có thiết bị nào khác kết nối với hệ thống thanh toán của merchant



Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán có chức năng mã hoá kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền điện tử



TYPE 4 OVERVIEW

TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?

THIẾT BỊ ĐẦU CUỐI THANH TOÁN

MÁY TÍNH TIỀN ĐIỆN TỬ



Thiết bị đầu cuối thanh toán có chức năng mã hoá kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền điện tử



TYPE 4 OVERVIEW

TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?

Chúng ăn cắp dữ liệu thẻ bằng các thiết bị “gián điệp” gắn/ nhúng vào thiết bị đầu cuối thanh toán của bạn

THIẾT BỊ ĐẦU CUỐI THANH TOÁN

MÁY TÍNH TIỀN ĐIỆN TỬ

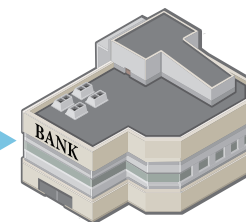
WI-FI
OPTIONAL

OR

WI-FI
OPTIONAL

ROUTER/
FIREWALL

INTERNET



Chúng đánh cắp thiết bị đầu cuối của bạn rồi thay thế chúng bằng một thiết bị khác nhằm chiếm đoạt dữ liệu thẻ

Chúng ăn cắp các phiếu thu, sao kê, hoá đơn được in ra mà không được bạn bảo mật, vẫn còn giữ khi không cần hoặc vứt bỏ cầu thả.

Thiết bị đầu cuối thanh toán có chức năng mã hoá kết nối với máy tính tiền điện tử. Dữ liệu thanh toán truyền qua Internet bằng máy tính tiền điện tử



TYPE 4 OVERVIEW

TYPE 4 RISKS

TYPE 4 THREATS

TYPE 4 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Cài đặt các bản vá từ nhà cung cấp thiết bị đầu cuối thanh toán



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập



Định kỳ rà soát lỗ hổng an ninh



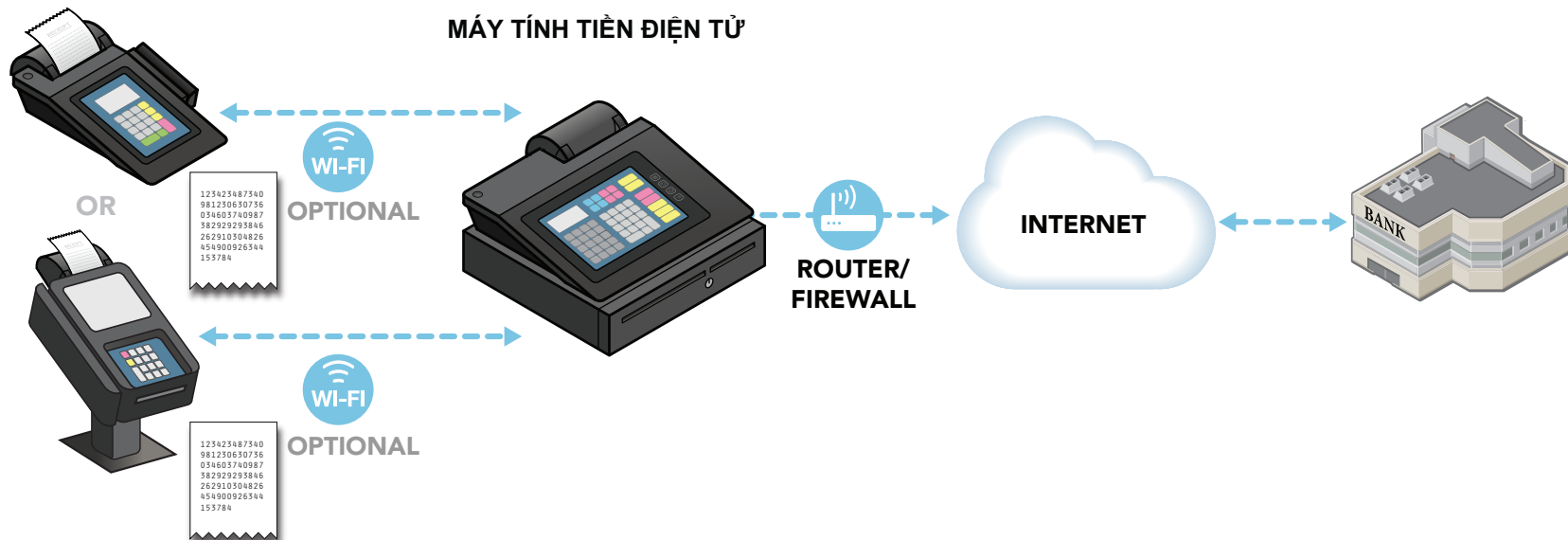
Sử dụng thiết bị đầu cuối thanh toán chính hãng



Bảo vệ doanh nghiệp trước mặt trái của Internet

THIẾT BỊ ĐẦU CUỐI THANH TOÁN

MÁY TÍNH TIỀN ĐIỆN TỬ



Thiết bị đầu cuối có chức năng mã hoá và máy tính tiền kết nối Internet. Dữ liệu thanh toán truyền qua Internet bằng thiết bị đầu cuối thanh toán.



cuối thanh

TYPE 5 OVERVIEW

TYPE 5 RISKS

TYPE 5 THREATS

TYPE 5 PROTECTIONS

Merchant không có quyền truy cập vào dữ liệu không được mã hoá

Không có thiết bị nào khác kết nối với hệ thống thanh toán của merchant

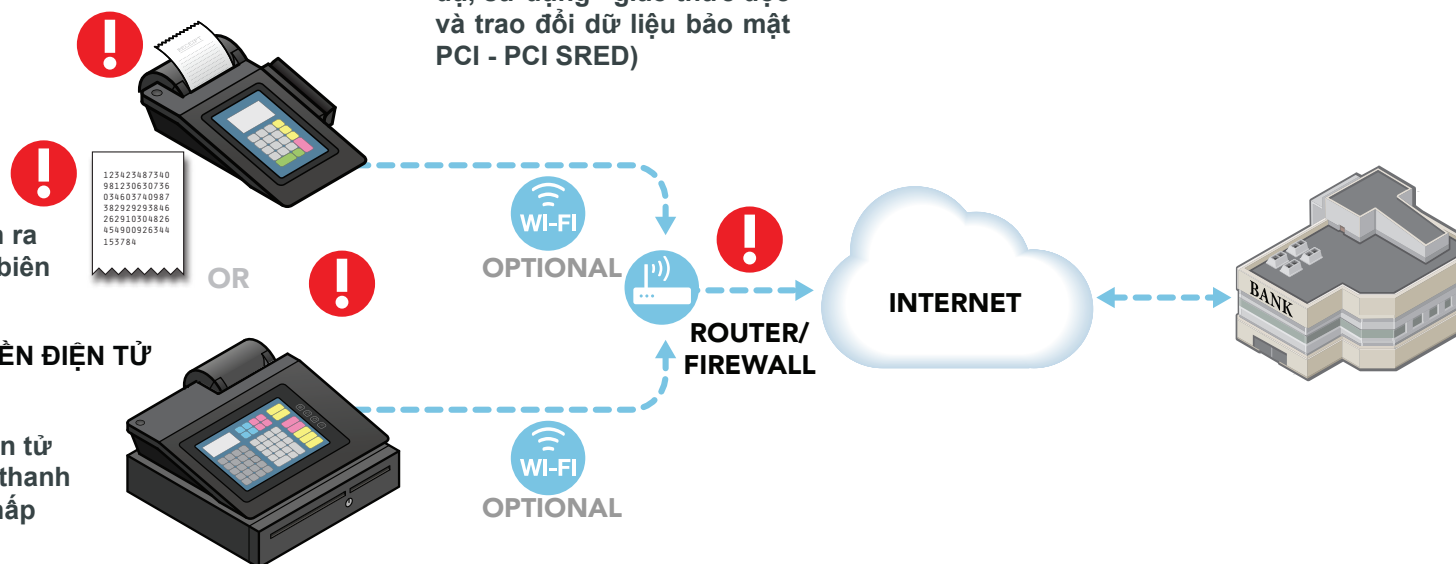
Dữ liệu thẻ được in ra dưới dạng sao kê, biên nhận, phiếu thu

MÁY TÍNH TIỀN ĐIỆN TỬ

Giá trị đơn hàng từ máy tính tiền điện tử được nhập tay vào thiết bị đầu cuối thanh toán. Máy tính tiền điện tử không chấp nhận thanh toán thẻ

THIẾT BỊ ĐẦU CUỐI THANH TOÁN

Thiết bị đầu cuối thanh toán mã hoá dữ liệu thẻ (ví dụ, sử dụng giao thức đọc và trao đổi dữ liệu bảo mật PCI - PCI SRED)



YES

This IS my setup.
Show me the details.

NO

This IS NOT my setup.
Show me the next setup.

BACK

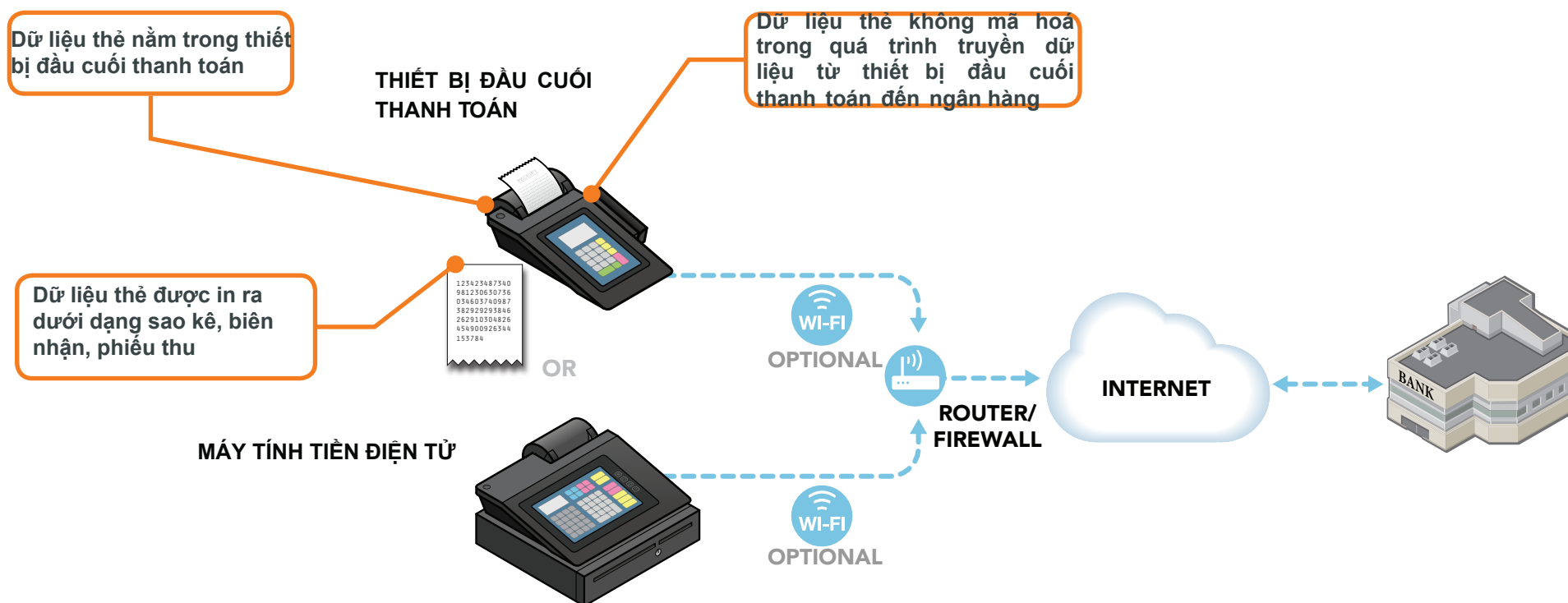
to previous diagram.

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối có chức năng mã hoá và máy tính tiền kết nối Internet. Dữ liệu thanh toán truyền qua Internet bằng thiết bị đầu cuối thanh toán.



Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối có chức năng mã hoá và máy tính tiền kết nối Internet. Dữ liệu thanh toán truyền qua Internet bằng thiết bị đầu cuối thanh toán.



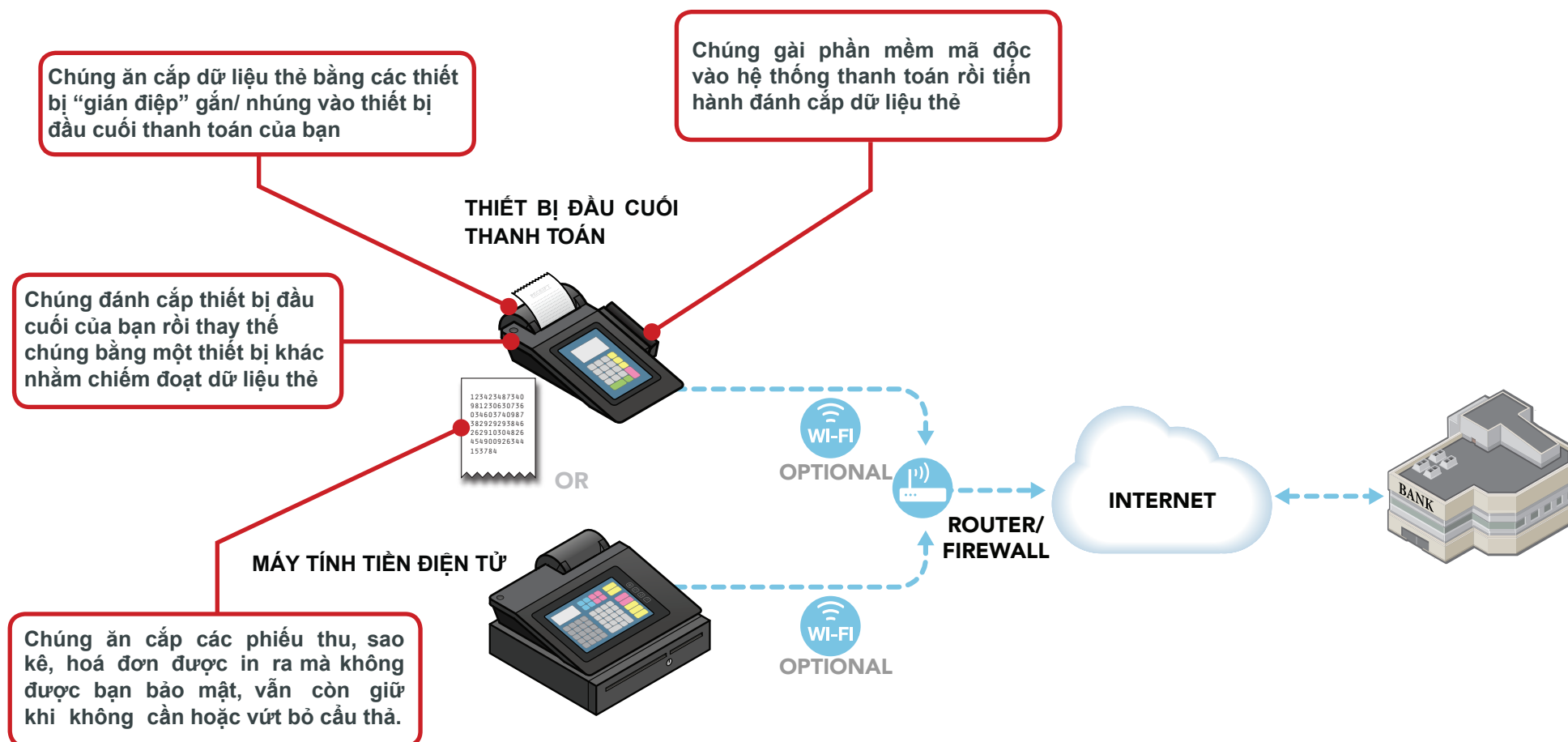
TYPE 5 OVERVIEW

TYPE 5 RISKS

TYPE 5 THREATS

TYPE 5 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối có chức năng mã hoá và máy tính tiền kết nối Internet. Dữ liệu thanh toán truyền qua Internet bằng thiết bị đầu cuối thanh toán.



