The Payment Data That Criminals Want

John Elliott

Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire

Have You Ever Wondered …

Criminal + **Data** = **Cash**

Criminal Aims

This is the Card

I am the Customer

An Issuer Wants To

Validate the Card

Validate the Cardholder

Two Types of Authentication

Validate the Card

Hologram

Is it a “real” card?

Validate the Cardholder

Signature

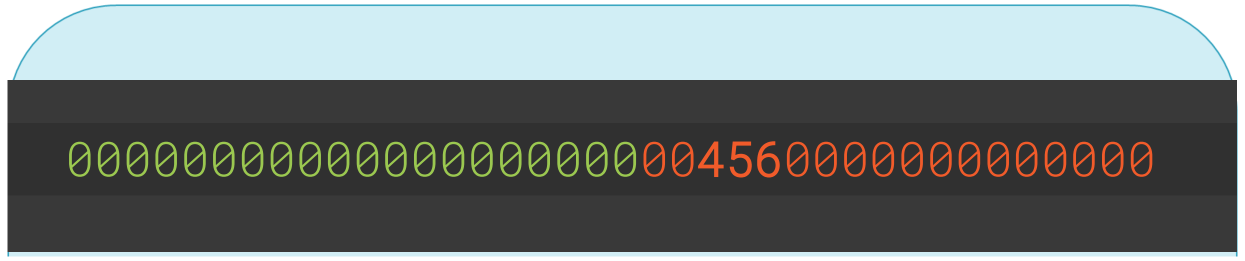
Does it match?

AUTHORIZED SIGNATURE
NOT VALID UNLESS SIGNED
Ann Cardholder
7890 654

Two Types of Authentication

Validate the Card

Hologram
Is it a "real" card?



Magnetic Stripe
Data correct?
CVV correct?

Validate the Cardholder

Signature
Does it match?

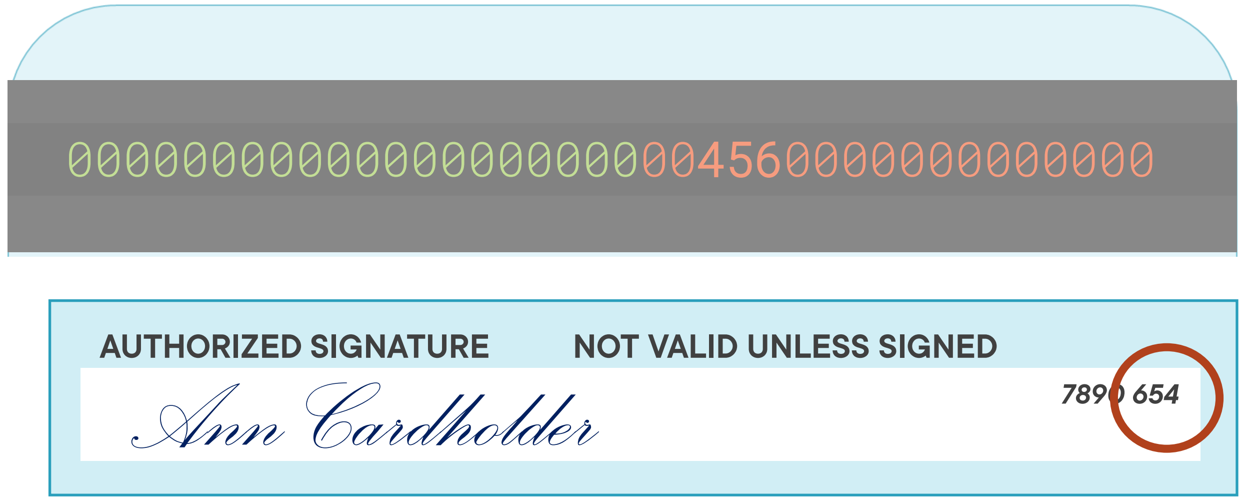
Personal Identification Number (PIN)
Does it match?

****

Two Types of Authentication

Validate the Card

Hologram
Is it a “real” card?



Magnetic Stripe
Data correct?
CVV correct?

CVV2 correct?

Validate the Cardholder

Signature
Does it match?

Personal Identification Number (PIN)
Does it match?

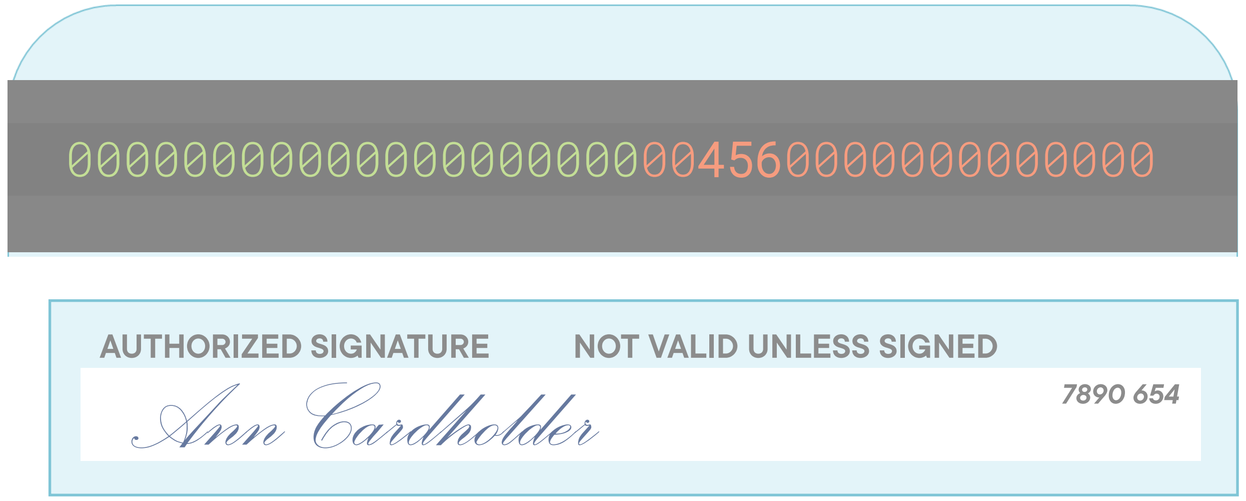
****

Address Verification
Does it match?

Two Types of Authentication

Validate the Card

Hologram
Is it a “real” card?



Magnetic Stripe
Data correct?
CVV correct?

CVV2 correct?

Chip
iCVV correct?
Correct secret?

Validate the Cardholder

Signature
Does it match?

Personal Identification Number (PIN)
Does it match?

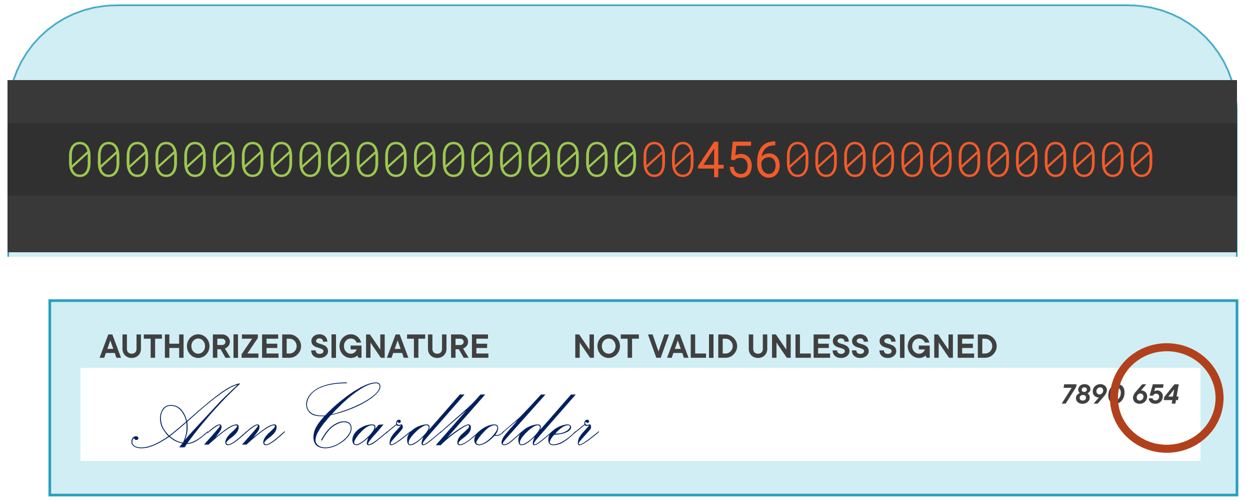
****

Address Verification
Does it match?

Biometric
Does it match?

What Criminals Want

Create a Fake Card



Magnetic Stripe
Data correct?
CVV correct?

CVV2 correct?

Impersonate the Cardholder

Personal Identification Number (PIN)
Does it match?

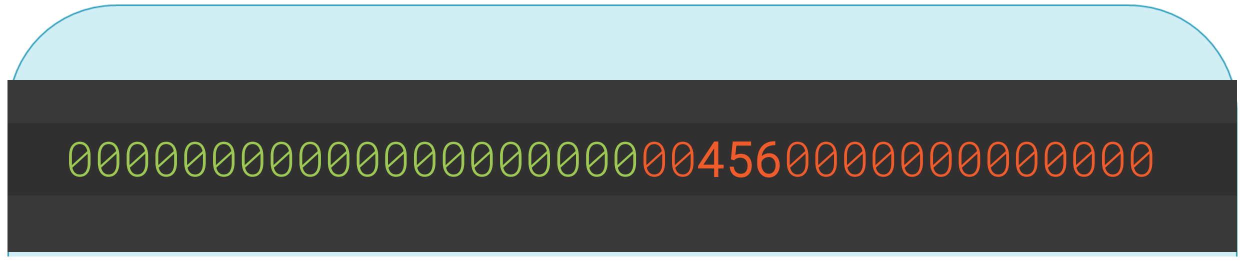
****

What Criminals Want

Create a Fake Card

Hologram

Is it a “real” card?



Magnetic Stripe

Data correct?

CVV correct?

AUTHORIZED SIGNATURE
NOT VALID UNLESS SIGNED
Ann Cardholder
7890 654

CVV2 correct?

Impersonate the Cardholder

Signature

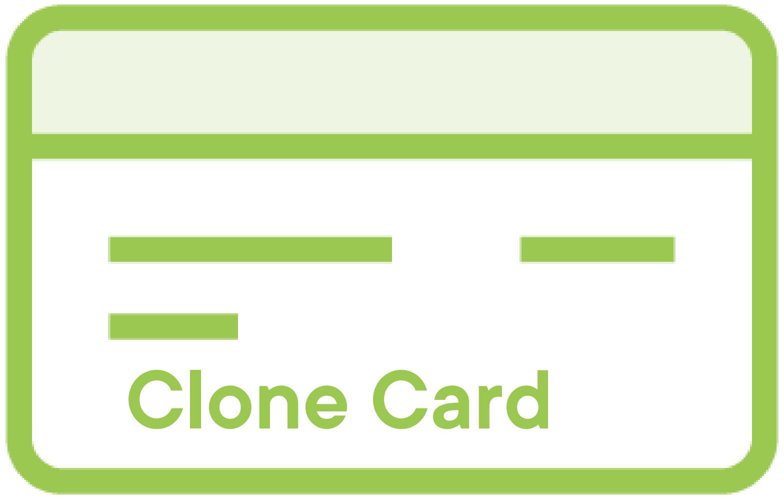
Does it match?

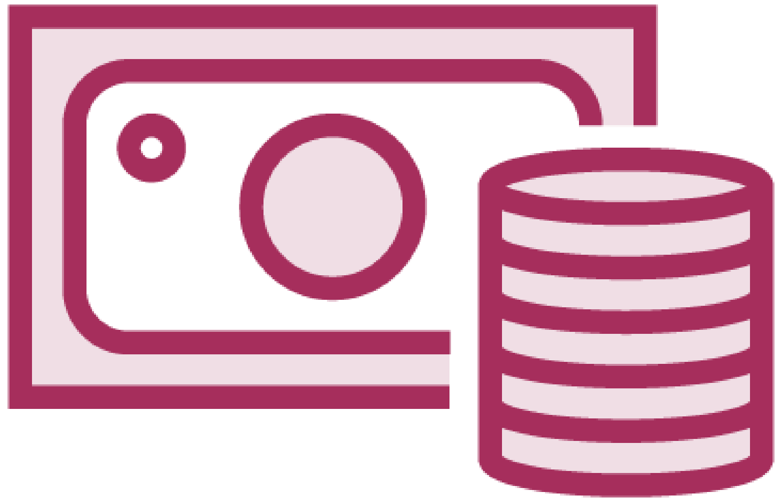
Personal Identification Number (PIN)

Does it match?