TYPE 5 OVERVIEW

TYPE 5 RISKS

TYPE 5 THREATS

TYPE 5 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Sử dụng thiết bị đầu cuối thanh toán chính hãng



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ

Bảo vệ doanh nghiệp trước mặt trái của Internet



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập

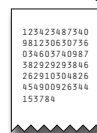


Cài đặt các bản vá từ nhà cung cấp thiết bị đầu cuối thanh toán



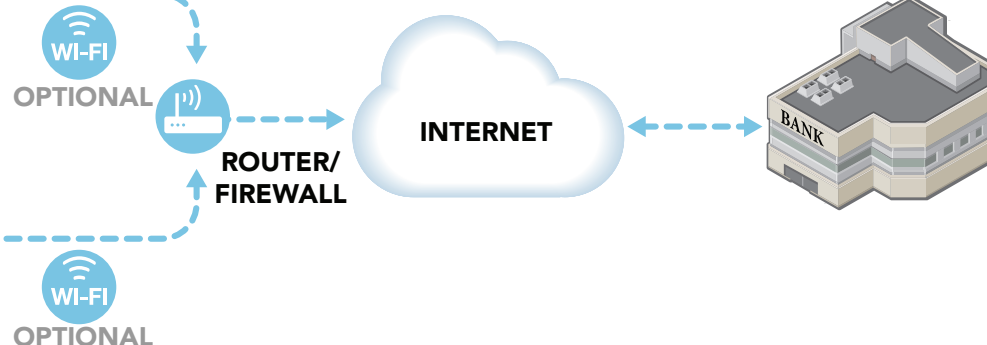
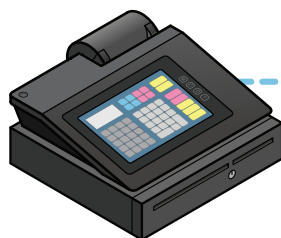
Định kỳ rà soát lỗ hổng an ninh

THIẾT BỊ ĐẦU CUỐI THANH TOÁN



OR

MÁY TÍNH TIỀN ĐIỆN TỬ



Thiết bị đầu cuối thanh toán có chức năng mã hoá và máy tính tiền điện tử chia sẻ dữ liệu phi thẻ. Dữ liệu truyền qua Internet bằng thiết bị đầu cuối



TYPE 6 OVERVIEW

TYPE 6 RISKS

TYPE 6 THREATS

TYPE 6 PROTECTIONS

Không có dữ liệu thẻ được chia sẻ giữa máy tính tiền điện tử và thiết bị đầu cuối thanh toán

Không có thiết bị nào khác kết nối với hệ thống thanh toán của merchant

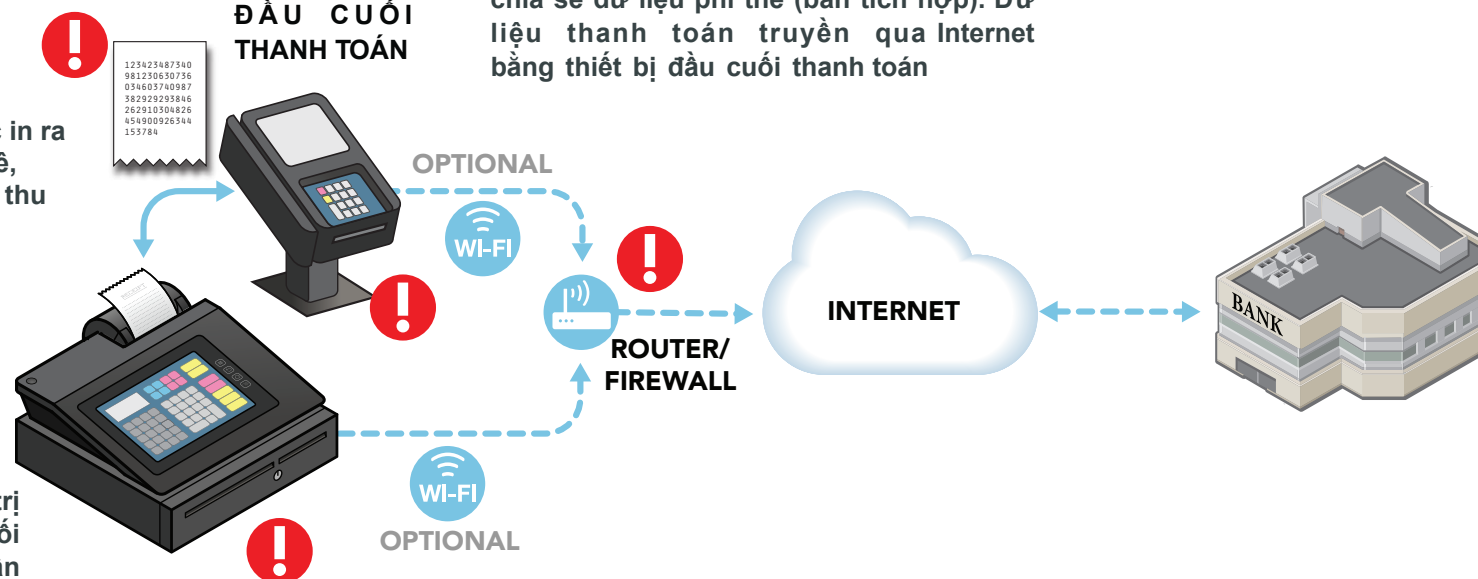
Dữ liệu thẻ được in ra dưới dạng sao kê, biên nhận, phiếu thu

MÁY TÍNH TIỀN ĐIỆN TỬ

Máy tính tiền điện tử gửi giá trị đơn hàng đến thiết bị đầu cuối thanh toán; không chấp nhận thanh toán bằng thẻ từ máy tính tiền điện tử

THIẾT BỊ
ĐẦU CUỐI
THANH TOÁN

Thiết bị đầu cuối thanh toán có khả năng mã hoá và máy tính tiền điện tử chia sẻ dữ liệu phi thẻ (bán tích hợp). Dữ liệu thanh toán truyền qua Internet bằng thiết bị đầu cuối thanh toán



YES

This IS my setup.
Show me the details.

NO

This IS NOT my setup.
Show me the next setup.

BACK

to previous diagram.

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán có chức năng mã hoá và máy tính tiền điện tử chia sẻ dữ liệu phi thẻ. Dữ liệu truyền qua Internet bằng thiết bị đầu cuối



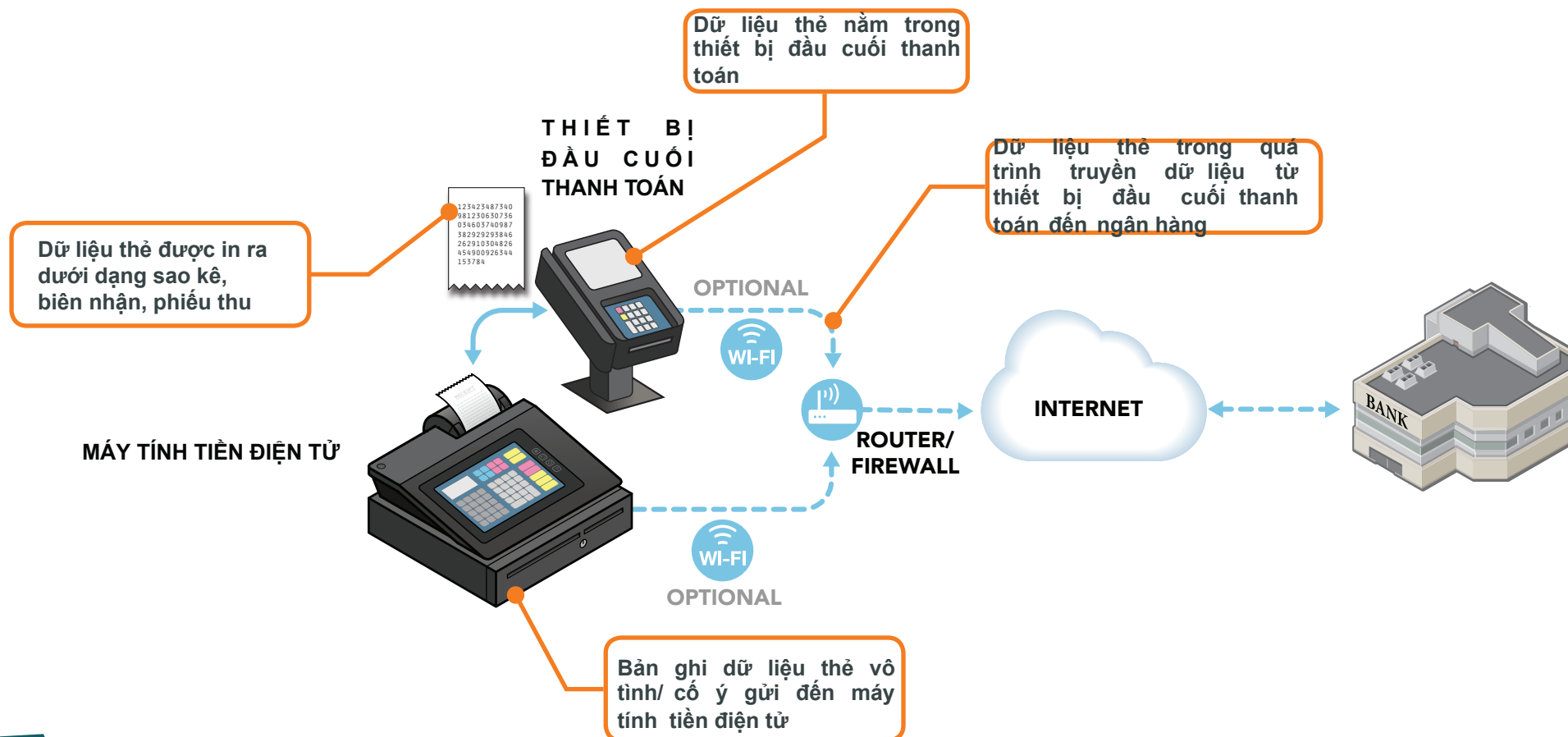
TYPE 6 OVERVIEW

TYPE 6 RISKS

TYPE 6 THREATS

TYPE 6 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối thanh toán có chức năng mã hoá và máy tính tiền điện tử chia sẻ dữ liệu phi thẻ. Dữ liệu truyền qua Internet bằng thiết bị đầu cuối

RISK PROFILE



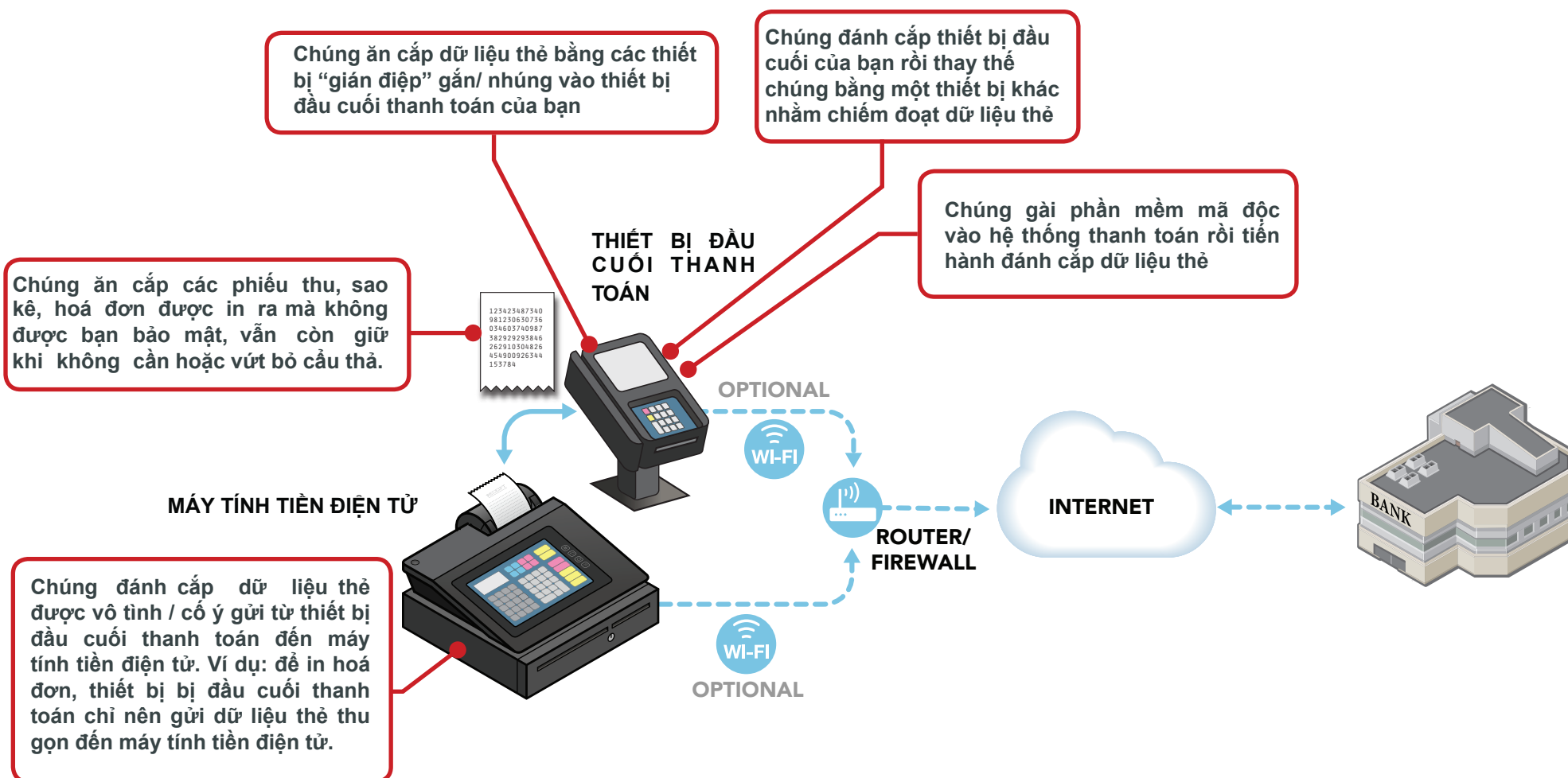
TYPE 6 OVERVIEW

TYPE 6 RISKS

TYPE 6 THREATS

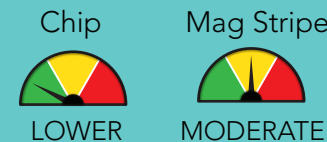
TYPE 6 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối thanh toán có chức năng mã hoá và máy tính tiền điện tử chia sẻ dữ liệu phi thẻ. Dữ liệu truyền qua Internet bằng thiết bị đầu cuối

RISK PROFILE



TYPE 6 OVERVIEW

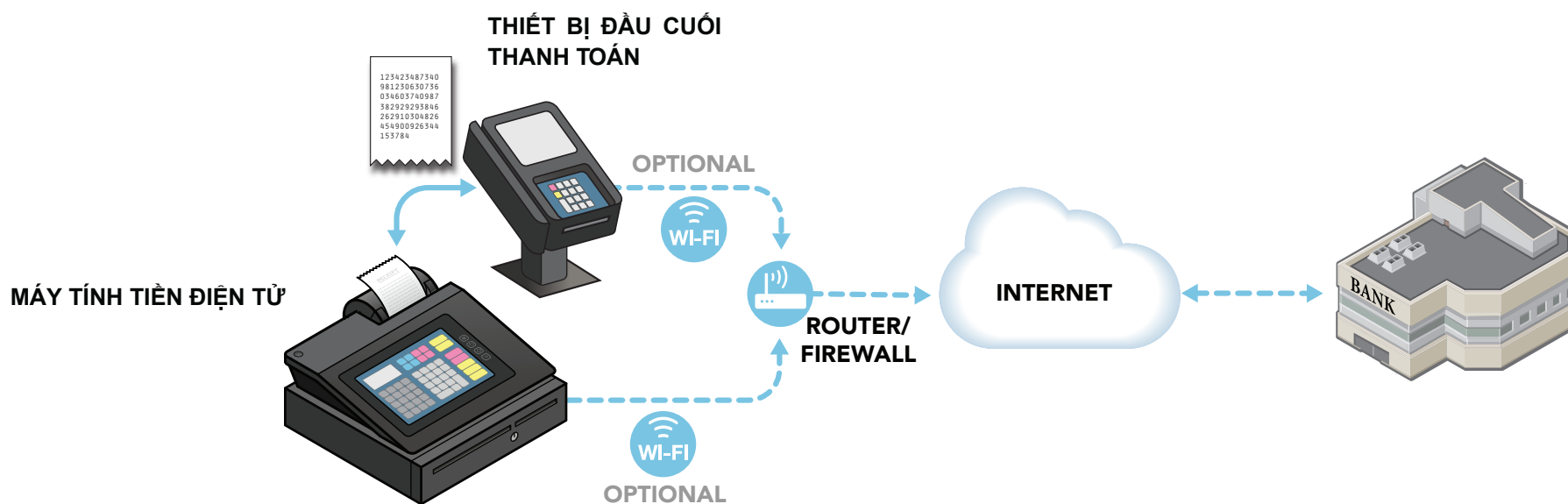
TYPE 6 RISKS

TYPE 6 THREATS

TYPE 6 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?