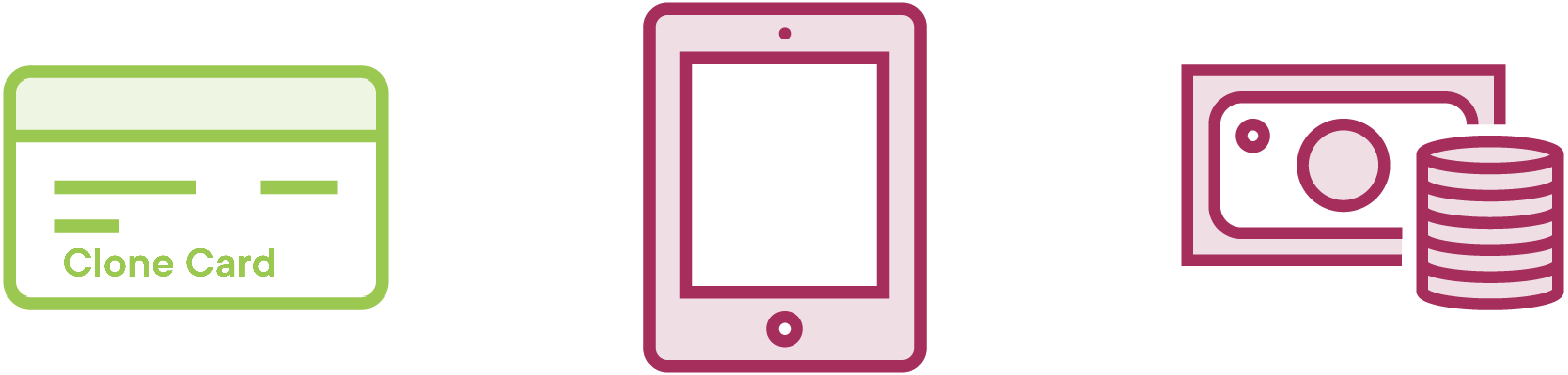
****

Card to Cash

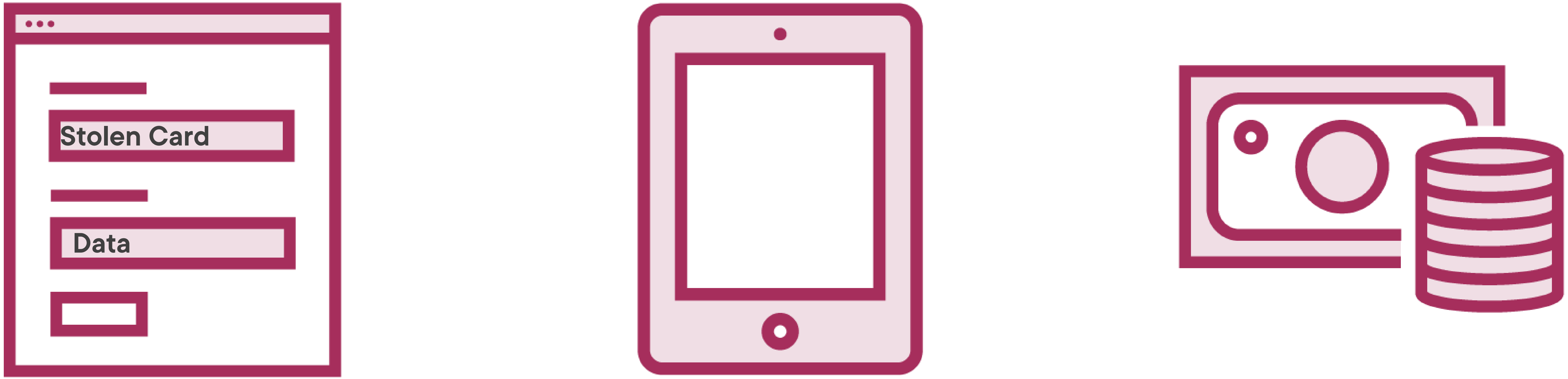




Card to Cash

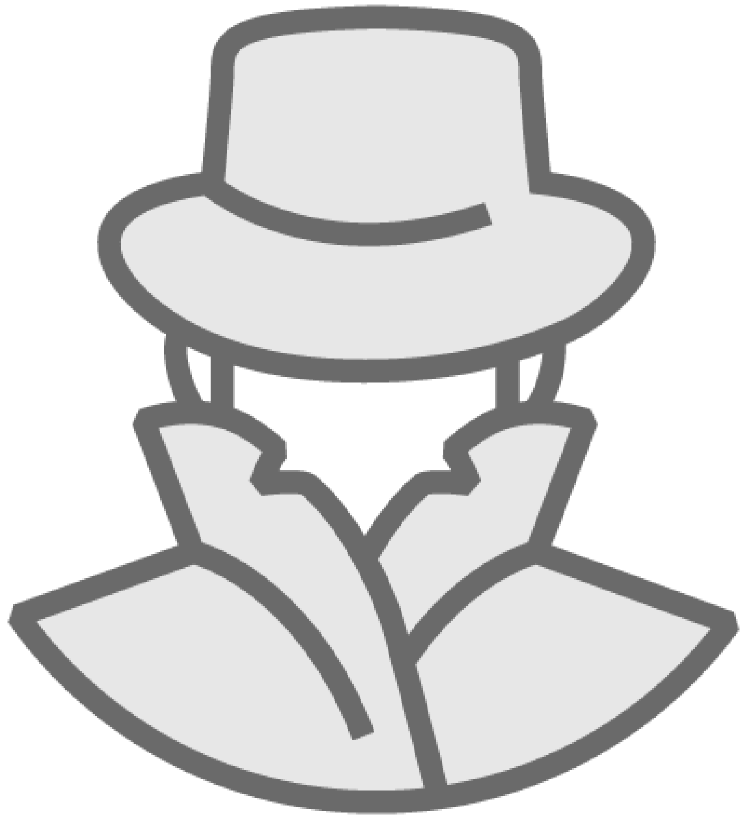


Card to Cash



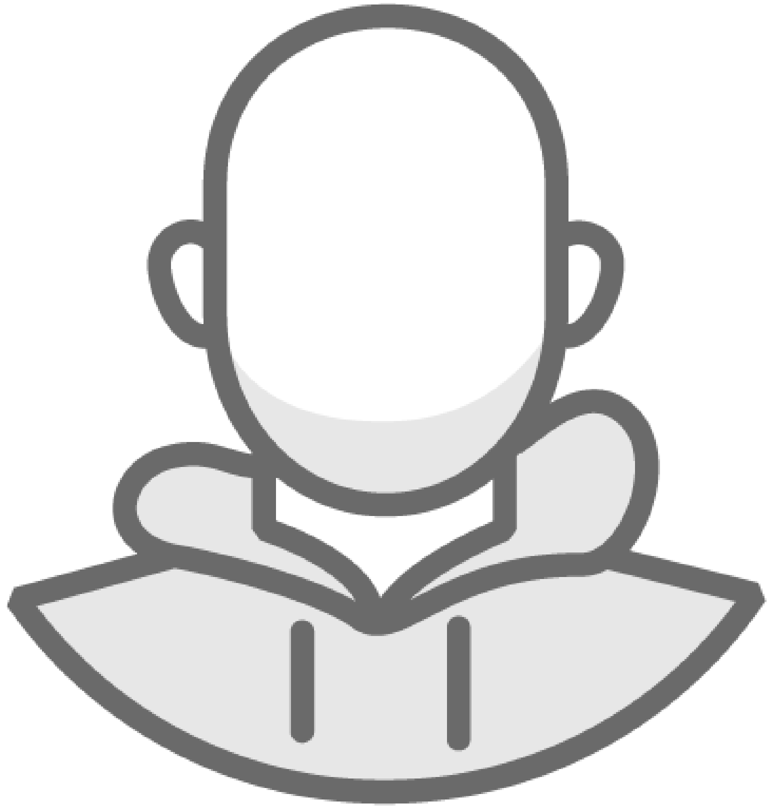
Criminal Value Chain

1



2

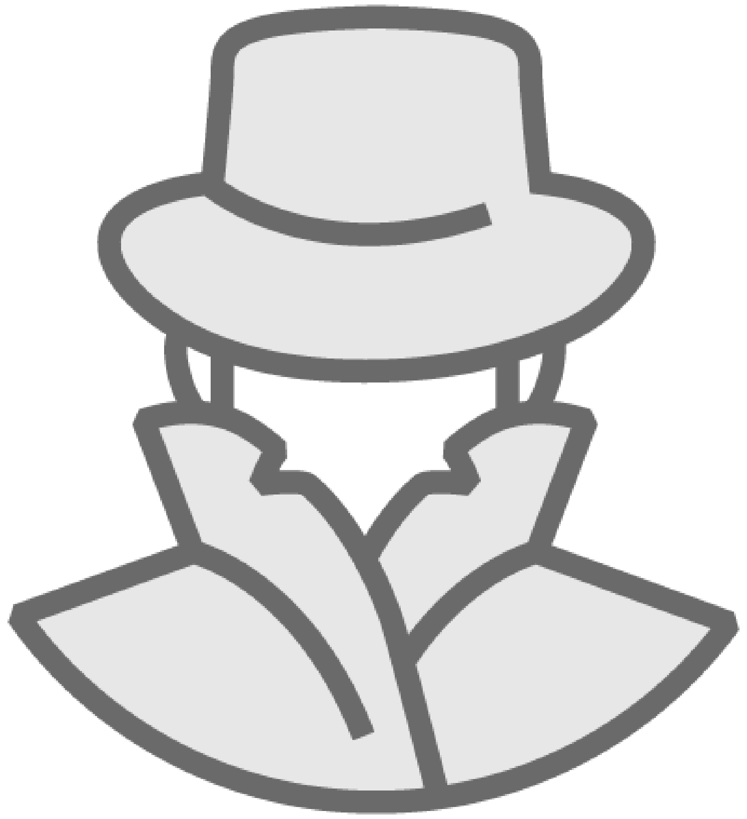
3



4

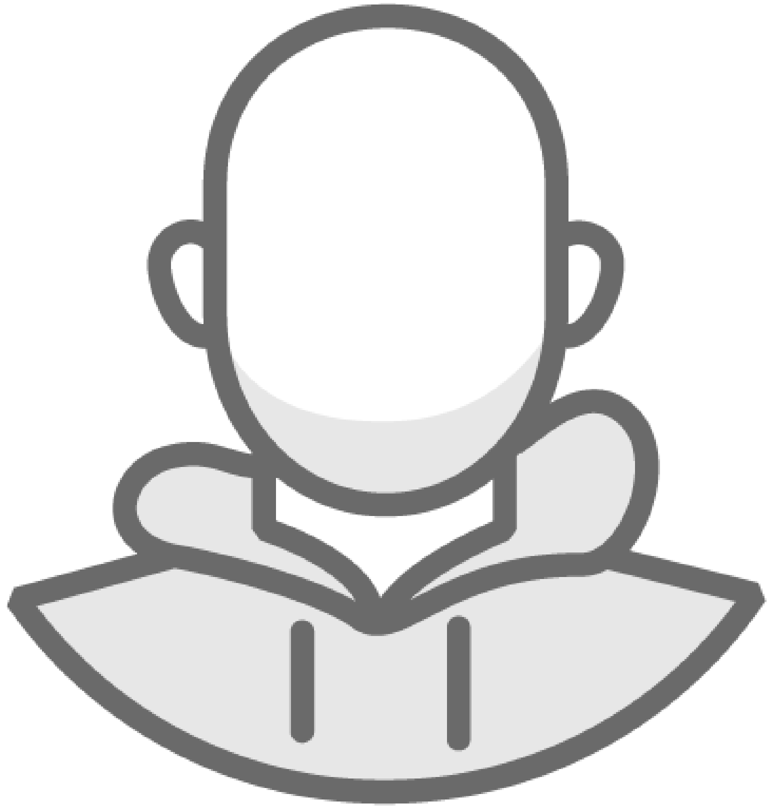
Criminal Value Chain

1. Steal the Data



2

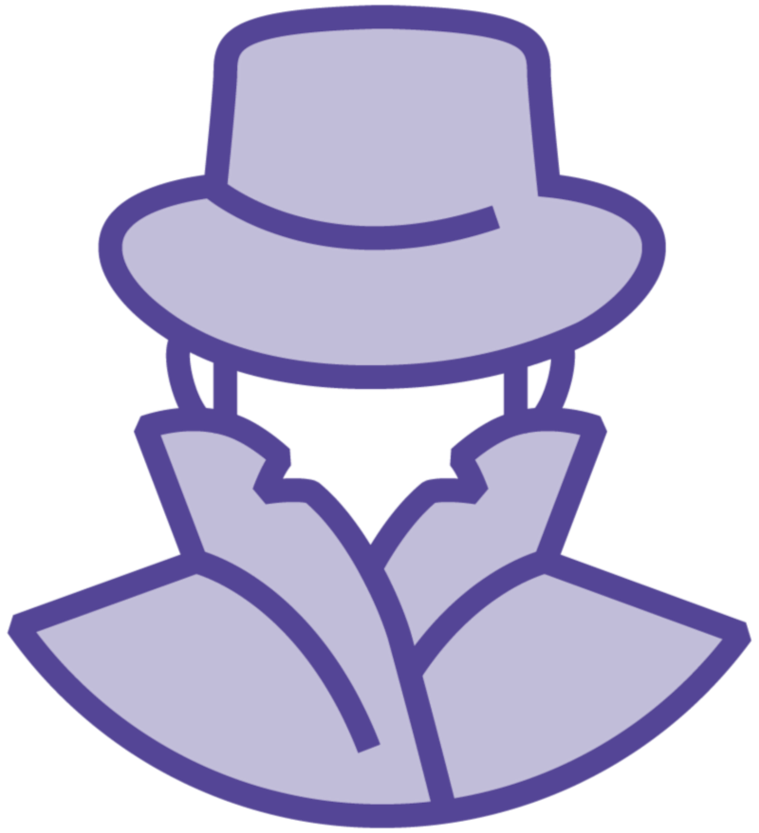
3



4

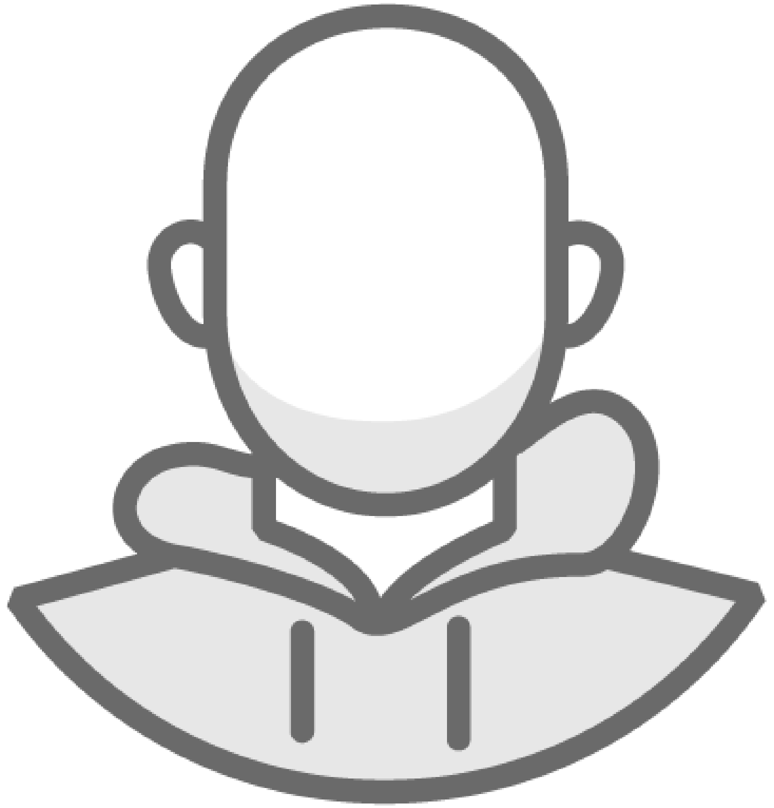
Criminal Value Chain

1. Steal the Data



2. Sell the Data

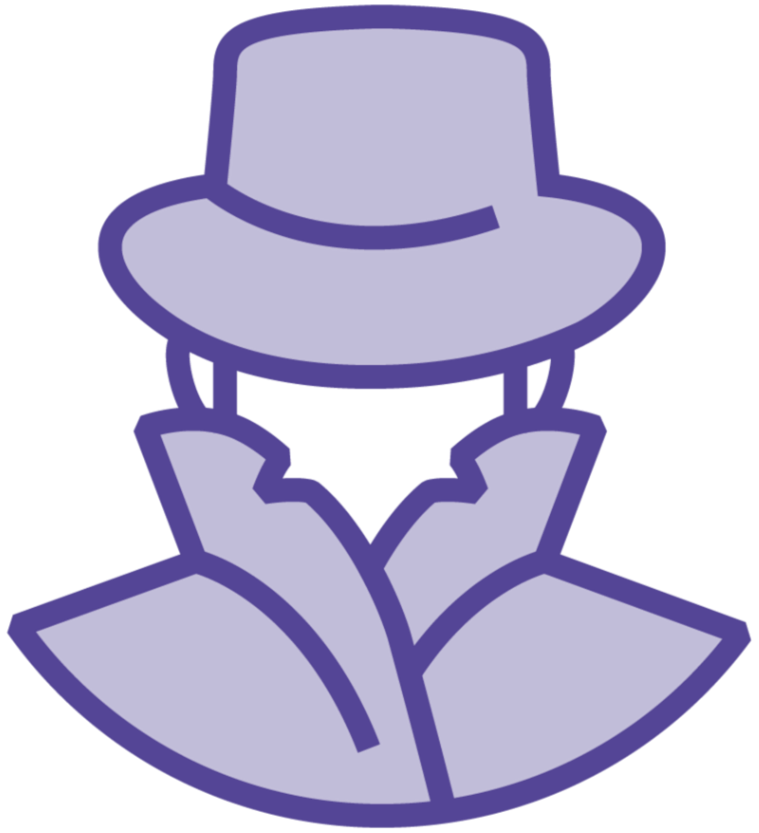
3



4

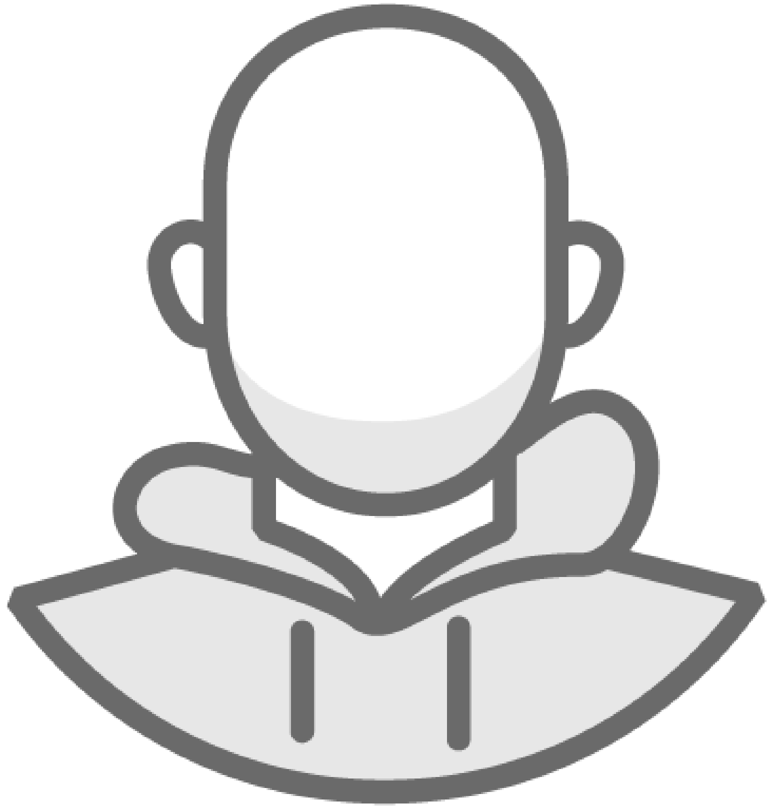
Criminal Value Chain

1. Steal the Data



2. Sell the Data

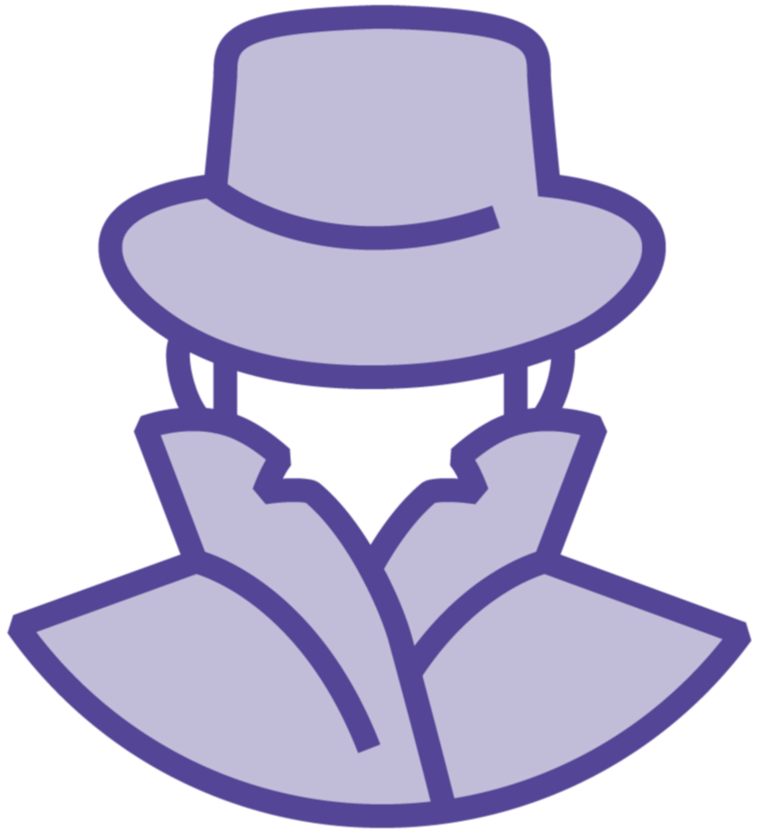
3. Monetize the Data



4

Criminal Value Chain

1. Steal the Data



2. Sell the Data

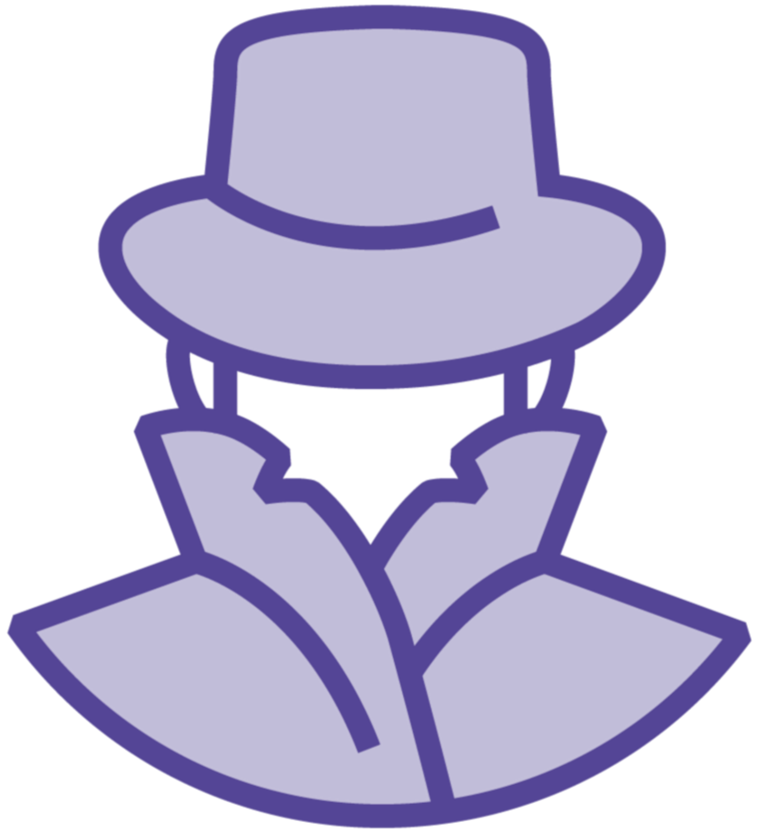
3. Monetize the Data

4. Mule:

Money or Goods

Criminal Value Chain

1. Steal the Data

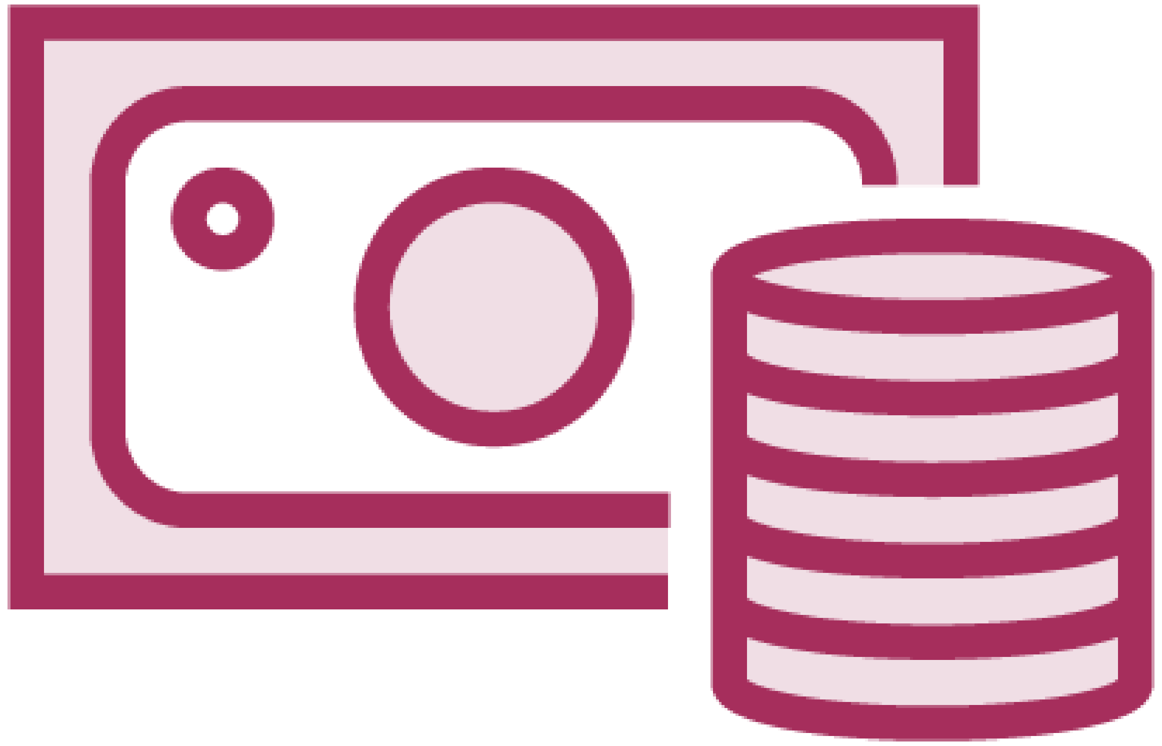


2. Sell the Data

3. Monetize the Data

4. Mule:

Money or Goods



This should only work if the ATM is not able to read a chip

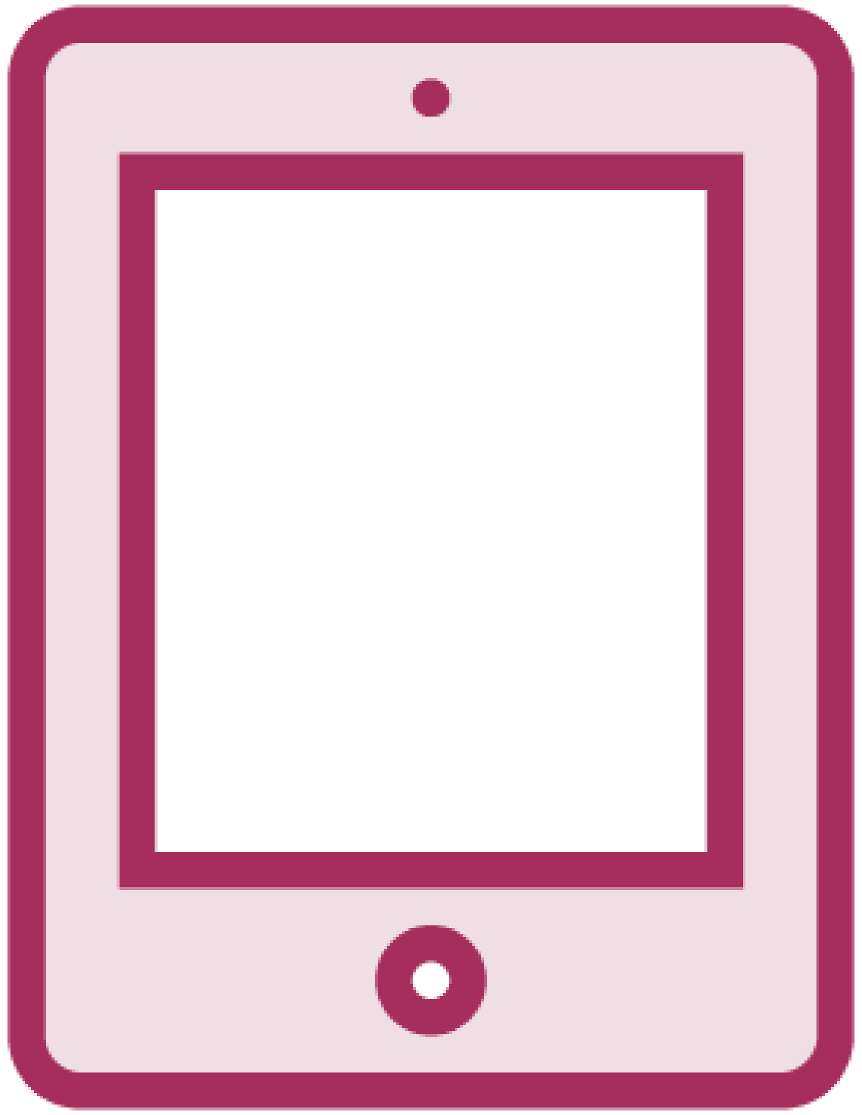
Cash: At an Automated Teller Machine (ATM)

Fake card:

- Requires clone magnetic stripe card (Track 1 data)

Impersonate the cardholder:

- PIN



Physical goods: In-store (face-to-face, customer present)

Fake card:

- Clone magnetic stripe card (Track 1 data)

Physical goods: E-commerce (customer not present)

Data:

- PAN, expiration date, name

Impersonate customer

- CVV2 (not always requested)
- Billing address

Where's the Data the Criminal Needs?

A

Authorization (auth)

C

Clearing

S

Settlement

U

Undo: Chargeback and Refunds

Where's the Data the Criminal Needs?

A

Authorization (auth)

C

Clearing

S

Settlement

U

Undo:

Chargeback and Refunds

Where's the Data the Criminal Needs?

A

Authorization (auth)

Track 1
- ATM or
- In-store
- Fuel, Ticketing, etc.