- Dùng mật khẩu mạnh
- Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ
- Bảo vệ doanh nghiệp trước mặt trái của Internet
- Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần
- Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập
- Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán
- Định kỳ rà soát lỗ hổng an ninh
- Yêu cầu nhà cung cấp hỗ trợ khi cần thiết
- Sử dụng thiết bị đầu cuối thanh toán chính hãng



Thiết bị đầu cuối thanh toán tích hợp và phần mềm trung gian chia sẻ dữ liệu thẻ. Dữ liệu thanh toán truyền qua Internet.



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.

Thiết bị đầu cuối thanh toán tích hợp với máy tính tiền điện tử

Thẻ được quét bởi nhân viên; sơ đồ không áp dụng đối với thẻ chip

Không có thiết bị nhập mã PIN riêng biệt

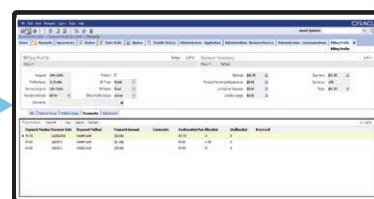
Không có thiết bị nào khác kết nối với hệ thống thanh toán của merchant

THIẾT BỊ ĐẦU CUỐI THANH TOÁN TÍCH HỢP



Thiết bị đầu cuối thanh toán chia sẻ dữ liệu thẻ với phần mềm trung gian thanh toán

PHẦN MỀM TRUNG GIAN THANH TOÁN

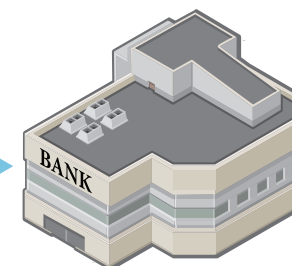


Phần mềm được sử dụng như 1 phần của giao dịch thanh toán

ROUTER/FIREWALL



INTERNET

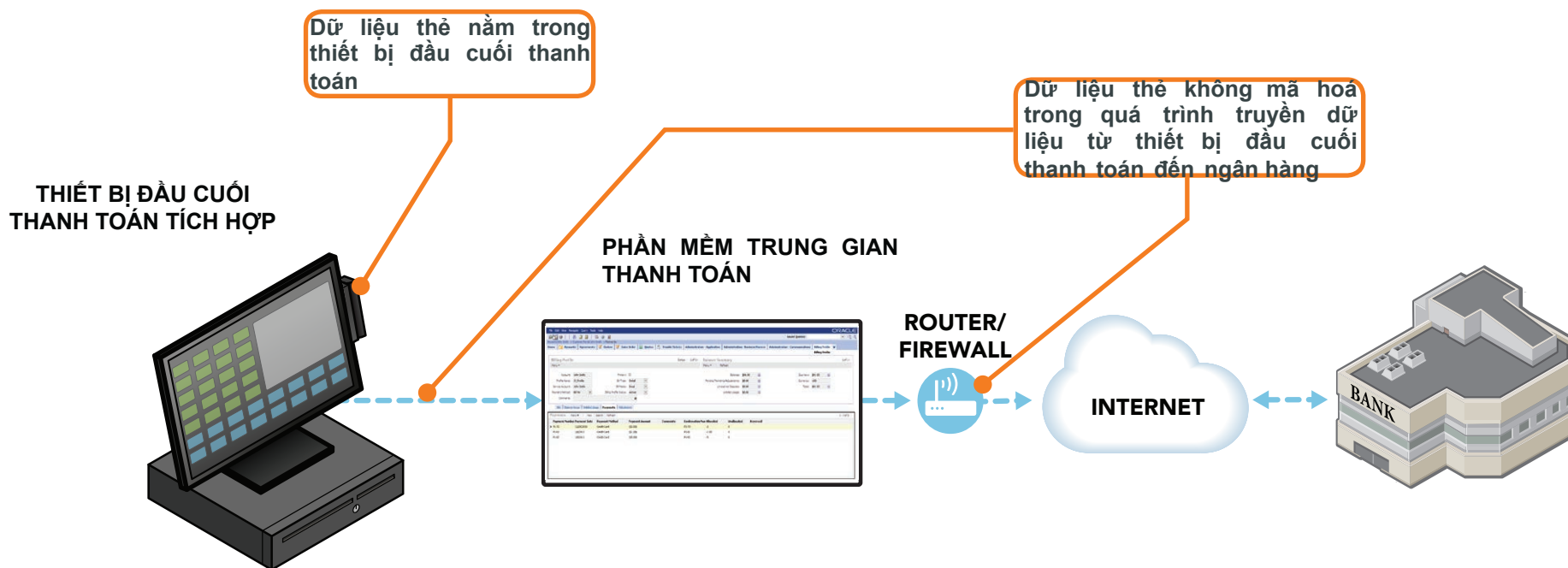


Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán tích hợp và phần mềm trung gian chia sẻ dữ liệu thẻ. Dữ liệu thanh toán truyền qua Internet.



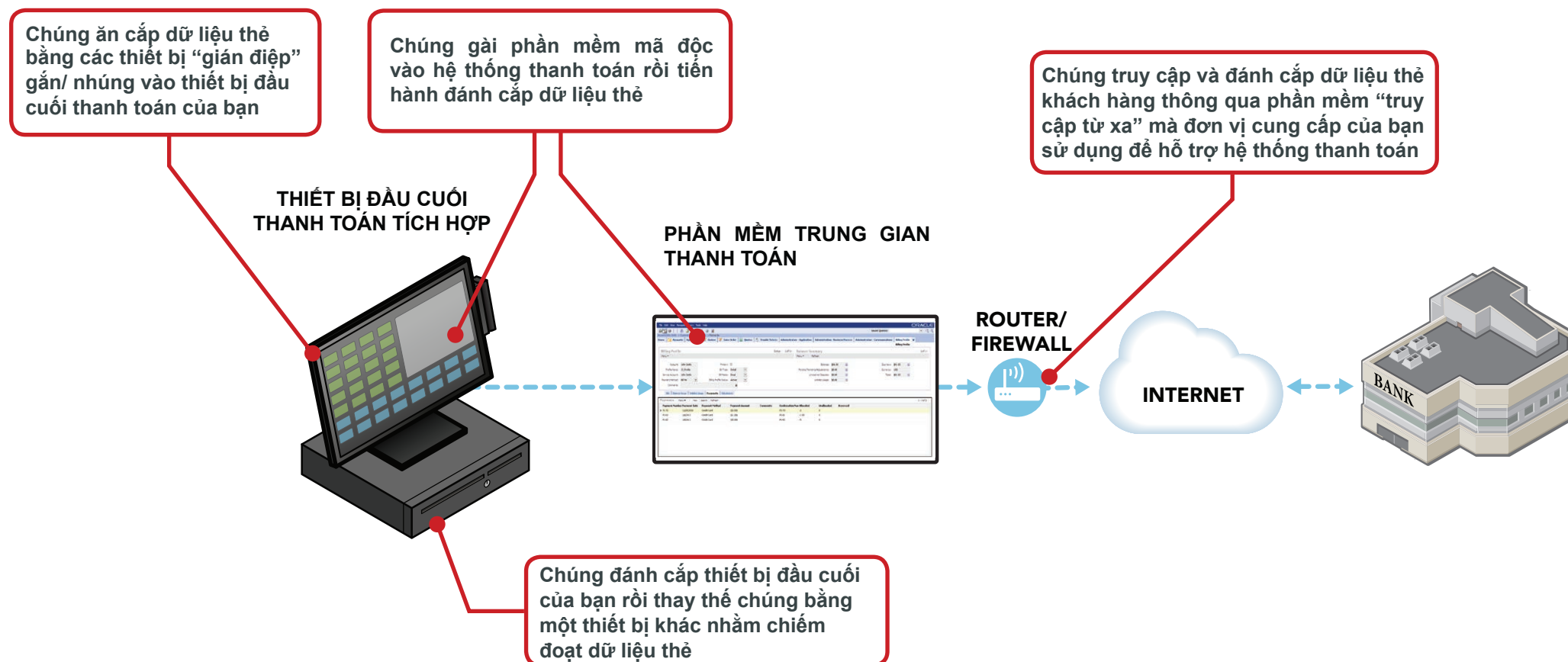
Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối thanh toán tích hợp và phần mềm trung gian chia sẻ dữ liệu thẻ. Dữ liệu thanh toán truyền qua Internet.



Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối thanh toán tích hợp và phần mềm trung gian chia sẻ dữ liệu thẻ. Dữ liệu thanh toán truyền qua Internet.



TYPE 7 OVERVIEW

TYPE 7 RISKS

TYPE 7 THREATS

TYPE 7 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập



Sử dụng phần mềm anti-virus



Định kỳ rà soát lỗ hổng an ninh



Sử dụng thiết bị đầu cuối thanh toán chính hãng



Bảo vệ doanh nghiệp trước mặt trái của Internet

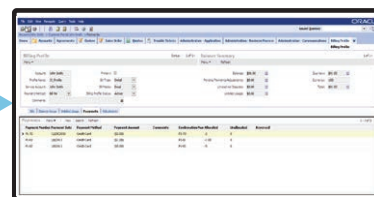


Khiến cho dữ liệu thẻ trở nên vô dụng với tội phạm

THIẾT BỊ ĐẦU CUỐI THANH TOÁN TÍCH HỢP



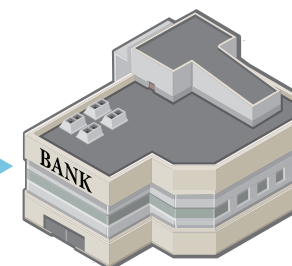
PHẦN MỀM TRUNG GIAN THANH TOÁN



ROUTER/FIREWALL



INTERNET



Thiết bị đầu cuối thanh toán không dây mã hoá với thiết bị đầu cuối thanh toán được tích hợp và phần mềm trung gian. Dữ liệu truyền qua Internet.



TYPE 8 OVERVIEW

TYPE 8 RISKS

TYPE 8 THREATS

TYPE 8 PROTECTIONS

Dữ liệu thẻ được mã hoá được chia sẻ với thiết bị đầu cuối thanh toán và phần mềm trung gian

Không có thiết bị nào khác kết nối với hệ thống thanh toán của merchant

THIẾT BỊ ĐẦU CUỐI THANH TOÁN TÍCH HỢP

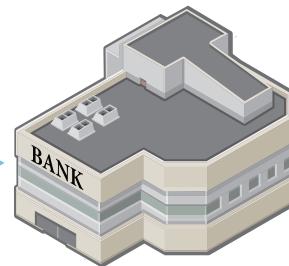
Thiết bị đầu cuối thanh toán mã hoá dữ liệu thẻ (ví dụ, sử dụng giao thức đọc và trao đổi dữ liệu bảo mật PCI - PCI SRED)

Thiết bị đầu cuối thanh toán tích hợp với đầu đọc thẻ đã được vô hiệu hoá

PHẦN MỀM TRUNG GIAN THANH TOÁN

ROUTER/FIREWALL

INTERNET



THIẾT BỊ ĐẦU CUỐI THANH TOÁN KHÔNG DÂY



Thanh toán được tiến hành qua thiết bị đầu cuối thanh toán không dây

Phần mềm được sử dụng như 1 phần của giao dịch thanh toán

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

YES

This IS my setup.
Show me the details.

NO

This IS NOT my setup.
Show me the next setup.

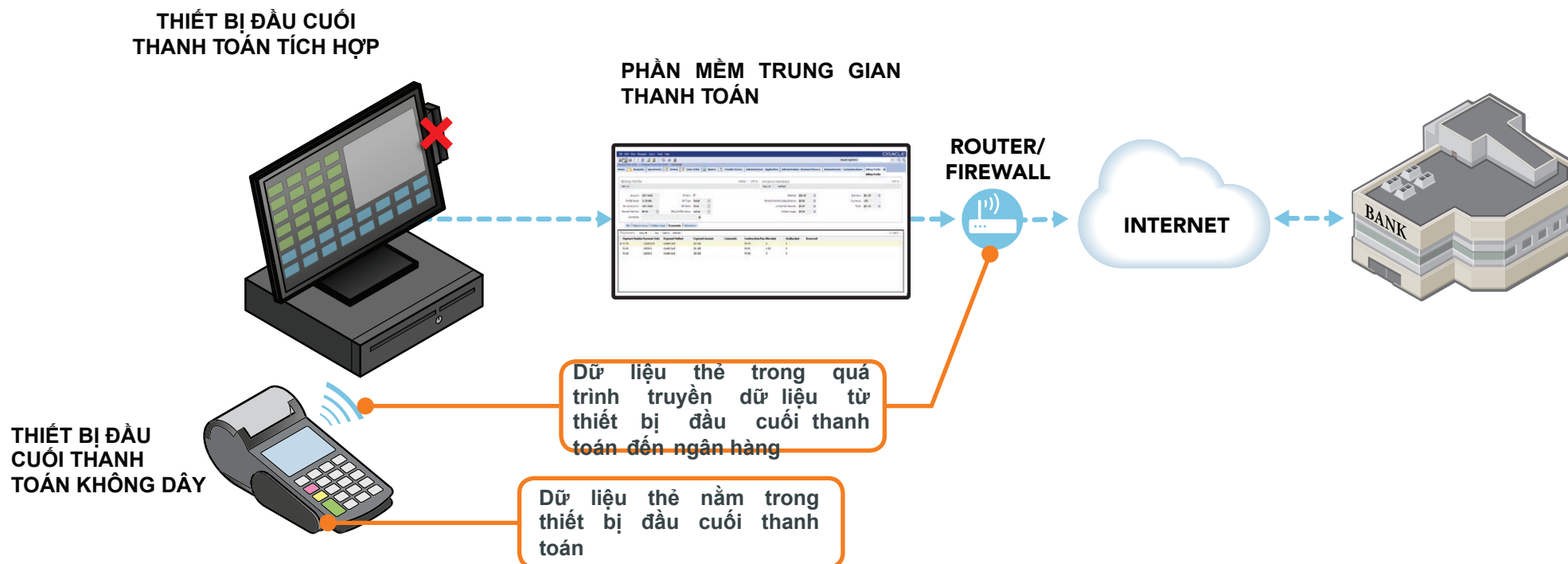
BACK

to previous diagram.

Thiết bị đầu cuối thanh toán không dây mã hoá với thiết bị đầu cuối thanh toán được tích hợp và phần mềm trung gian. Dữ liệu truyền qua Internet.



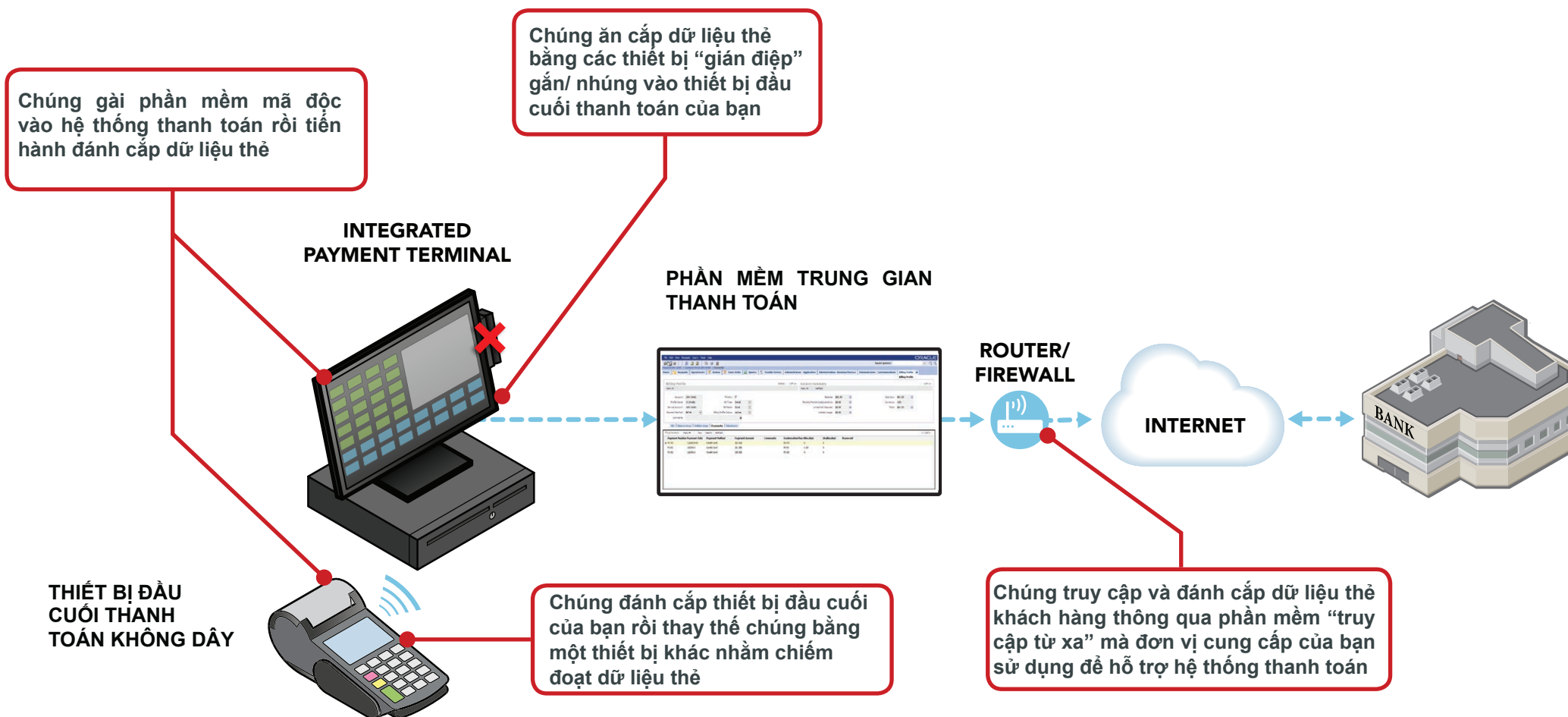
Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối thanh toán không dây mã hoá với thiết bị đầu cuối thanh toán được tích hợp và phần mềm trung gian. Dữ liệu truyền qua Internet.



Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối thanh toán không dây mã hoá với thiết bị đầu cuối thanh toán được tích hợp và phần mềm trung gian. Dữ liệu truyền qua Internet.

RISK PROFILE



TYPE 8 OVERVIEW

TYPE 8 RISKS

TYPE 8 THREATS

TYPE 8 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập



Sử dụng phần mềm anti-virus



Định kỳ rà soát lỗ hổng an ninh



Sử dụng thiết bị đầu cuối thanh toán chính hãng



Bảo vệ doanh nghiệp trước mặt trái của Internet

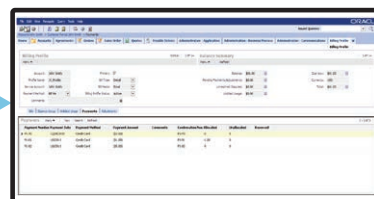


Khiến cho dữ liệu thẻ trở nên vô dụng với tội phạm

THIẾT BỊ ĐẦU CỐI THANH TOÁN TÍCH HỢP



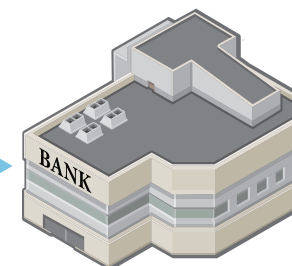
PHẦN MỀM TRUNG GIAN THANH TOÁN



ROUTER/
FIREWALL



INTERNET



THIẾT BỊ ĐẦU CỐI THANH TOÁN KHÔNG DÂY



Thiết bị đầu cuối thanh toán kết nối với máy tính tiền điện tử có gắn thêm thiết bị. Dữ liệu thanh toán truyền qua Internet.

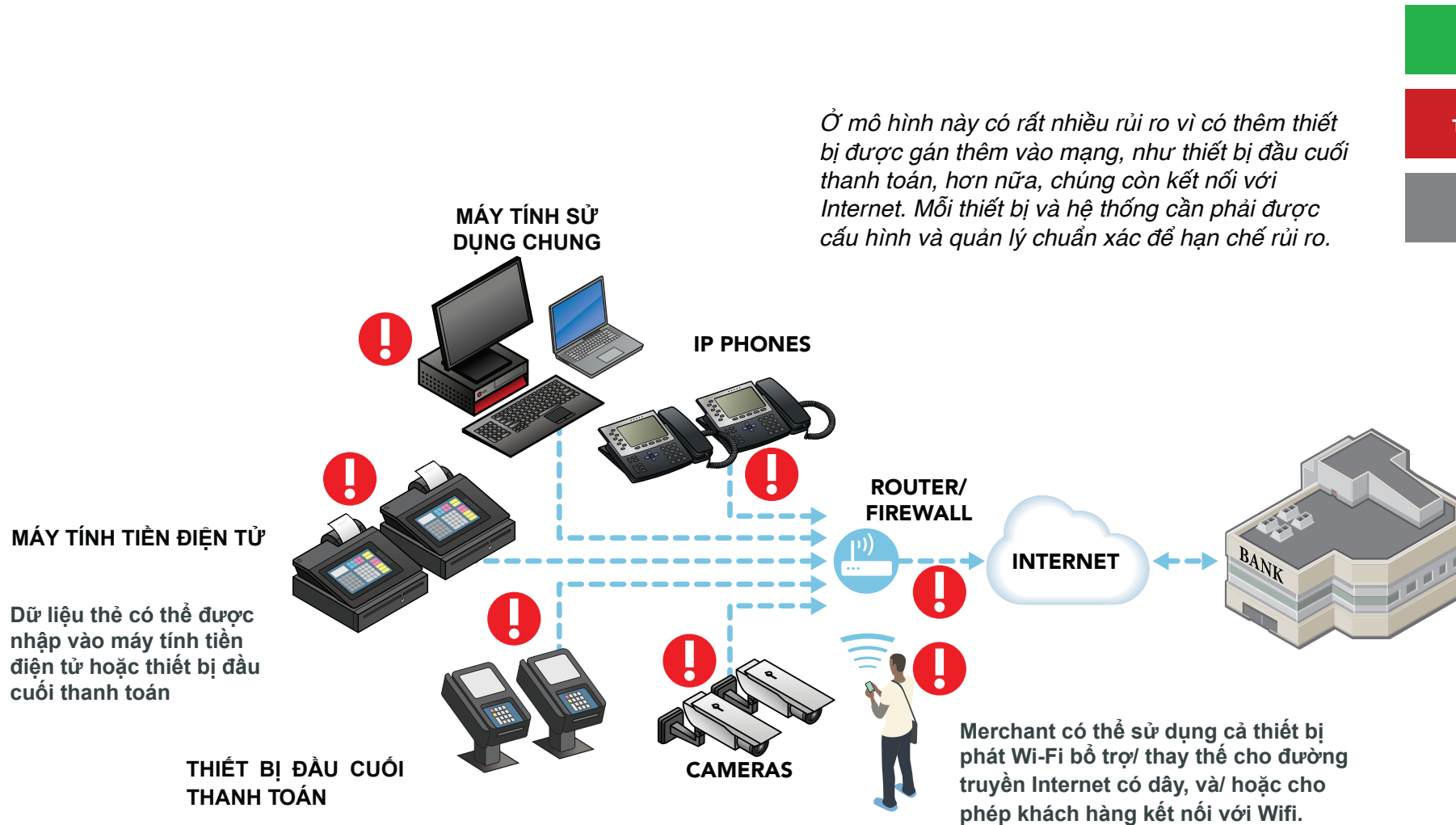


TYPE 9 OVERVIEW

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.

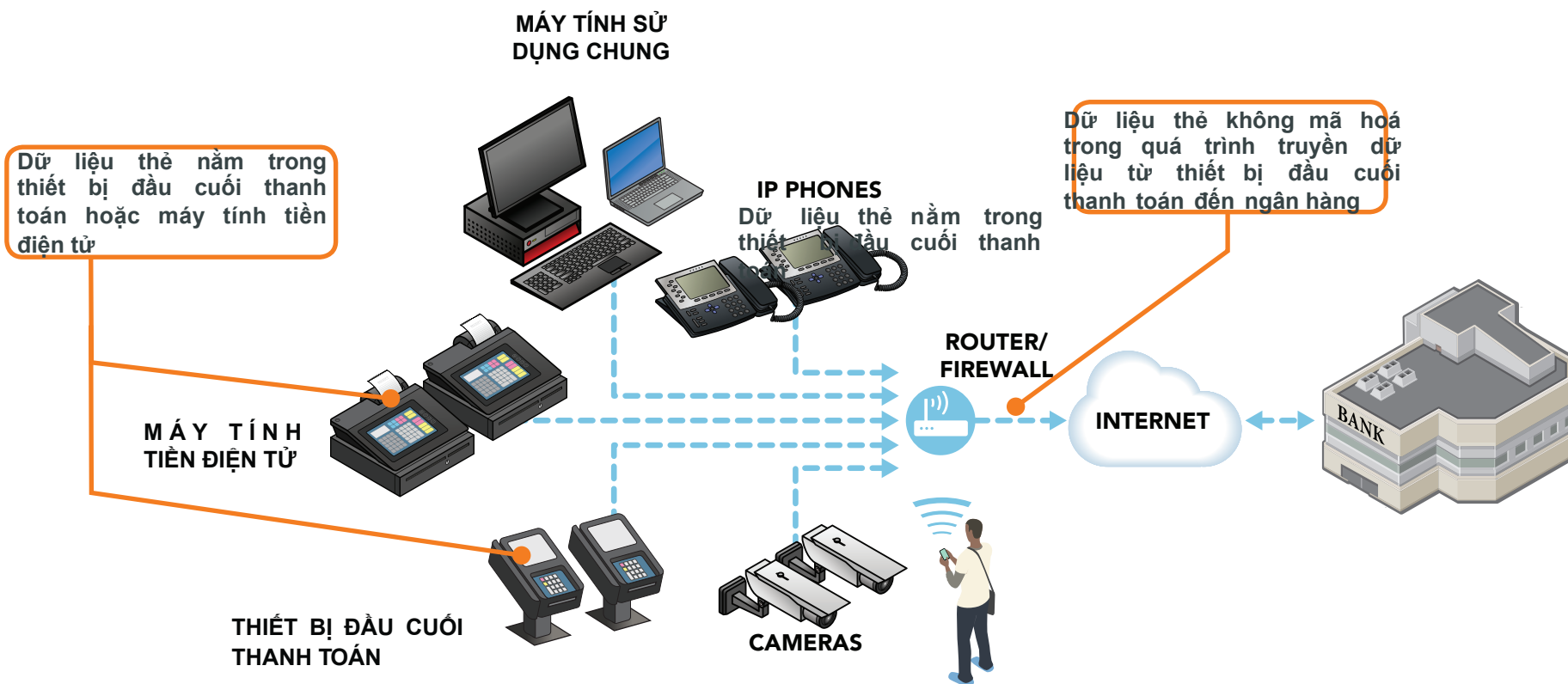
BACK

to previous diagram.

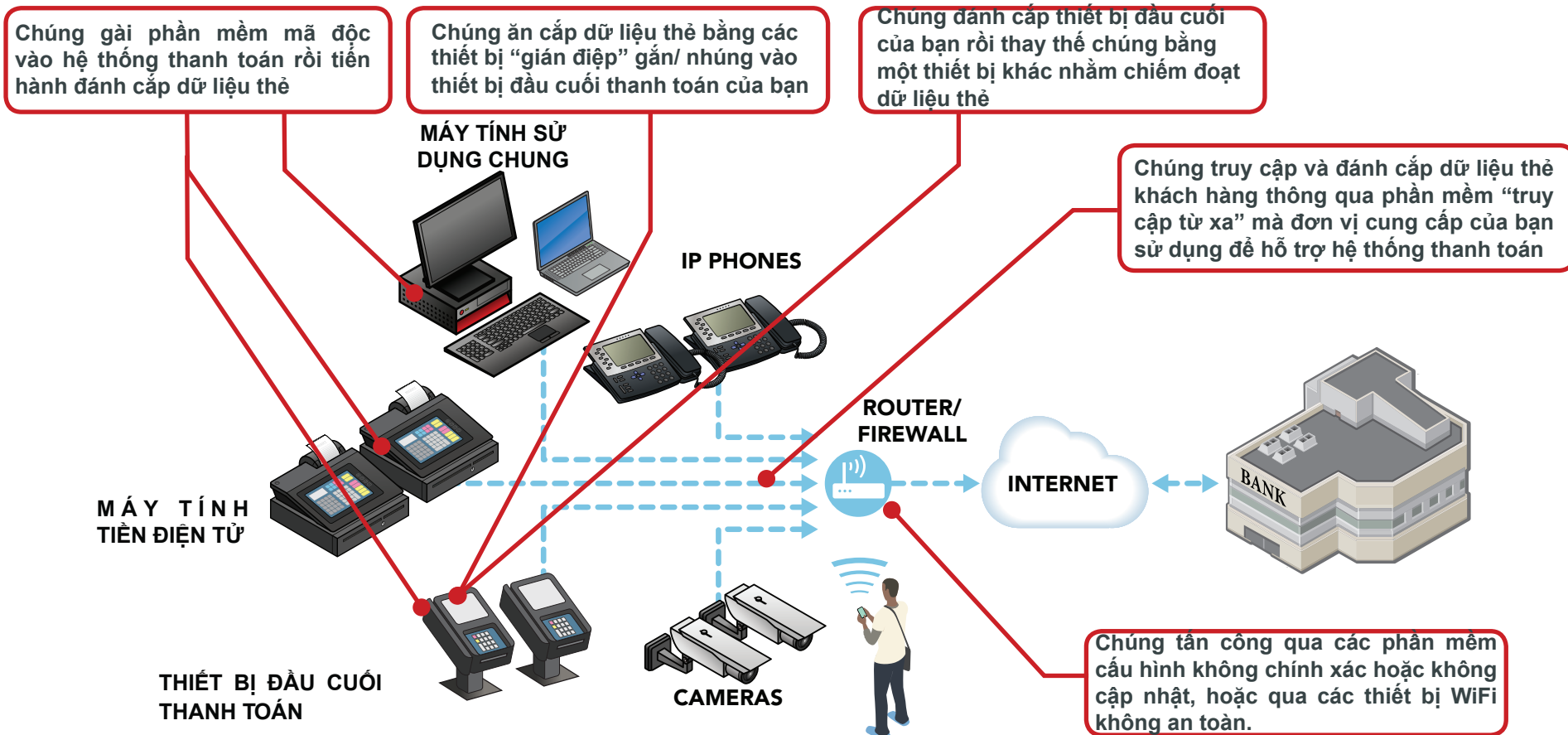
Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán kết nối với máy tính tiền điện tử có gắn thêm thiết bị. Dữ liệu thanh toán truyền qua Internet.

Rủi ro dữ liệu thẻ nằm ở đâu?



Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối thanh toán kết nối với máy tính tiền điện tử có gắn thêm thiết bị. Dữ liệu thanh toán truyền qua Internet.