PAN+Exp+CVV2
- E-commerce
- Mail Order / Telephone Order (MOTO)

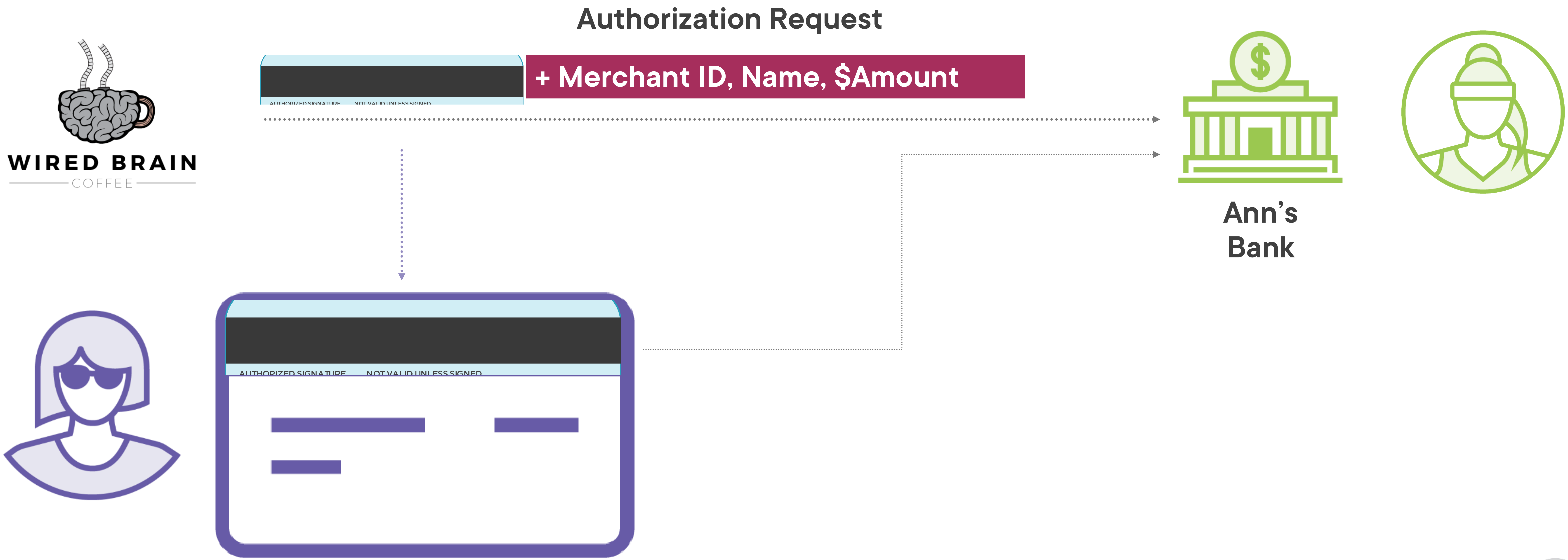
PAN+Exp
- All Track 1 data
- E-commerce or MOTO

So far I’ve mostly ignored EMV chip cards.

We’ll talk about how they change things in a few minutes.

Where Do Criminals Steal Data From?

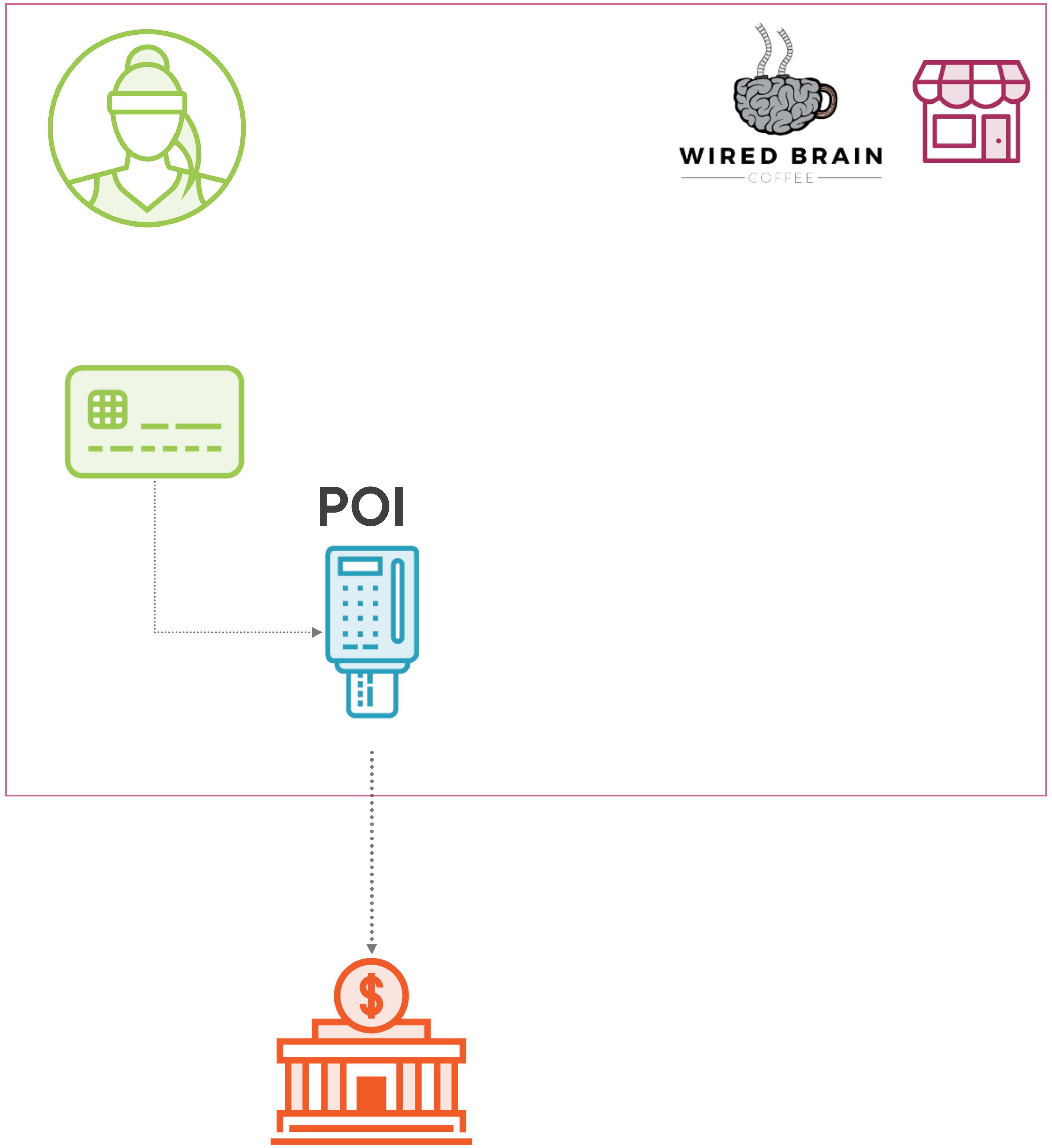
Magnetic Stripe Authorization



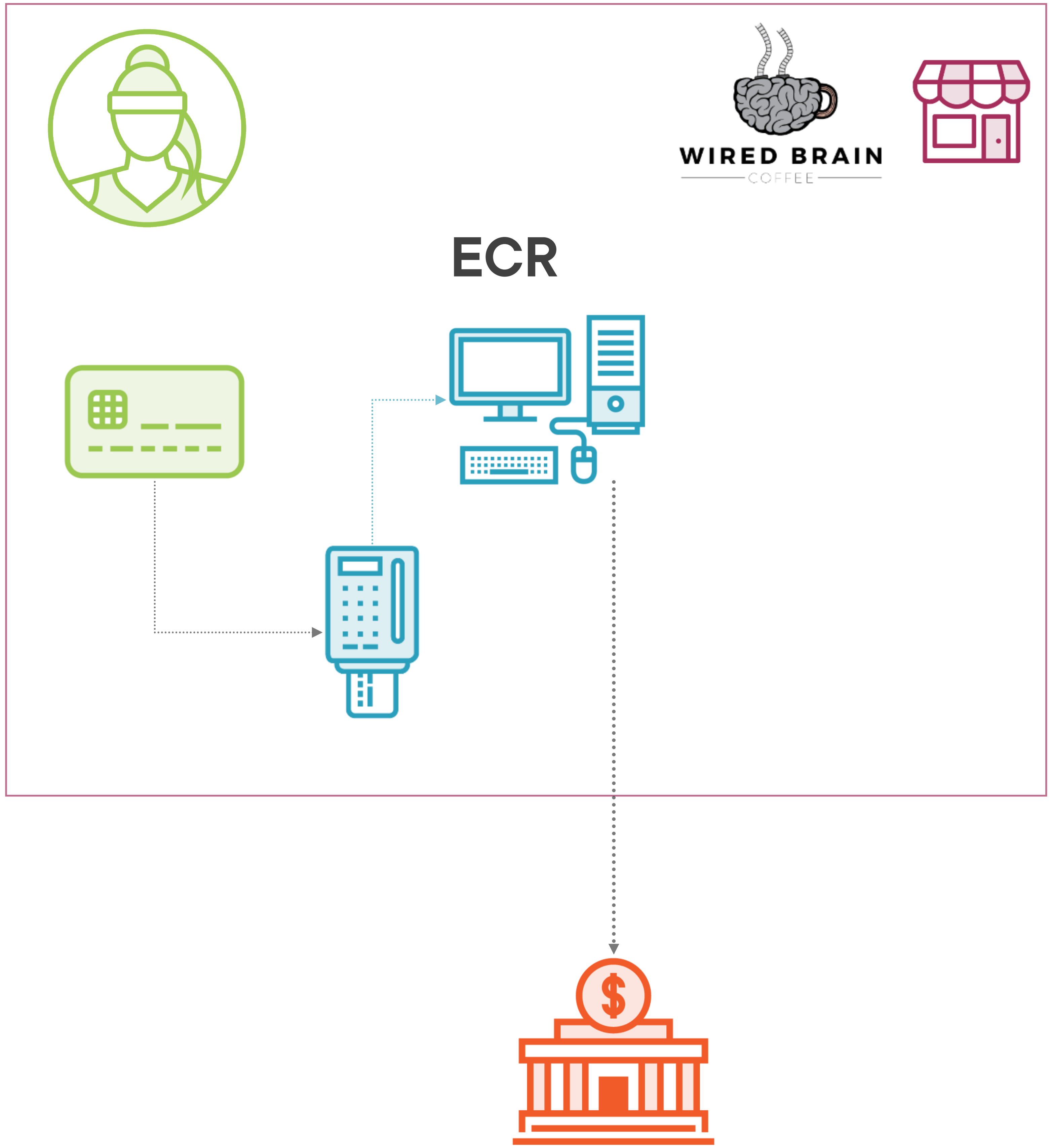
Authorization Request

+ Merchant ID, Name, $Amount

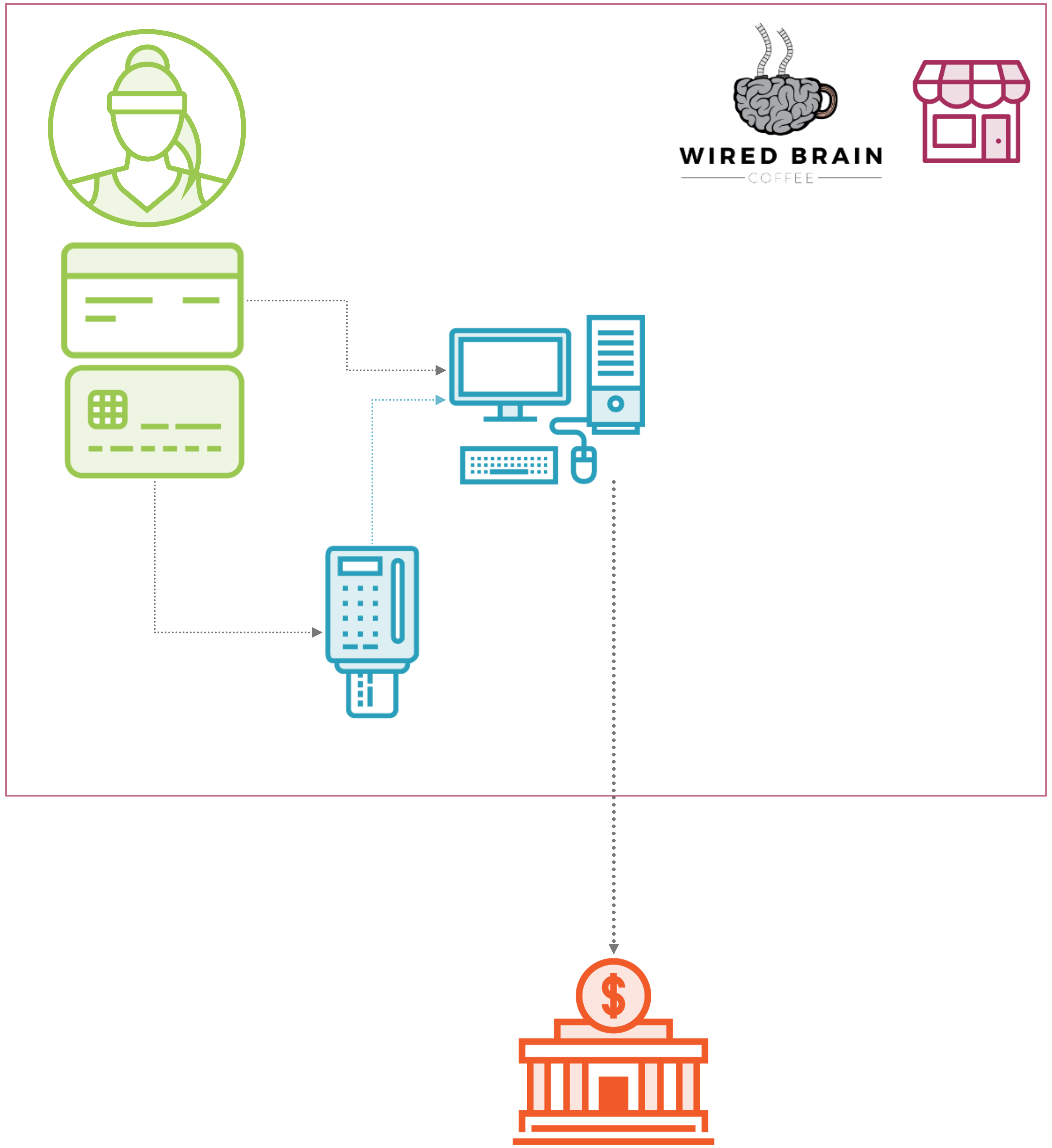
Where to Find Authorization Data (Face-to-face)



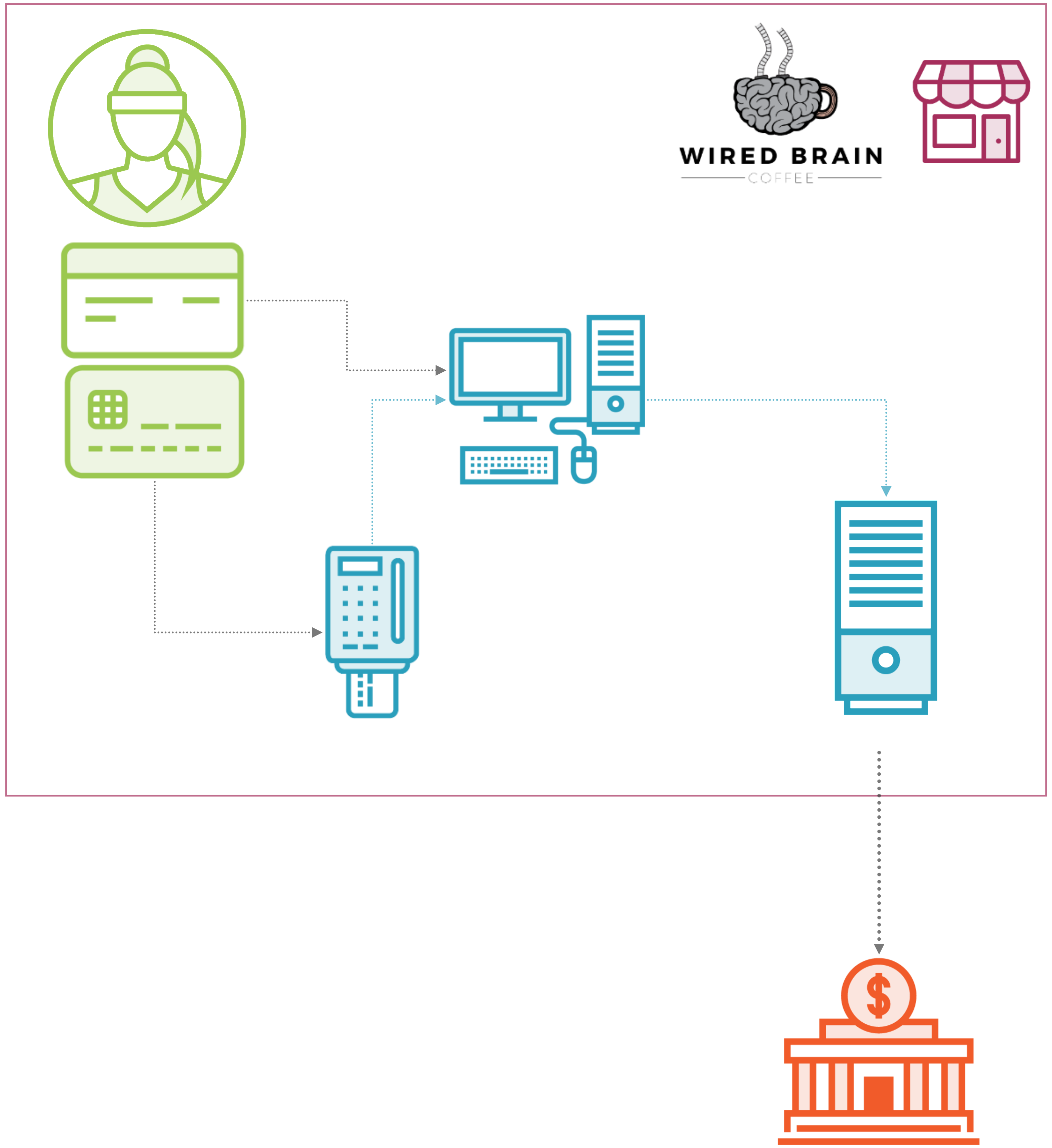
Where to Find Authorization Data (Face-to-face)



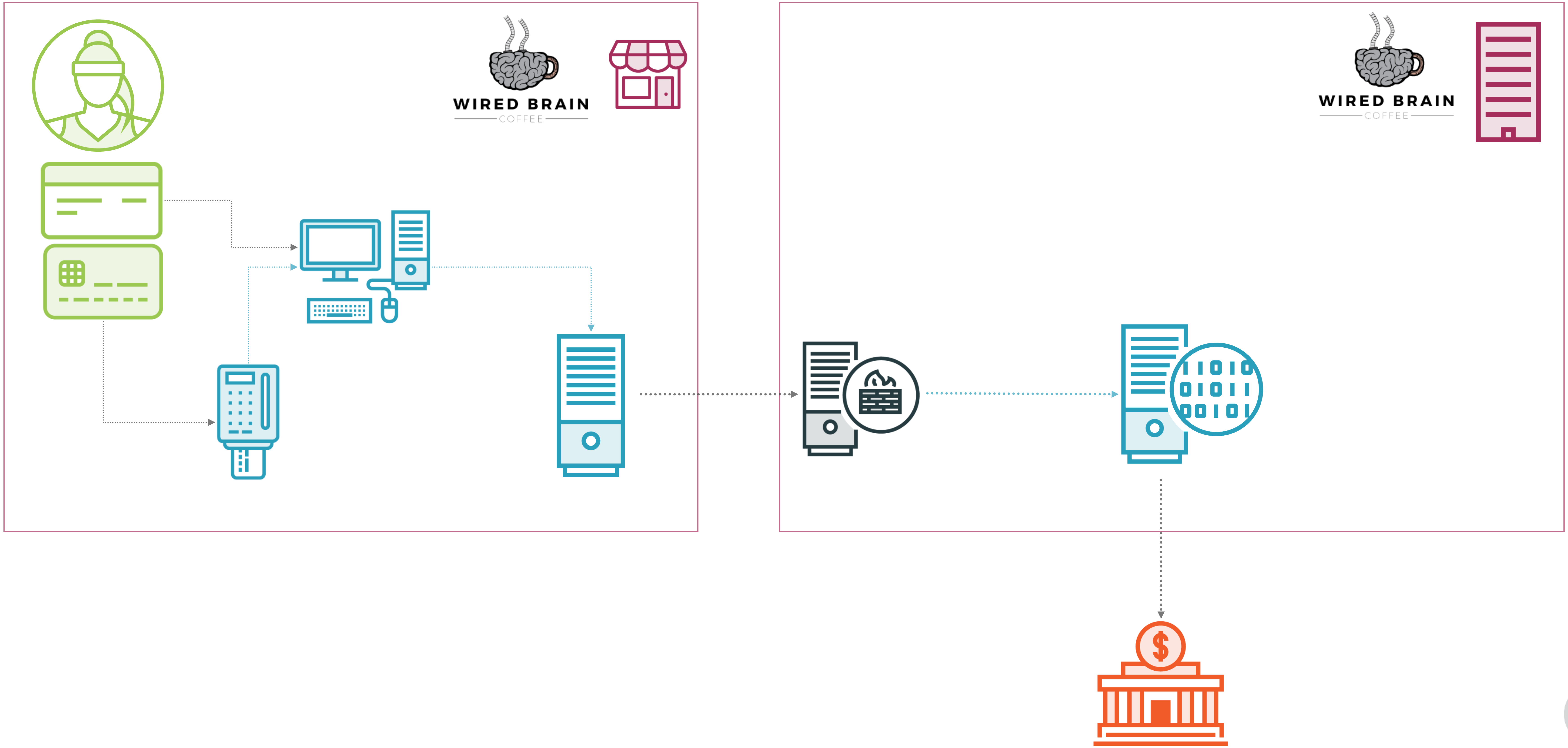
Where to Find Authorization Data (Face-to-face)