TYPE 9 OVERVIEW

TYPE 9 RISKS

TYPE 9 THREATS

TYPE 9 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ



Sử dụng thiết bị đầu cuối thanh toán chính hãng



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập



Bảo vệ doanh nghiệp trước mặt trái của Internet



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Sử dụng phần mềm anti-virus



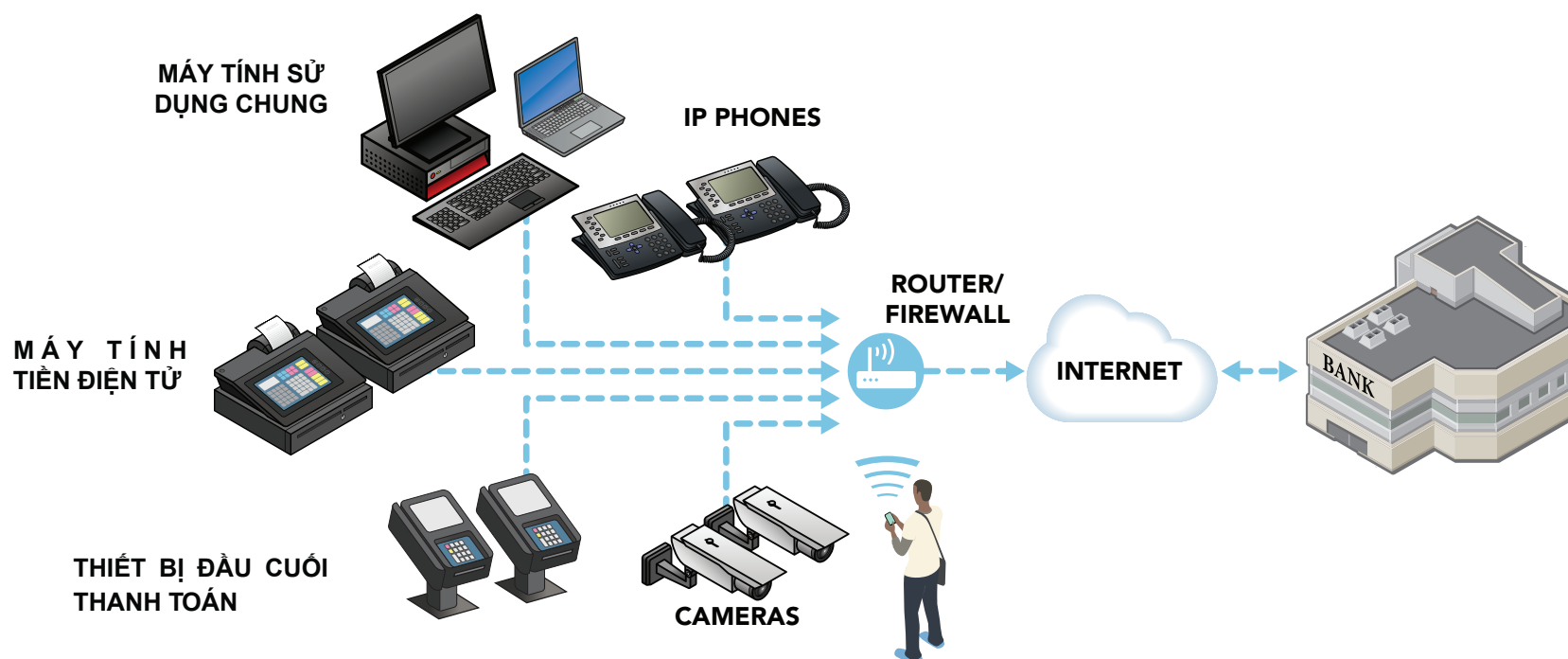
Khiến cho dữ liệu thẻ trở nên vô dụng với tội phạm



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Định kỳ rà soát lỗ hổng an ninh



Merchant TMĐT với trang thanh toán hoàn toàn thuê ngoài. Dữ liệu truyền qua Internet bởi bên cung cấp thứ ba.



TYPE 10 OVERVIEW

TYPE 10 RISKS

TYPE 10 THREATS

TYPE 10 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.

Toàn bộ trang thanh toán của merchant sẽ được thuê ngoài thông qua bên thứ 3 đã đạt tiêu chuẩn PCI DSS

Merchant quản lý website nhưng không có quyền truy cập trang thanh toán.

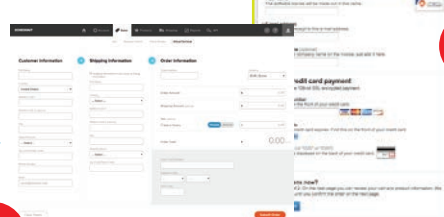
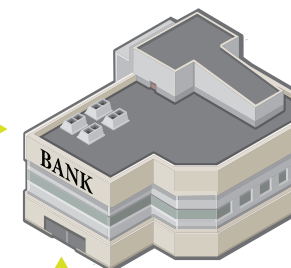
Merchant chỉ có thông tin sản phẩm (trang shopping) và không có quyền và khả năng kiểm soát dữ liệu thẻ.

WEBSITE TMĐT CỦA MERCHANT

TRANG SHOPPING CỦA MERCHANT

TRANG THANH TOÁN CỦA BÊN THỨ 3

WEBSITE CỦA BÊN THỨ 3



Khách hàng duyệt trang shopping của merchant

Khách hàng nhập dữ liệu thẻ vào trang thanh toán của bên thứ 3

INTERNET

ROUTER/FIREWALL

Trang shopping có thể được phân phối bởi chính merchant hoặc nhà cung cấp dịch vụ hosting của merchant.

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

TYPE 10 Merchant TMĐT với trang thanh toán hoàn toàn thuê ngoài. Dữ liệu truyền qua Internet bởi bên cung cấp thứ ba.

RISK PROFILE



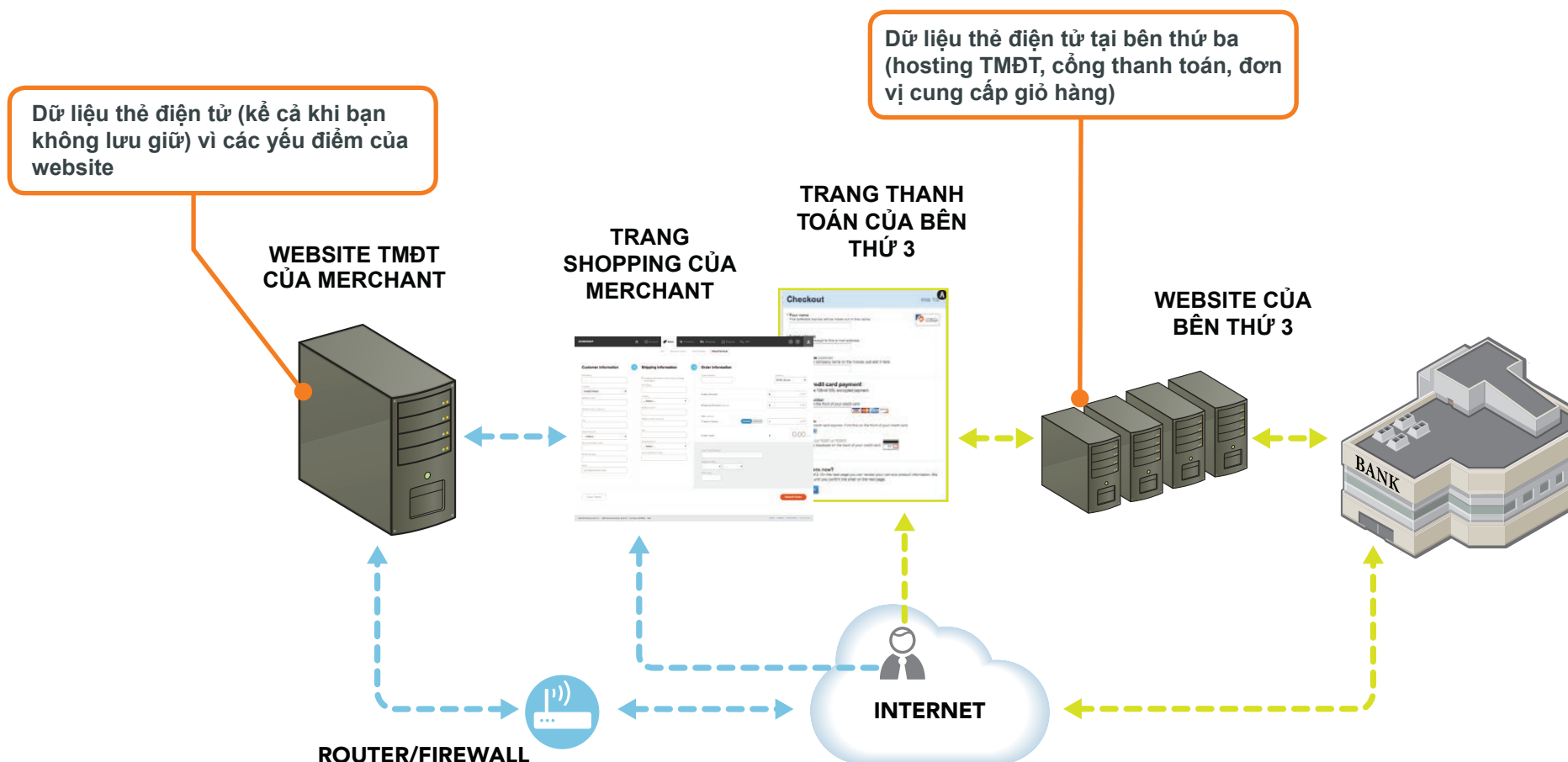
TYPE 10 OVERVIEW

TYPE 10 RISKS

TYPE 10 THREATS

TYPE 10 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?



Tội phạm chiếm dữ liệu thẻ như thế nào?

Chúng xâm nhập vào website của bạn thông qua các lỗ hổng bảo mật và sau đó chặn bắt dữ liệu thẻ khi khách hàng gửi đến trang thanh toán của nhà cung cấp

Chúng có thể đánh cắp dữ liệu thẻ từ nhà cung cấp sử dụng một loạt các biện pháp như cài mã độc, hay các phần mềm bị lỗi cấu hình)

WEBSITE TMĐT CỦA MERCHANT

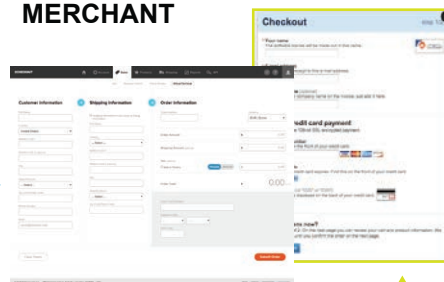
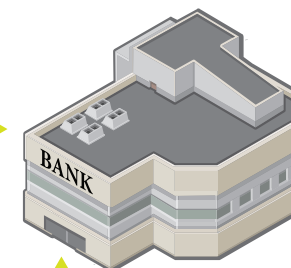
TRANG SHOPPING CỦA MERCHANT

TRANG THANH TOÁN CỦA BÊN THỨ 3

WEBSITE CỦA BÊN THỨ 3

ROUTER/FIREWALL

INTERNET



TYPE 10 Merchant TMĐT với trang thanh toán hoàn toàn thuê ngoài. Dữ liệu truyền qua Internet bởi bên cung cấp thứ ba.

RISK PROFILE



TYPE 10 OVERVIEW

TYPE 10 RISKS

TYPE 10 THREATS

TYPE 10 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



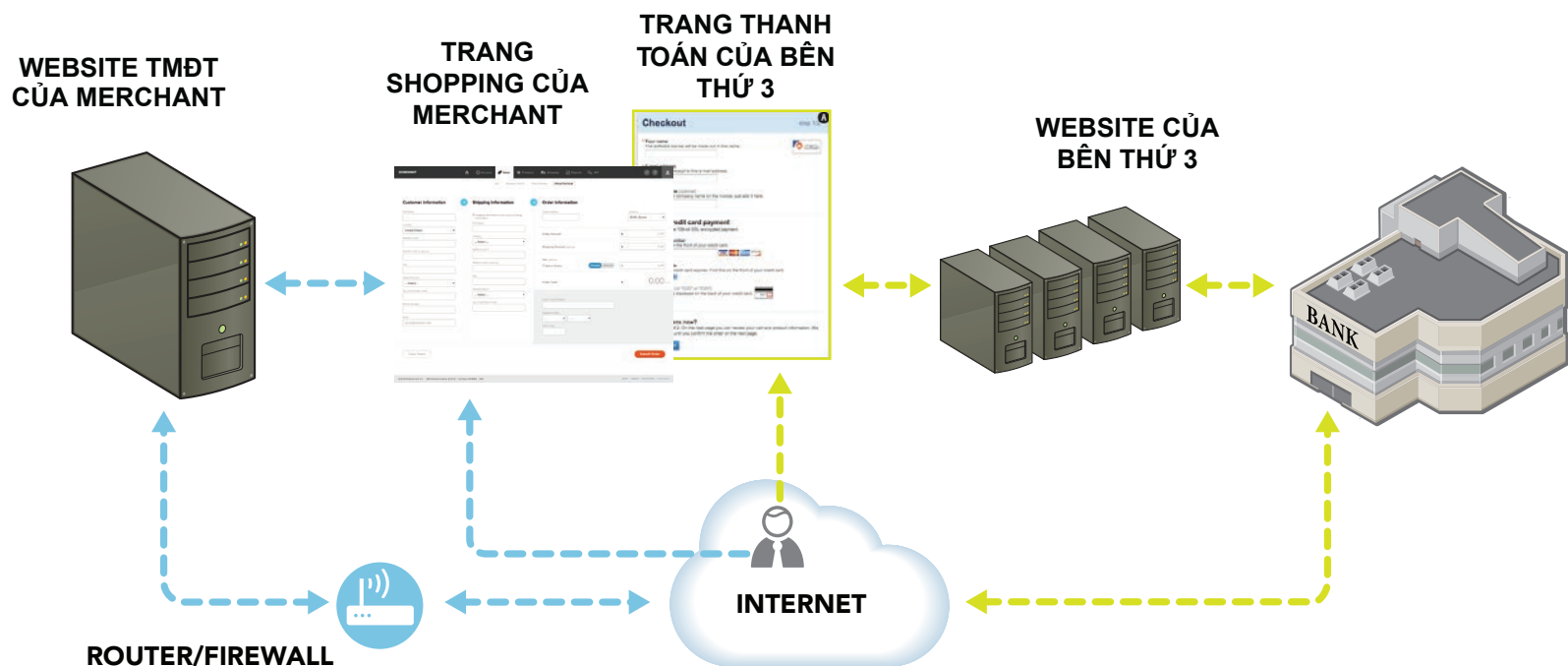
Cài đặt các bản vá từ hãng



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Bảo vệ doanh nghiệp trước mặt trái của Internet



Merchant TMĐT chấp nhận thanh toán trên trang thanh toán của chính mình và tự quản lý website. Dữ liệu truyền qua Internet bởi chính merchant.



TYPE 11 OVERVIEW

TYPE 11 RISKS

TYPE 11 THREATS

TYPE 11 PROTECTIONS

YES

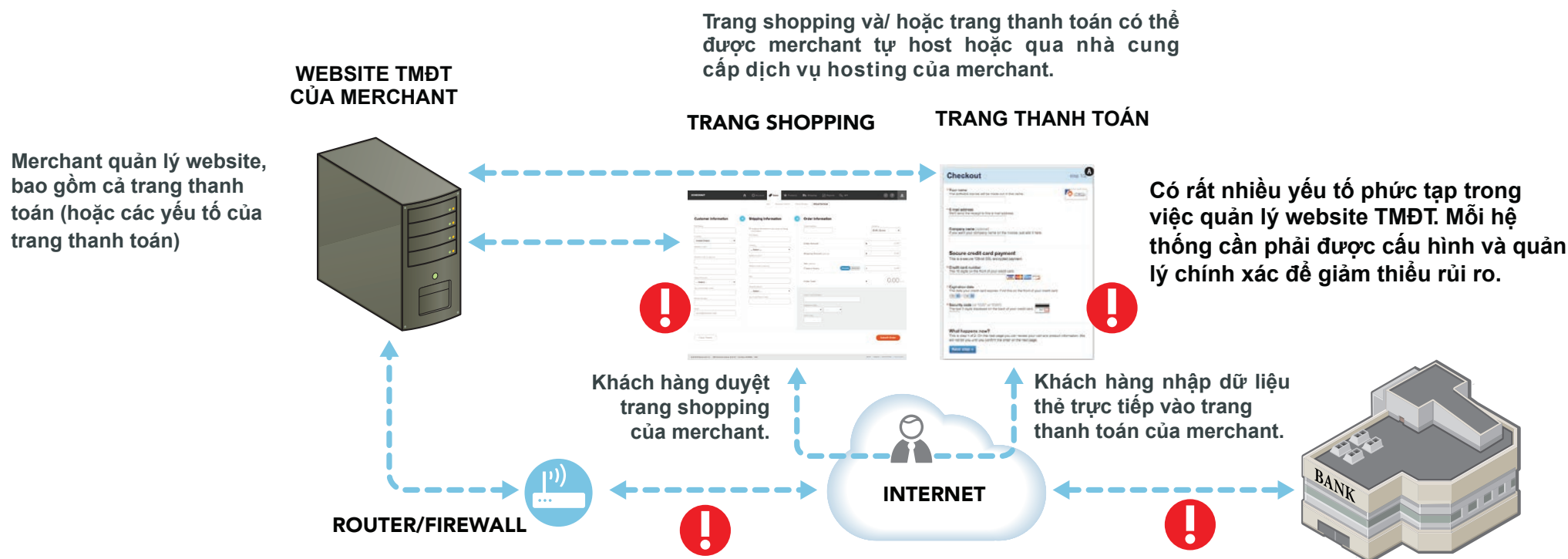
This IS my setup.
Show me the details.

NO

This IS NOT my setup.
Show me the next setup.

BACK

to previous diagram.

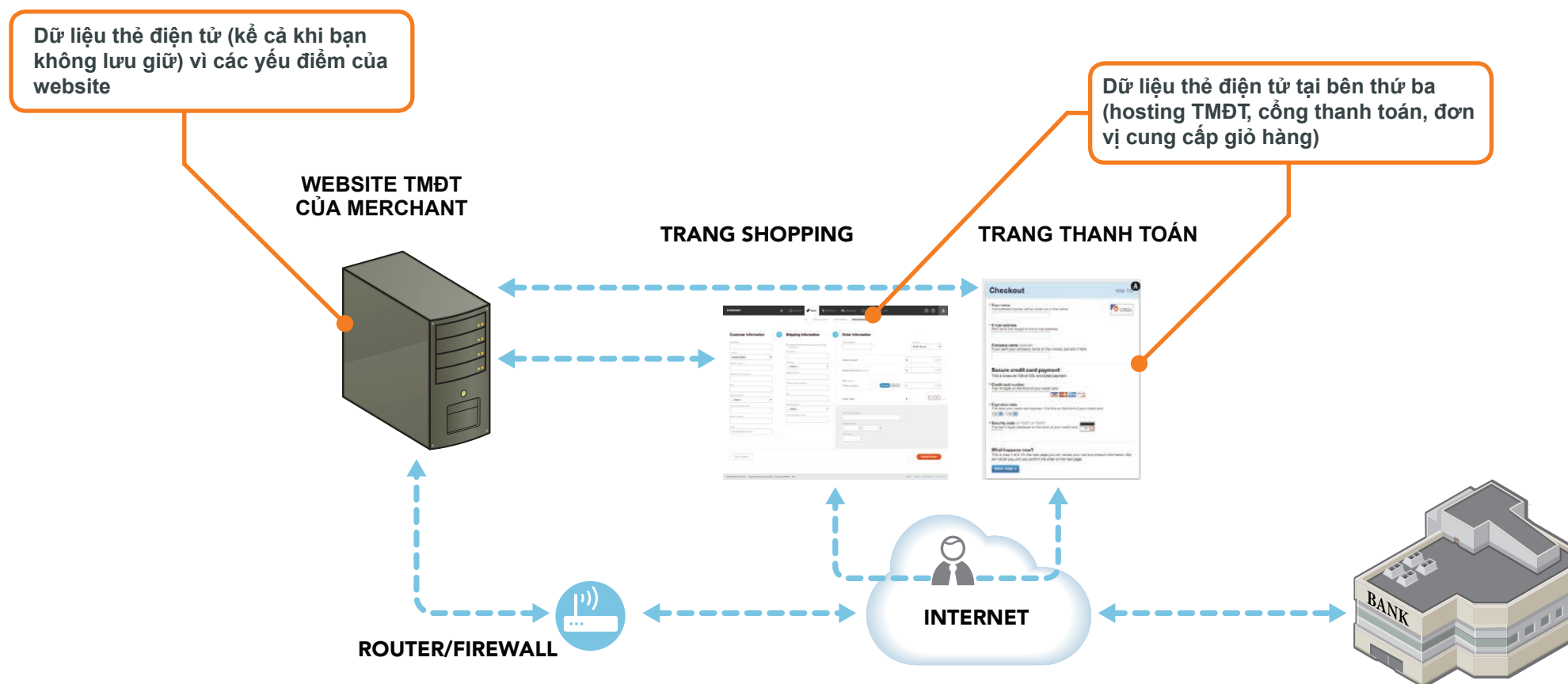


Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Merchant TMĐT chấp nhận thanh toán trên trang thanh toán của chính mình và tự quản lý website. Dữ liệu truyền qua Internet bởi chính merchant.



Rủi ro dữ liệu thẻ nằm ở đâu?



Merchant TMĐT chấp nhận thanh toán trên trang thanh toán của chính mình và tự quản lý website. Dữ liệu truyền qua Internet bởi chính merchant.



Tội phạm chiếm dữ liệu thẻ như thế nào?

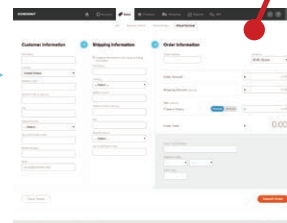
Chúng xâm nhập vào website của bạn thông qua các lỗ hổng bảo mật và sau đó chặn bắt dữ liệu thẻ khi khách hàng gửi đến trang thanh toán của nhà cung cấp

Chúng có thể đánh cắp dữ liệu thẻ từ nhà cung cấp sử dụng một loạt các biện pháp như cài mã độc, hay các phần mềm bị lỗi cấu hình)

WEBSITE TMĐT CỦA MERCHANT

TRANG SHOPPING

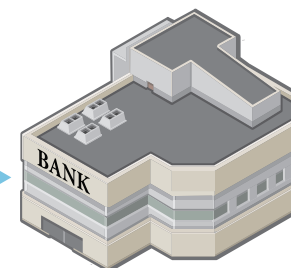
TRANG THANH TOÁN



ROUTER/FIREWALL



INTERNET



Merchant TMĐT chấp nhận thanh toán trên trang thanh toán của chính mình và tự quản lý website. Dữ liệu truyền qua Internet bởi chính merchant.



TYPE 11 OVERVIEW

TYPE 11 RISKS

TYPE 11 THREATS

TYPE 11 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ



Sử dụng thiết bị đầu cuối thanh toán chính hãng



Bảo vệ dữ liệu thẻ và chỉ giữ lại những gì bạn cần



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập



Bảo vệ doanh nghiệp trước mặt trái của Internet



Kiểm tra và giám sát rủi ro, thay đổi đối với thiết bị đầu cuối thanh toán



Sử dụng phần mềm anti-virus



Khiến cho dữ liệu thẻ trở nên vô dụng với tội phạm



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết

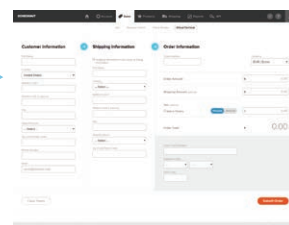


Định kỳ rà soát lỗ hổng an ninh

WEBSITE TMĐT CỦA MERCHANT

TRANG SHOPPING

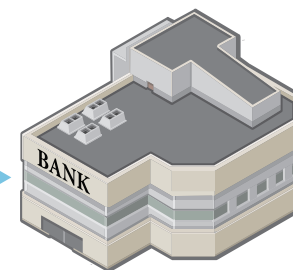
TRANG THANH TOÁN



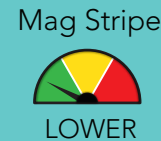
ROUTER/FIREWALL



INTERNET



Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động



TYPE 12 OVERVIEW

TYPE 12 RISKS

TYPE 12 THREATS

TYPE 12 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.

Các thiết bị khác nhau được sử dụng để đọc dữ liệu thẻ từ, nhập số định dạng cá nhân (PIN) và đọc dữ liệu thẻ chip

THIẾT BỊ NHẬP PIN

ĐẦU ĐỌC THẺ AN TOÀN (THIẾT BỊ ĐẦU CÚI THANH TOÁN)

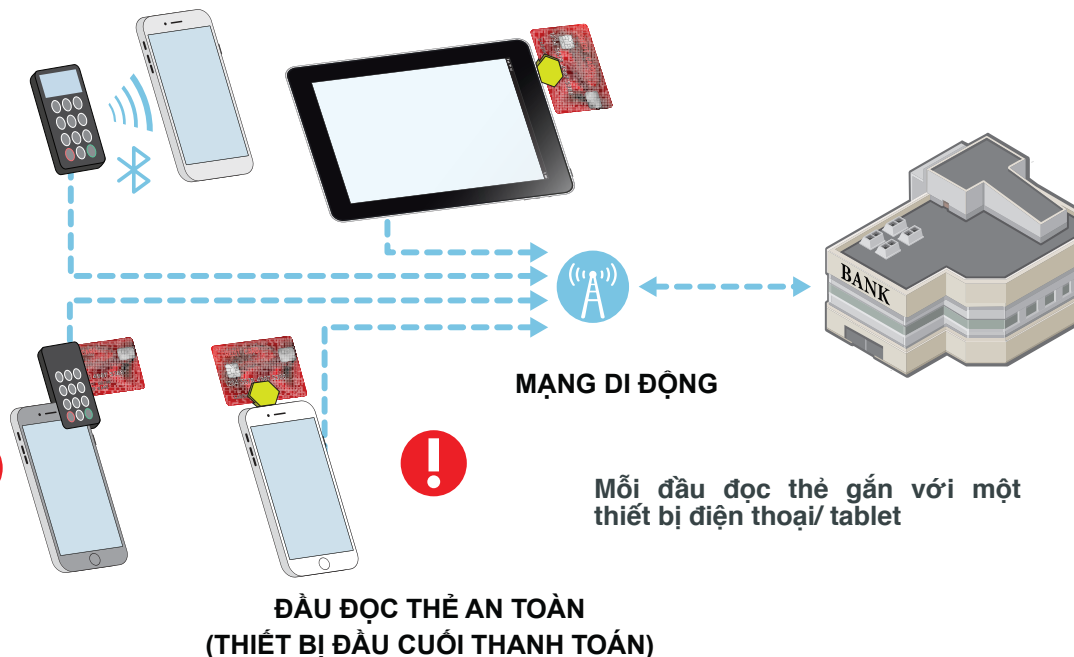
Thiết bị đầu cuối thanh toán di động chỉ kết nối với Internet qua sóng của mạng di động và không sử dụng WiFi.

Dành cho các merchant di động (chợ trời, hội chợ thương mại ...)

Dữ liệu thẻ và mã PIN được mã hoá bởi đầu đọc thẻ và nhập PIN an toàn trước khi gửi đến điện thoại/ tablet; điện thoại/ tablet chỉ nhận được dữ liệu thẻ được mã hoá

Merchant không có khả năng nhập thủ công dữ liệu thẻ

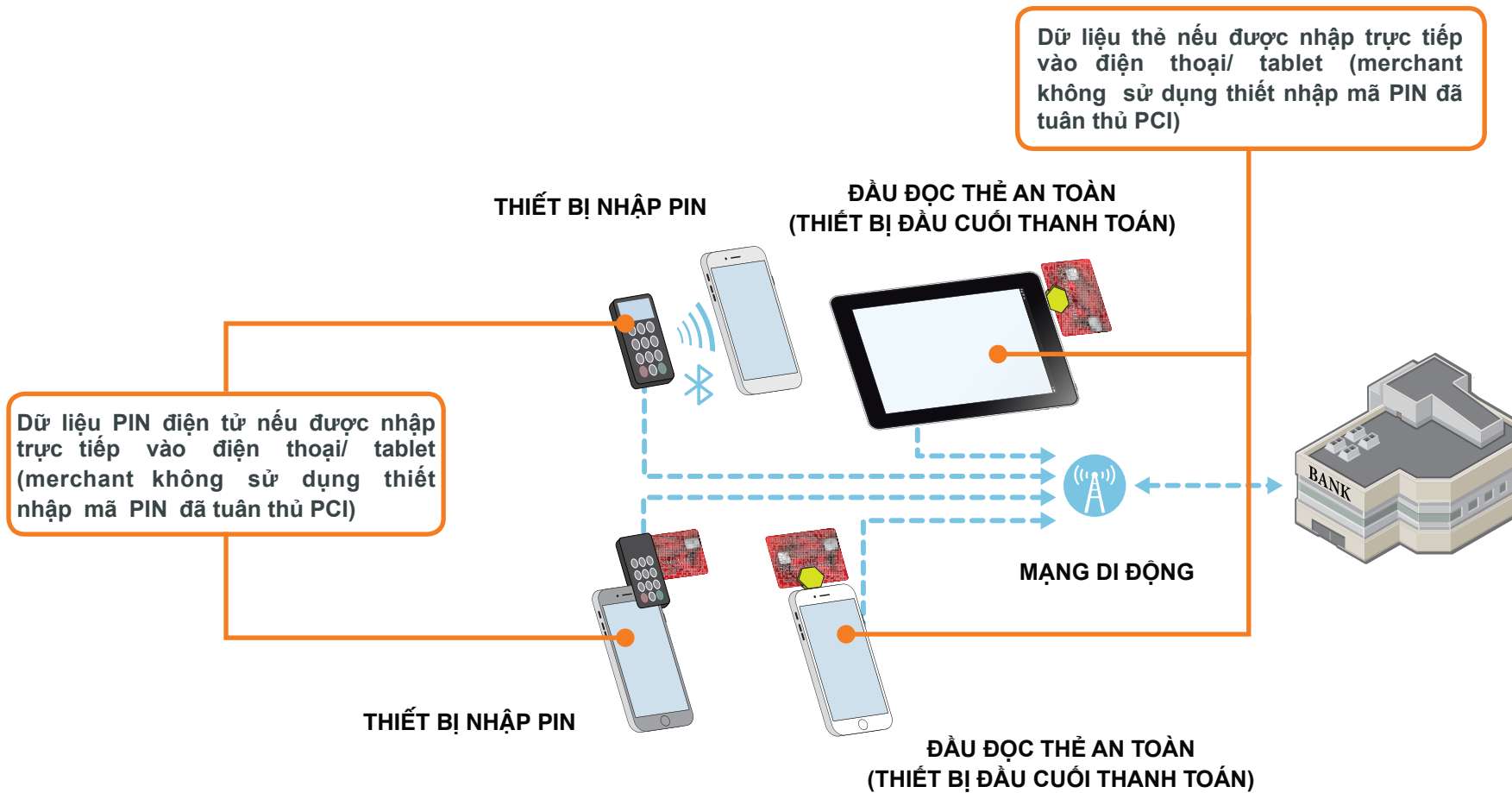
THIẾT BỊ NHẬP PIN



Mỗi đầu đọc thẻ gắn với một thiết bị điện thoại/ tablet

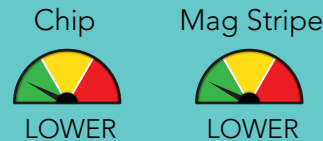
Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Rủi ro dữ liệu thẻ nằm ở đâu?



Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động

RISK PROFILE



TYPE 12 OVERVIEW

TYPE 12 RISKS

TYPE 12 THREATS

TYPE 12 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?