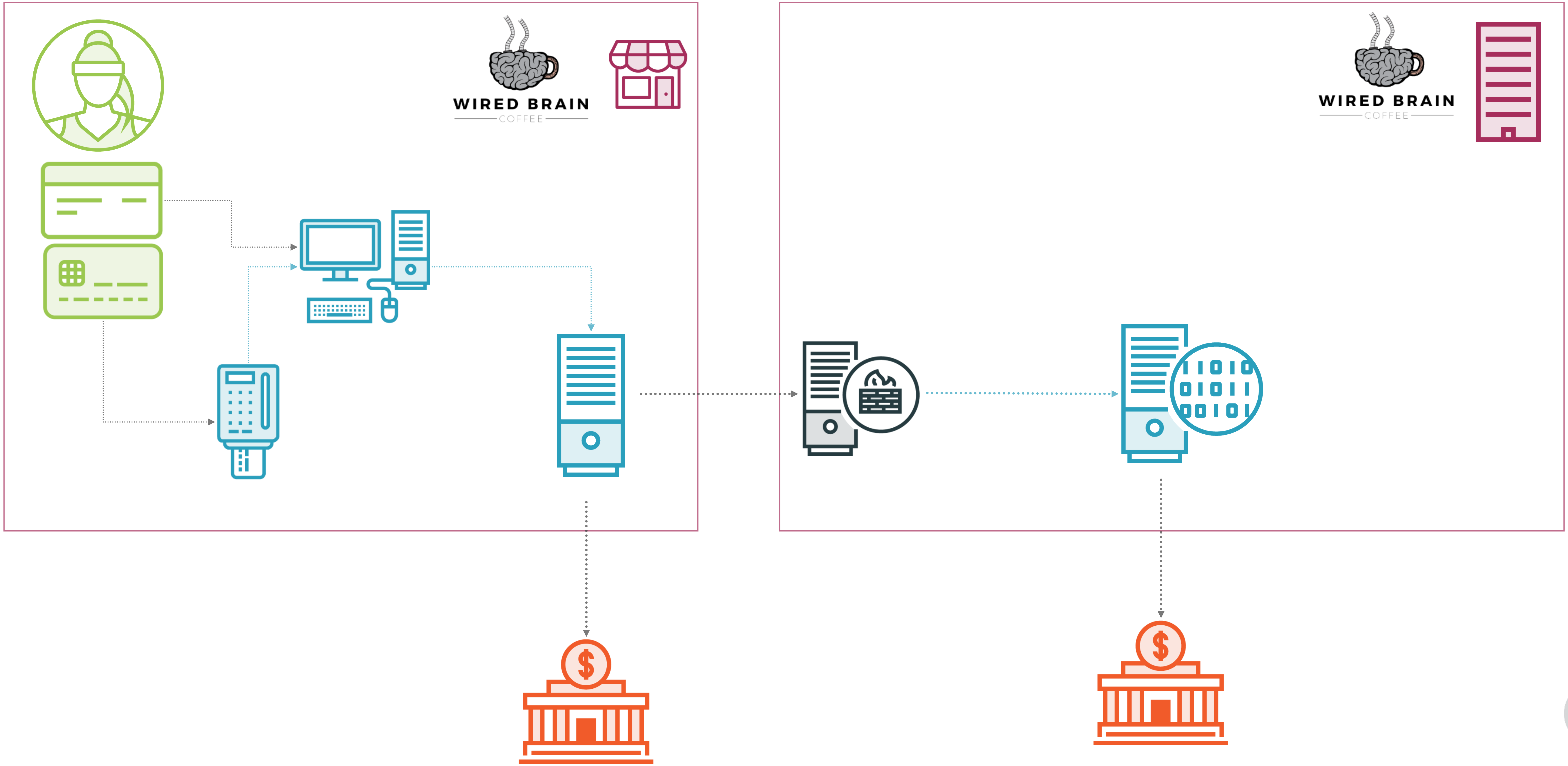
Where to Find Authorization Data (Face-to-face)



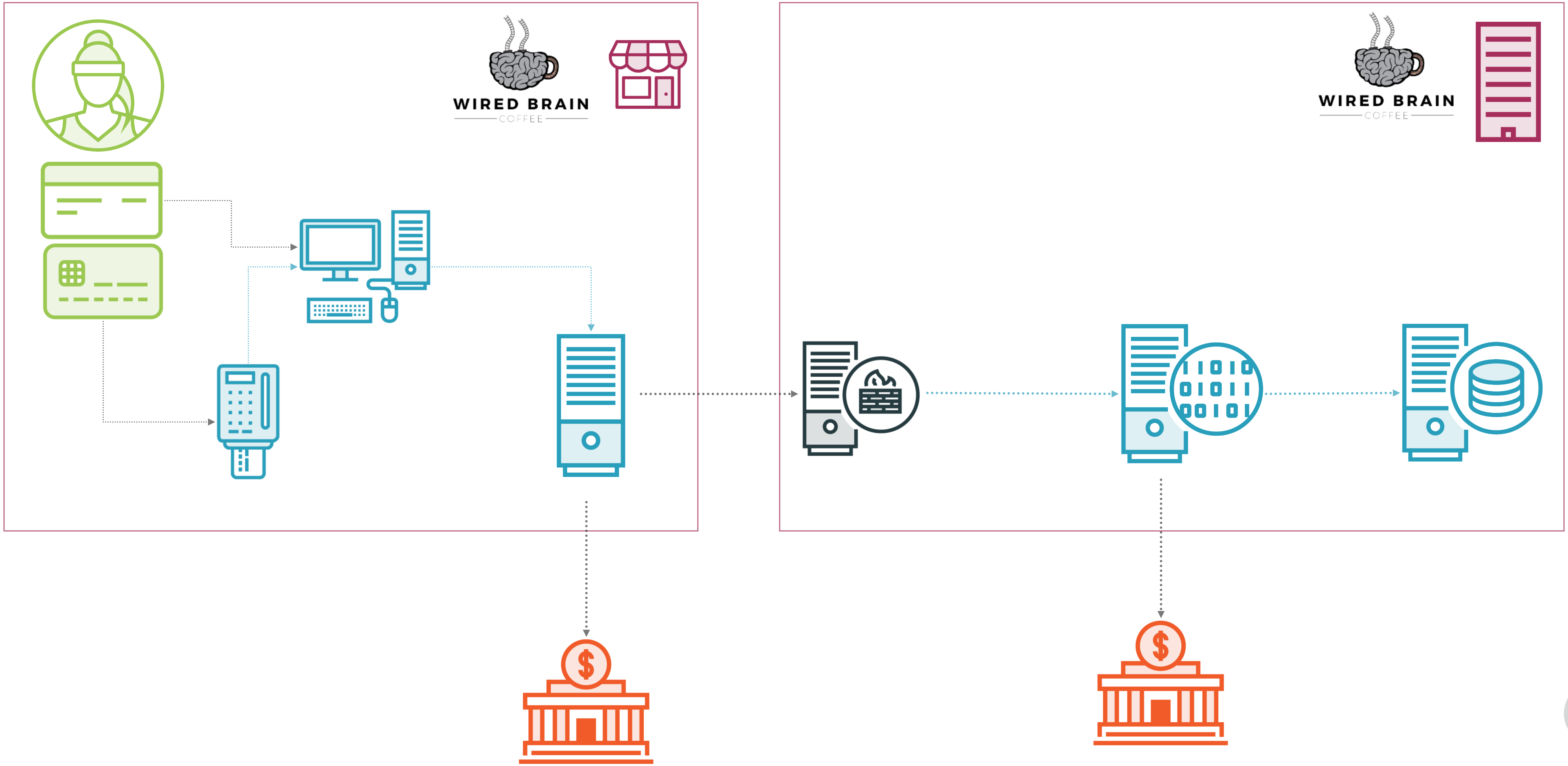
Where to Find Authorization Data (Face-to-face)



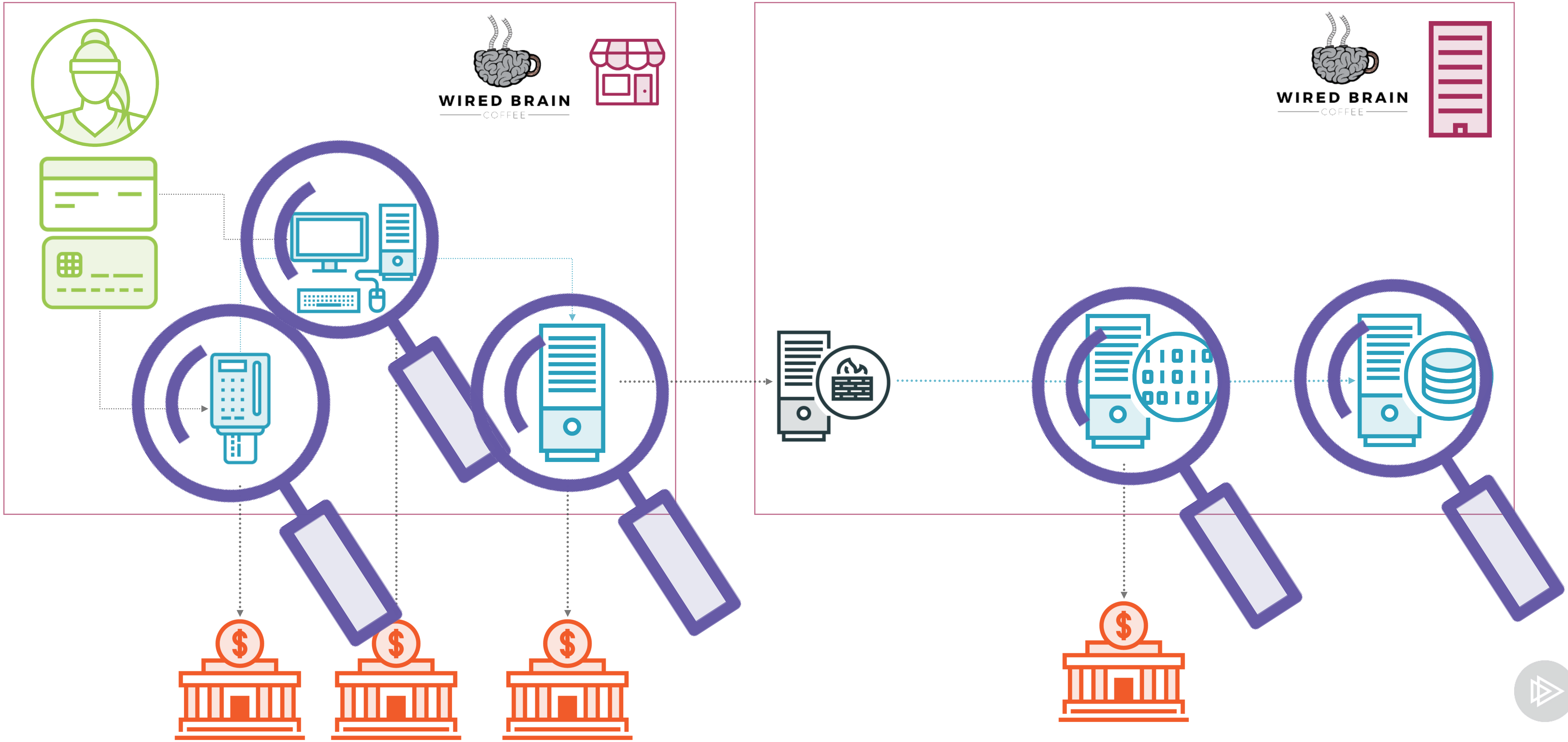
Where to Find Authorization Data (Face-to-face)