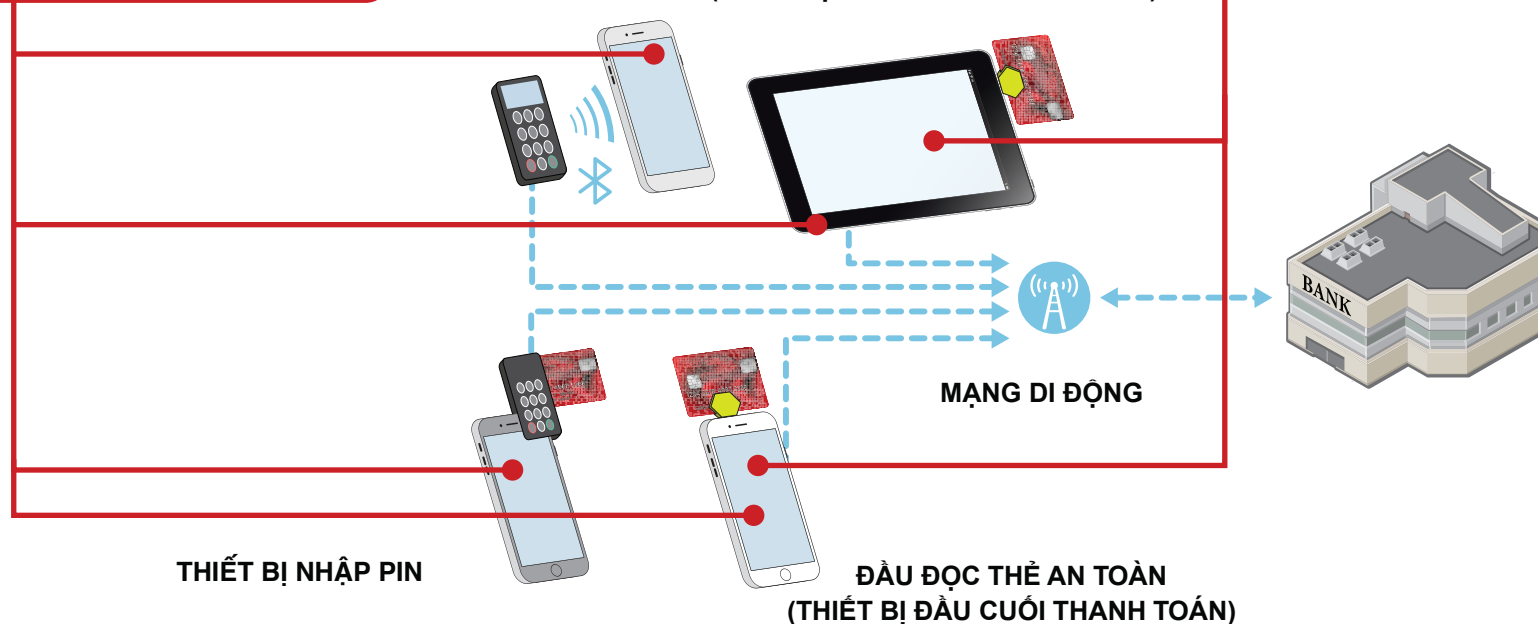
Chúng có thể hack vào phone/ tablet và cài phần mềm mã độc rồi tiến hành đánh cắp dữ liệu thẻ và PIN trên phone/ tablet

Chúng sử dụng các ứng dụng trong “app store” để đánh cắp dữ liệu thẻ và PIN khi bạn download ứng dụng về phone/ tablet của mình

Chúng có thể hoán đổi đầu đọc thẻ có chứa các công nghệ gián điệp

THIẾT BỊ NHẬP PIN

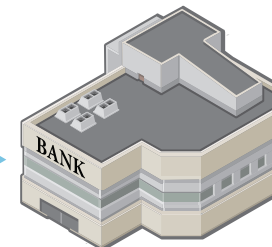
ĐẦU ĐỌC THẺ AN TOÀN
(THIẾT BỊ ĐẦU CUỐI THANH TOÁN)



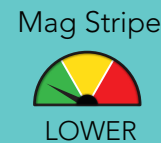
THIẾT BỊ NHẬP PIN

ĐẦU ĐỌC THẺ AN TOÀN
(THIẾT BỊ ĐẦU CUỐI THANH TOÁN)

MẠNG DI ĐỘNG



Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động



TYPE 12 OVERVIEW

TYPE 12 RISKS

TYPE 12 THREATS

TYPE 12 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Kiểm tra và giám sát đầu đọc thẻ và thiết bị nhập PIN nhằm phát hiện rủi ro và thay đổi



Cài đặt các bản vá từ hãng



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



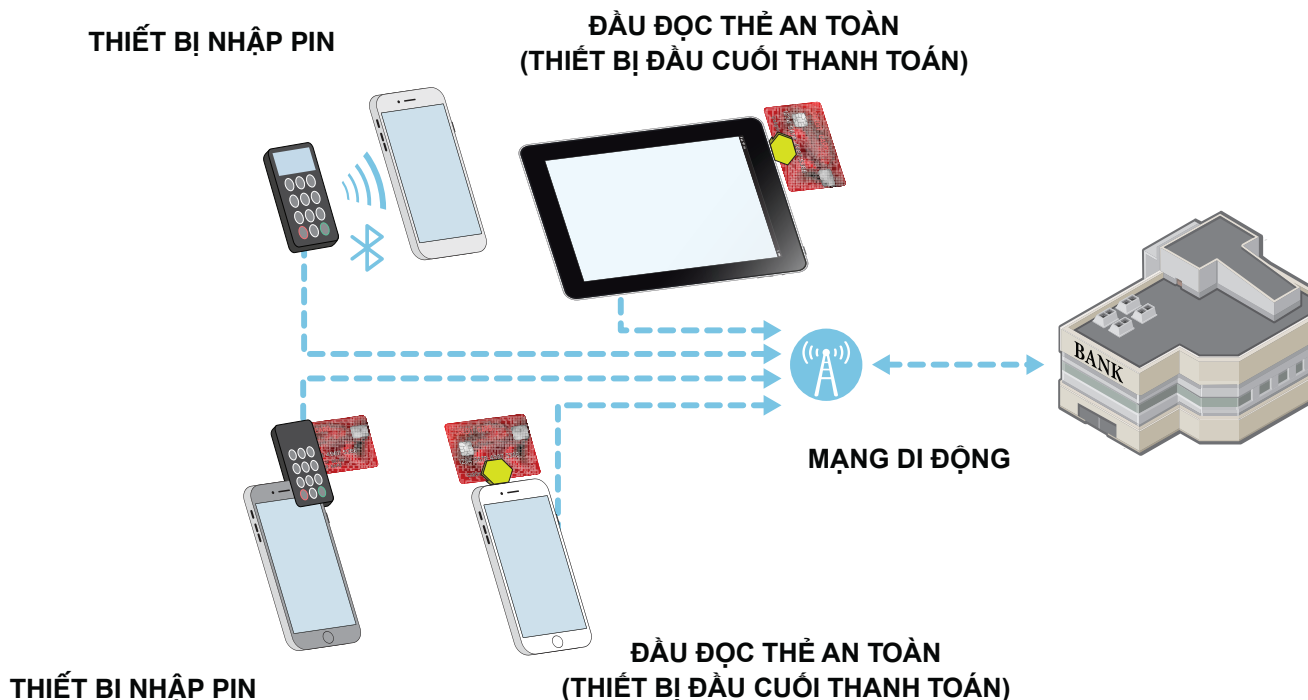
Sử dụng phần mềm anti-virus



Sử dụng đầu đọc thẻ và PIN an toàn



Khiến cho dữ liệu thẻ trở nên vô dụng với tội phạm



Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động hoặc WiFi

TYPE 13 OVERVIEW

TYPE 13 RISKS

TYPE 13 THREATS

TYPE 13 PROTECTIONS

Thiết bị đầu cuối thanh toán di động chỉ kết nối với Internet qua sóng của mạng di động và/ hoặc sử dụng WiFi.

Dành cho các merchant di động (chợ trời, hội chợ thương mại ...)

Dữ liệu thẻ và mã PIN được mã hoá bởi đầu đọc thẻ và nhập PIN an toàn trước khi gửi đến điện thoại/ tablet; điện thoại/ tablet chỉ nhận được dữ liệu thẻ được mã hoá

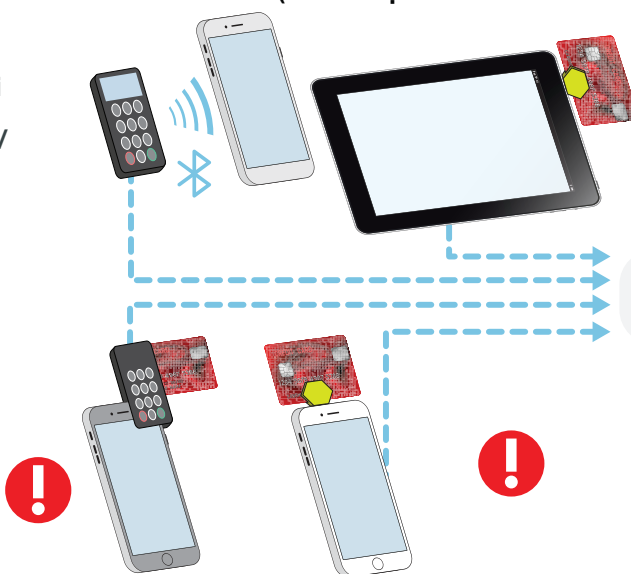
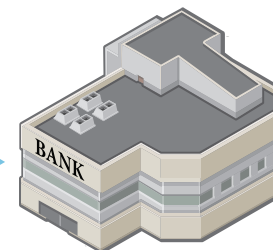
Merchant không có khả năng nhập thủ công dữ liệu thẻ

THIẾT BỊ NHẬP PIN

ĐẦU ĐỌC THẺ AN TOÀN
(THIẾT BỊ ĐẦU CUỐI THANH TOÁN)

Các thiết bị khác nhau được sử dụng để đọc dữ liệu thẻ từ, nhập số định dạng cá nhân (PIN) và đọc dữ liệu thẻ chip

MẠNG DI ĐỘNG
HOẶC WIFI



THIẾT BỊ NHẬP PIN

ĐẦU ĐỌC THẺ AN TOÀN
(THIẾT BỊ ĐẦU CUỐI THANH TOÁN)

Mỗi đầu đọc thẻ gắn với một thiết bị điện thoại/ tablet

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu
Rủi ro được mô tả ở trang sau

YES

This IS my setup.
Show me the details.

NO

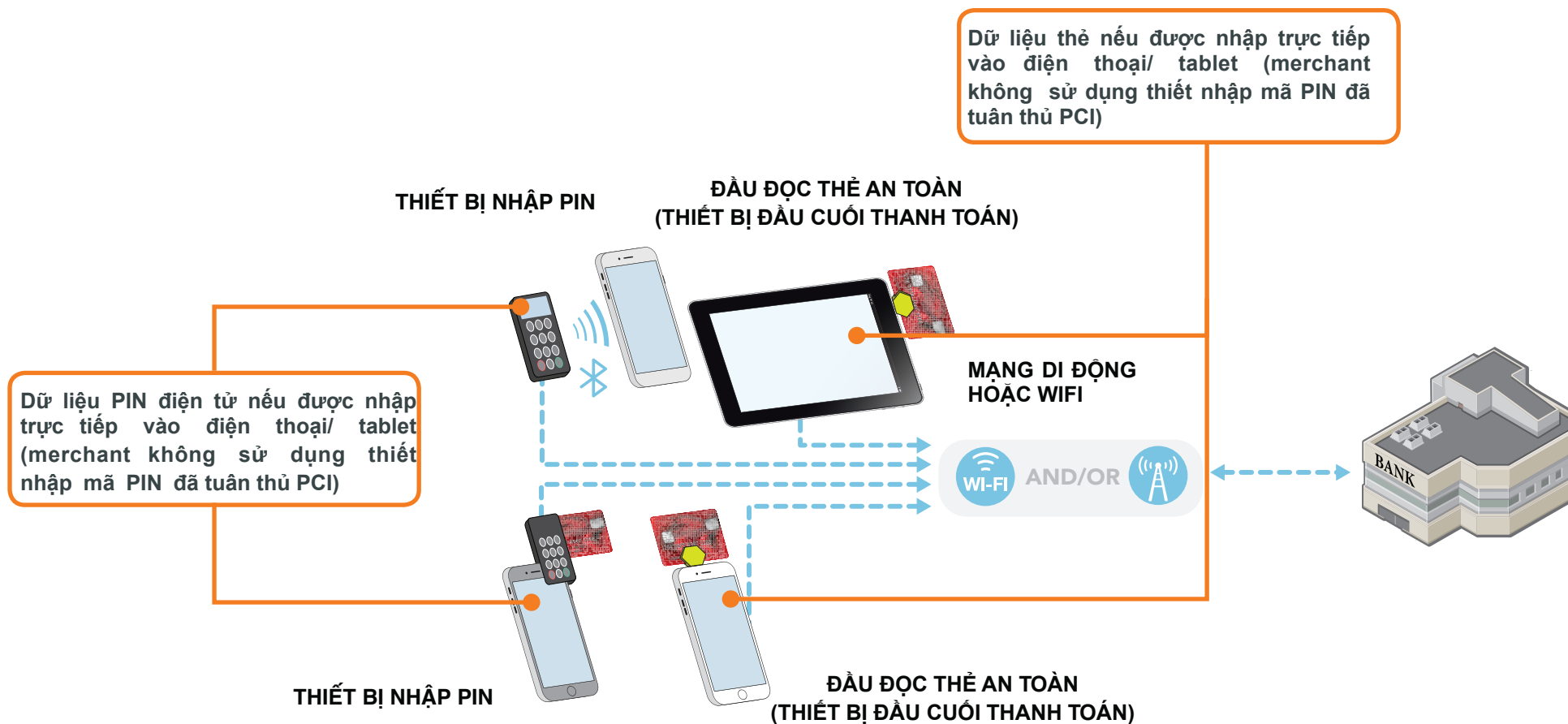
This IS NOT my setup.
Show me the next setup.

BACK

to previous diagram.

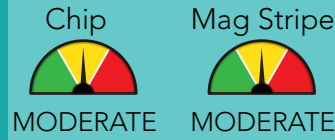
Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động hoặc WiFi

Rủi ro dữ liệu thẻ nằm ở đâu?



TYPE 13 Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động hoặc WiFi

RISK PROFILE



TYPE 13 OVERVIEW

TYPE 13 RISKS

TYPE 13 THREATS

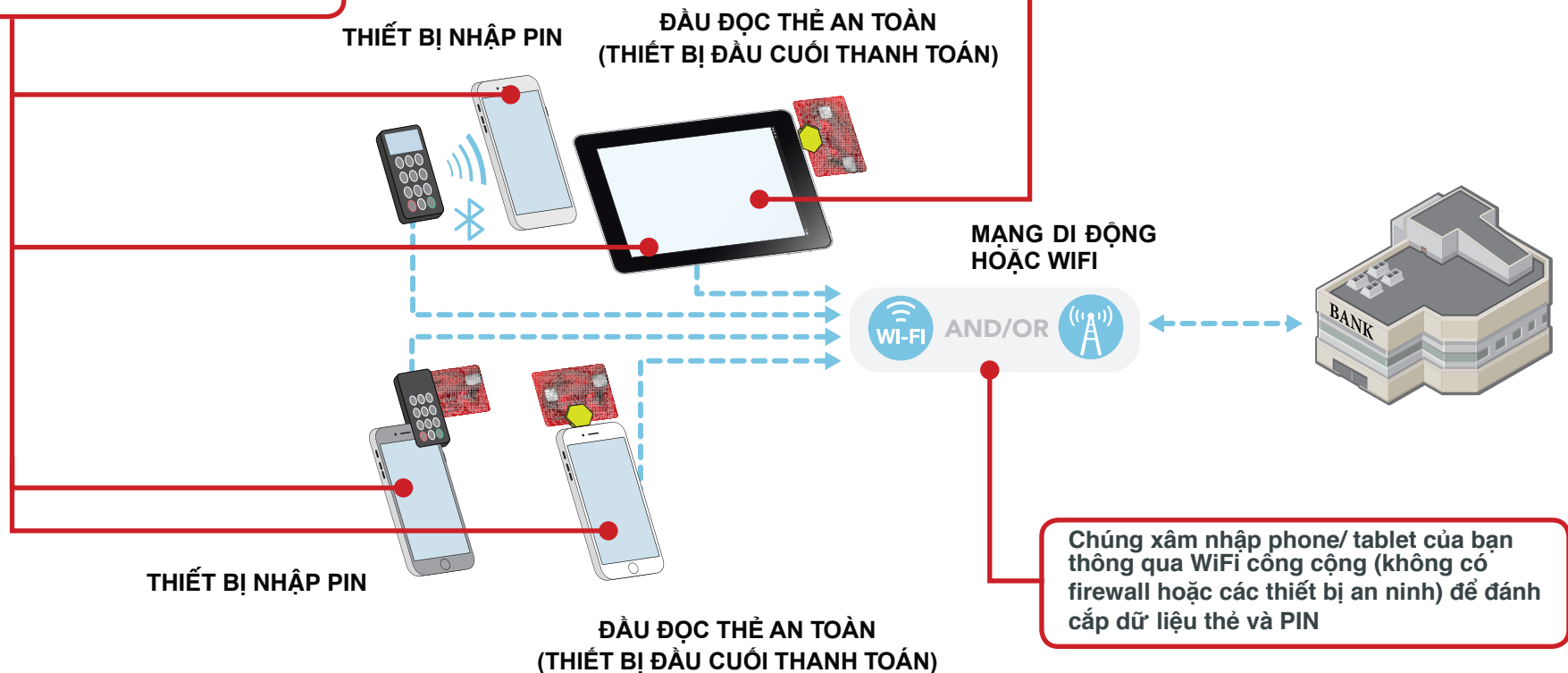
TYPE 13 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?