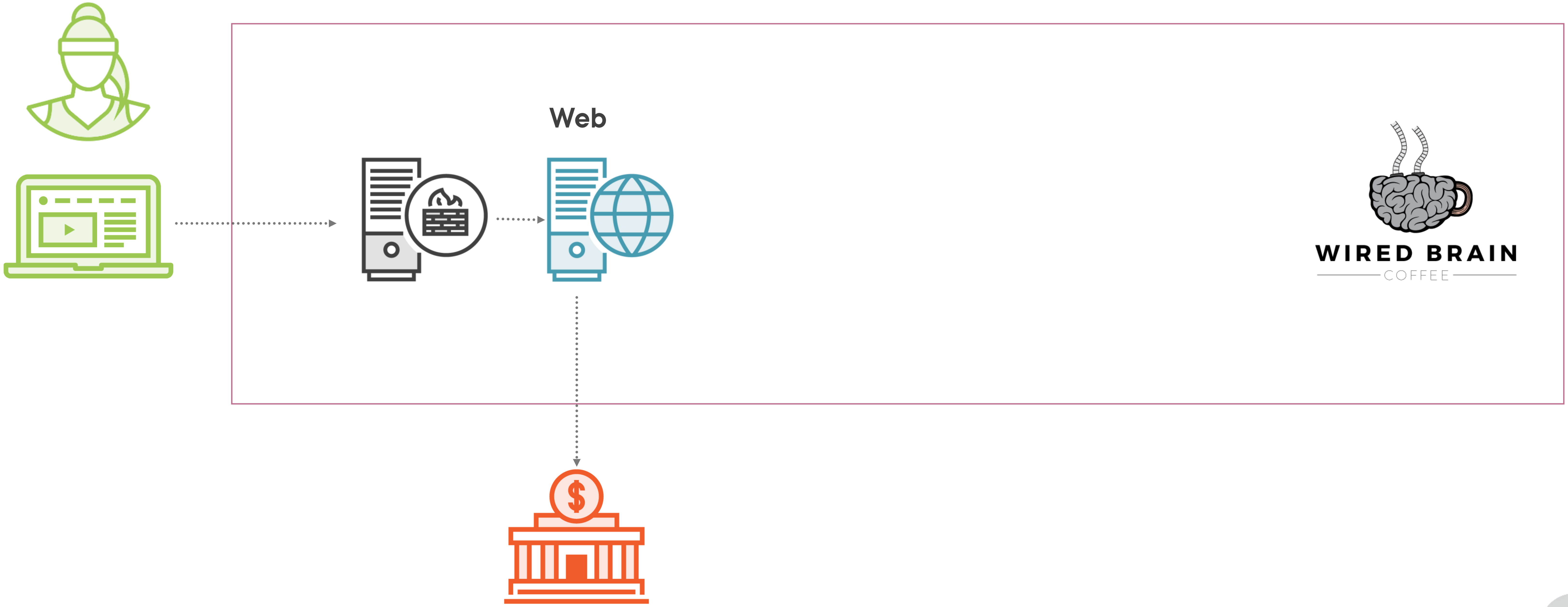
Where to Find Authorization Data (Face-to-face)



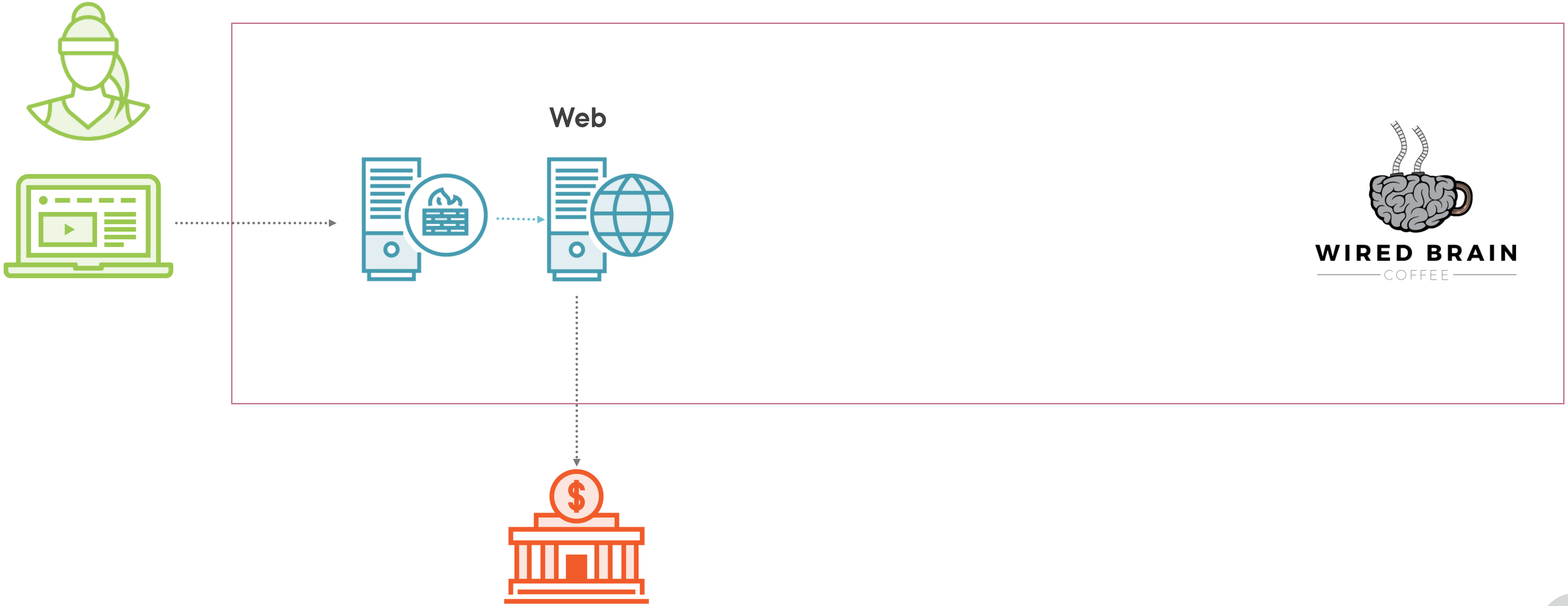
Where to Find Authorization Data (Face-to-face)



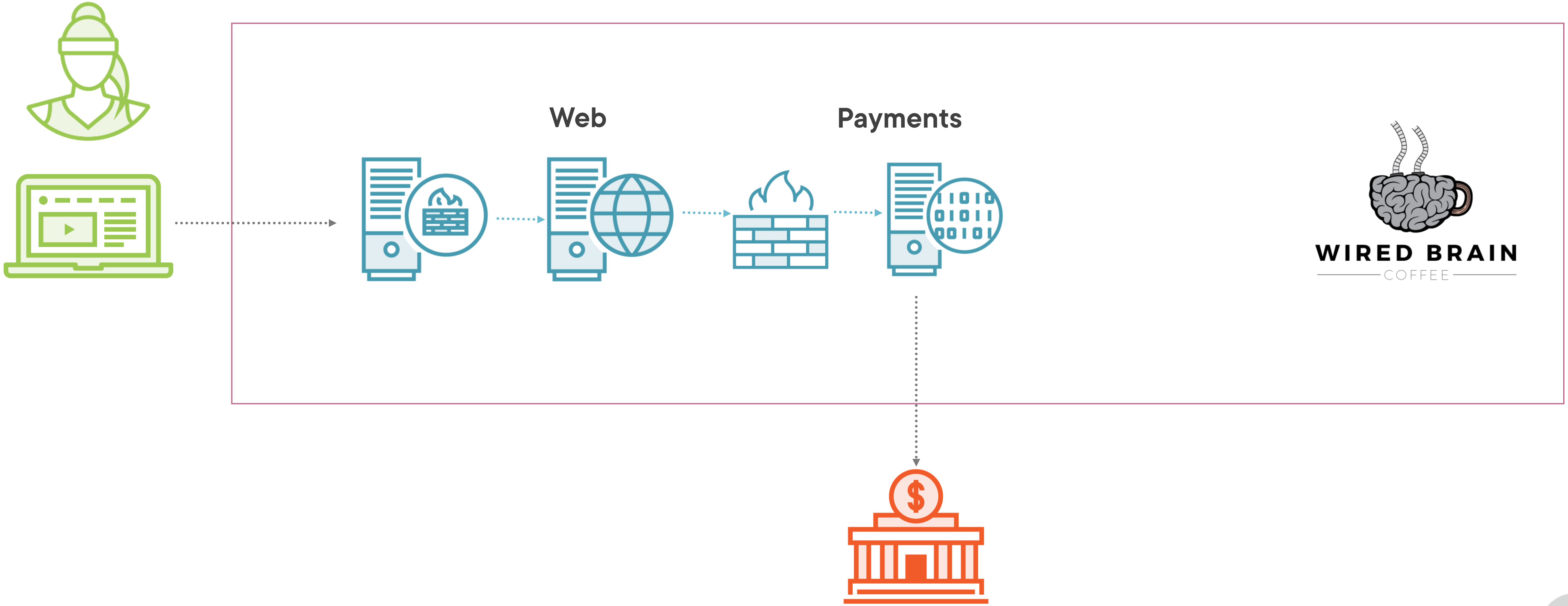
Where to Find Authorization Data (E-commerce)



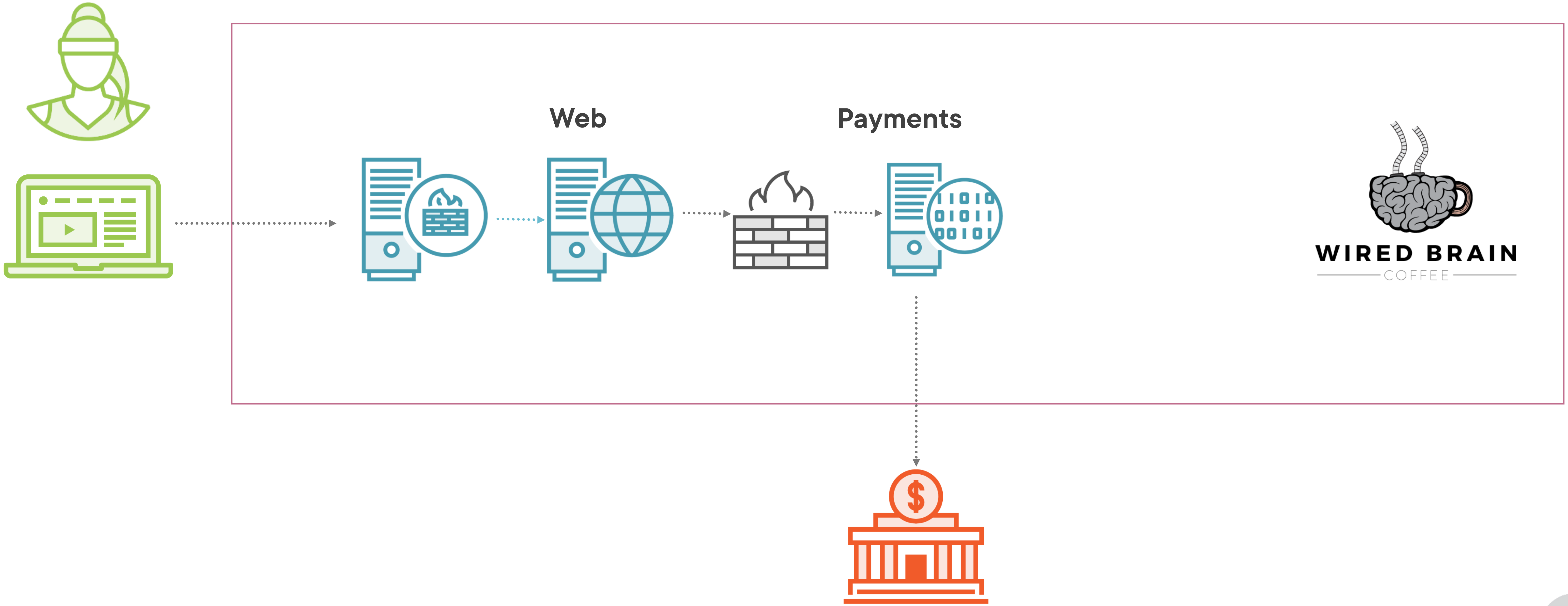
E-commerce