Chúng có thể hack vào phone/ tablet và gài phần mềm mã độc rồi tiến hành đánh cắp dữ liệu thẻ và PIN trên phone/ tablet

Chúng sử dụng các ứng dụng trong “app store” để đánh cắp dữ liệu thẻ và PIN khi bạn download ứng dụng về phone/ tablet của mình

Chúng có thể hoán đổi đầu đọc thẻ cổ chứa các công nghệ gián điệp



Chúng xâm nhập phone/ tablet của bạn thông qua WiFi công cộng (không có firewall hoặc các thiết bị an ninh) để đánh cắp dữ liệu thẻ và PIN

Đầu đọc thẻ được mã hoá an toàn và thiết bị đầu cuối thanh toán di động. Dữ liệu chỉ truyền qua sóng di động hoặc WiFi

TYPE 13 OVERVIEW

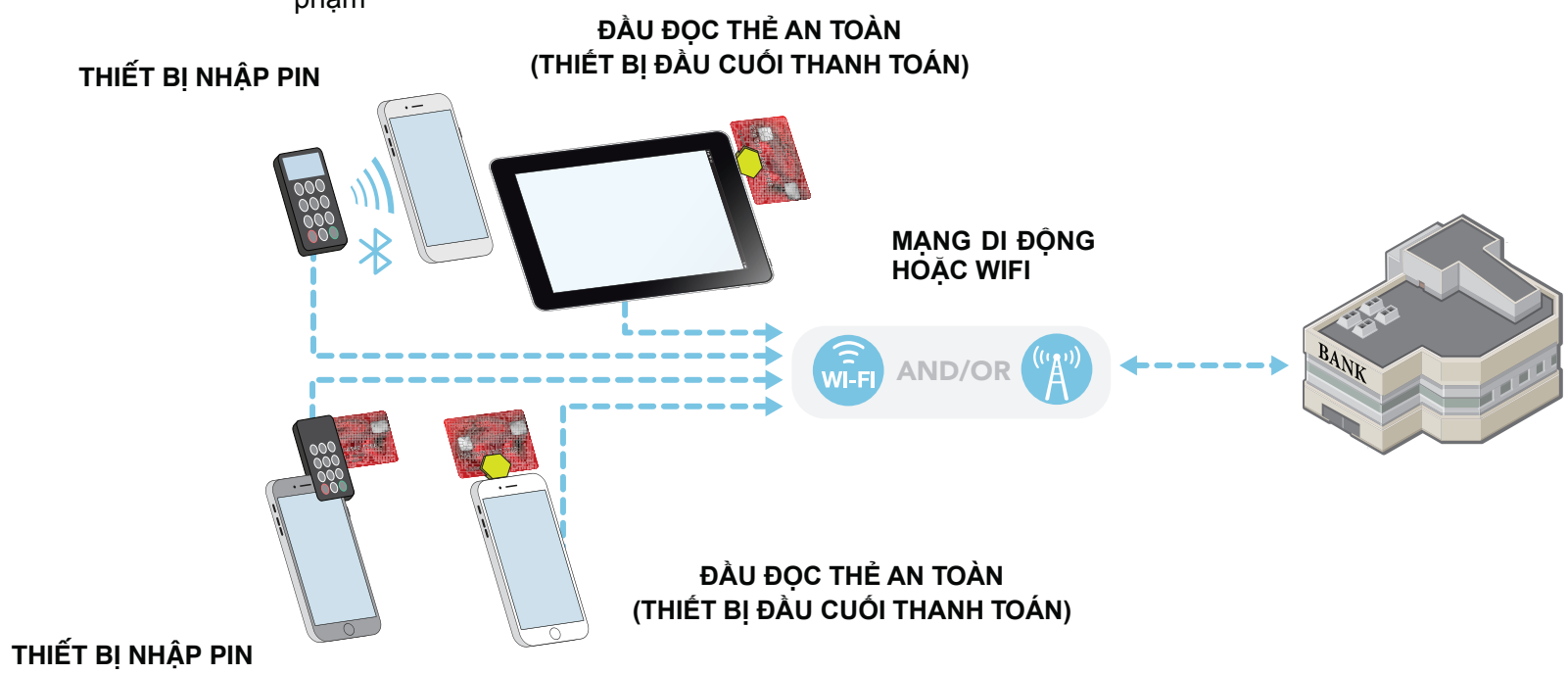
TYPE 13 RISKS

TYPE 13 THREATS

TYPE 13 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?

- | | | | | | | | |
|--|---|--|--|--|----------------------------|--|------------------------------------|
| | Dùng mật khẩu mạnh | | Kiểm tra và giám sát đầu đọc thẻ và thiết bị bị nhập PIN nhằm phát hiện rủi ro và thay đổi | | Cài đặt các bản vá từ hãng | | Sử dụng phần mềm anti-virus |
| | Bảo vệ quyền truy cập nội bộ vào dữ liệu thẻ | | Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập | | Giữ dữ liệu thẻ an toàn | | Sử dụng đầu đọc thẻ và PIN an toàn |
| | Bảo vệ doanh nghiệp trước mặt trái của Internet | | Khiến cho dữ liệu thẻ trở nên vô dụng với tội phạm | | | | |





Thiết bị đầu cuối thanh toán ảo được truy cập qua Internet browser của merchant. Dữ liệu thanh toán truyền qua Internet

TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

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.

Lưu ý rủi ro sẽ lớn hơn nếu thanh toán qua thiết bị di động được chấp nhận và dữ liệu được truyền qua WiFi, vì khi đó tin tặc có thể tấn công đánh cắp dữ liệu thẻ do mạng thiếu công cụ bảo mật.

MÁY TÍNH CỦA
MERCHANT



Một “thiết bị đầu cuối” ảo là một trang web mà merchant có quyền truy cập bằng máy tính hoặc tablet.

Merchant nhập thủ công dữ liệu thẻ vào thiết bị đầu cuối ảo qua màn hình trình duyệt

Dành cho các merchant không có thiết bị đầu cuối thanh toán truyền thống. Họ thường nhập thủ công từng giao dịch. Khối lượng giao dịch thanh toán thường không nhiều (ví dụ các shop online tại

Không có đầu đọc card hoặc thiết bị đầu cuối thanh toán kết nối với mạng hay thiết bị của merchant.

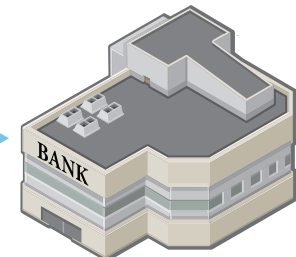


MERCHANT
PHONE/TABLET

THIẾT BỊ ĐẦU CUỐI ẢO TỪ CÔNG
THANH TOÁN/ NGÂN HÀNG ĐÃ ĐẠT
TUÂN THỦ PCI DSS



Ngân hàng/ Công thanh toán thứ 3 cung cấp dịch vụ thanh toán ảo.



INTERNET

ROUTER/
FIREWALL

Theo kịch bản này, các rủi ro dữ liệu thẻ ở các dấu ! Rủi ro được mô tả ở trang sau

Thiết bị đầu cuối thanh toán ảo được truy cập qua Internet browser của merchant. Dữ liệu thanh toán truyền qua Internet

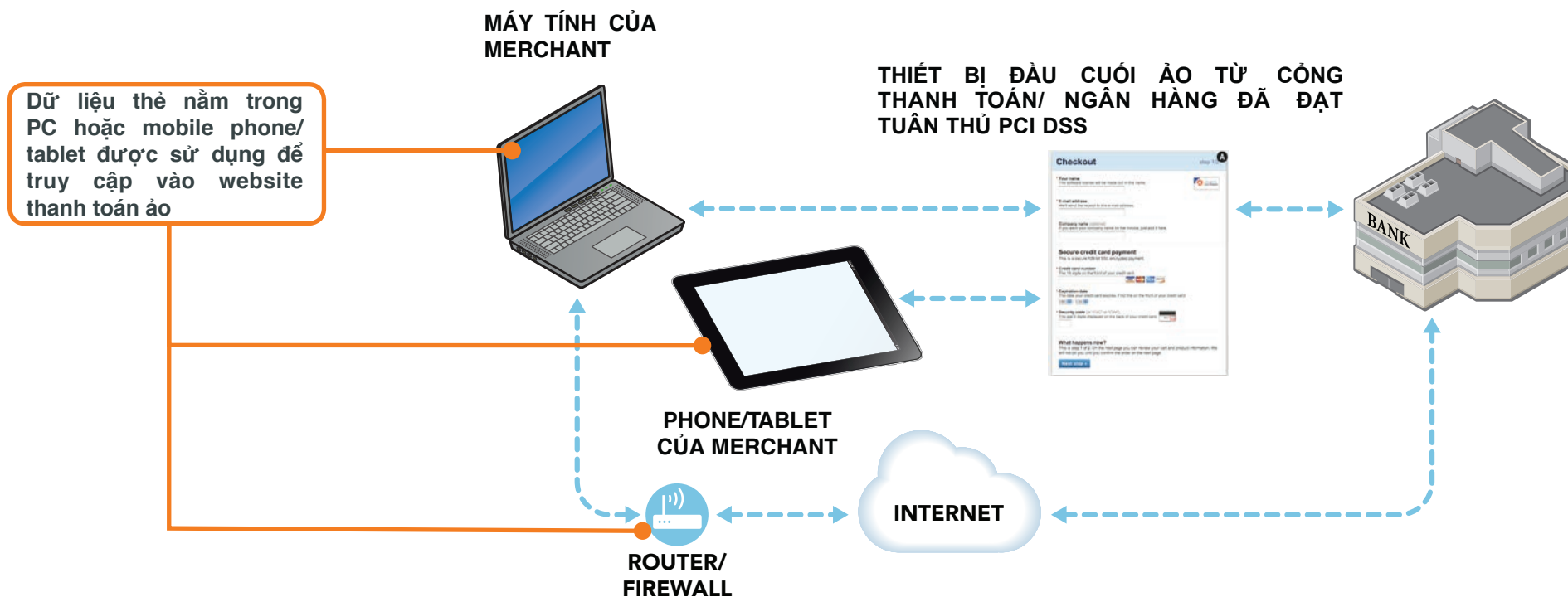
TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

Rủi ro dữ liệu thẻ nằm ở đâu?



Thiết bị đầu cuối thanh toán ảo được truy cập qua Internet browser của merchant. Dữ liệu thanh toán truyền qua Internet

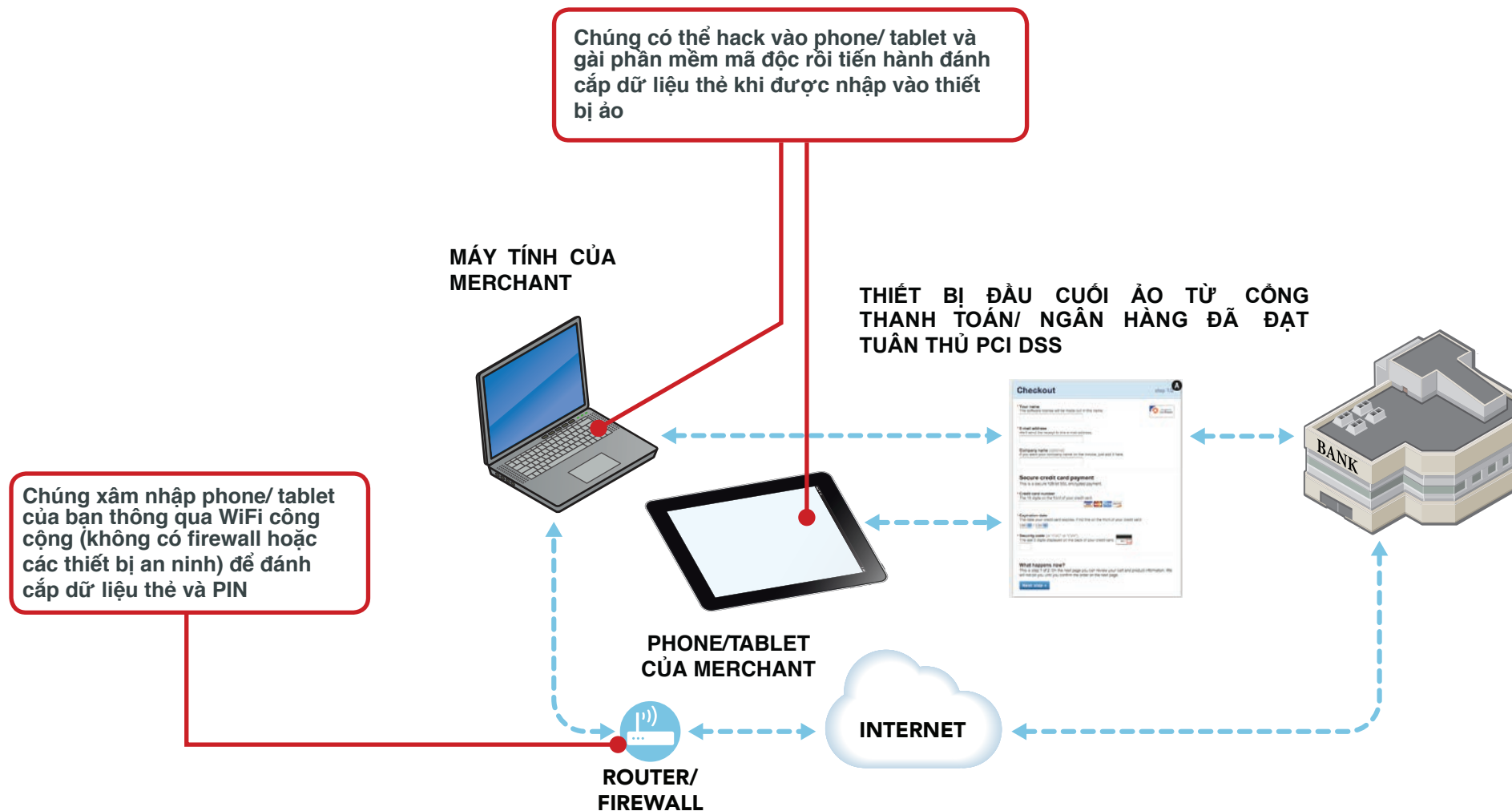
TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

Tội phạm chiếm dữ liệu thẻ như thế nào?



Thiết bị đầu cuối thanh toán ảo được truy cập qua Internet browser của merchant. Dữ liệu thanh toán truyền qua Internet

TYPE 14 OVERVIEW

TYPE 14 RISKS

TYPE 14 THREATS

TYPE 14 PROTECTIONS

Bạn cần làm gì để bảo mật dữ liệu thẻ?



Dùng mật khẩu mạnh



Cài đặt các bản vá từ hãng



Yêu cầu nhà cung cấp hỗ trợ khi cần thiết



Hạn chế truy cập từ xa của nhà cung cấp - đừng để hacker dễ dàng xâm nhập



Sử dụng phần mềm anti-virus



Định kỳ rà soát lỗ hổng an ninh



Dùng firewall (hoặc phần mềm firewall cá nhân nếu sử dụng WiFi công cộng)

MÁY TÍNH CỦA MERCHANT

THIẾT BỊ ĐẦU CUỐI ẢO TỪ CÔNG THANH TOÁN/ NGÂN HÀNG ĐÃ ĐẠT TUÂN THỦ PCI DSS

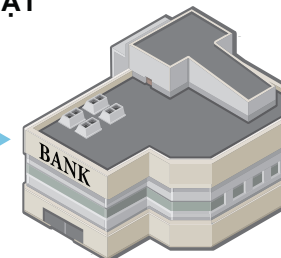


PHONE/TABLET CỦA MERCHANT



ROUTER/FIREWALL

INTERNET



Tài nguyên

Thư viện PCI cho merchant nhỏ

Tài nguyên	Link	URL
Hướng dẫn thanh toán an toàn	<i>Guide to Safe Payments</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Bộ câu hỏi merchant hỏi nhà cung cấp	<i>Small Merchant Questions for Vendors</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Thuật ngữ	<i>Small Merchant Glossary</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf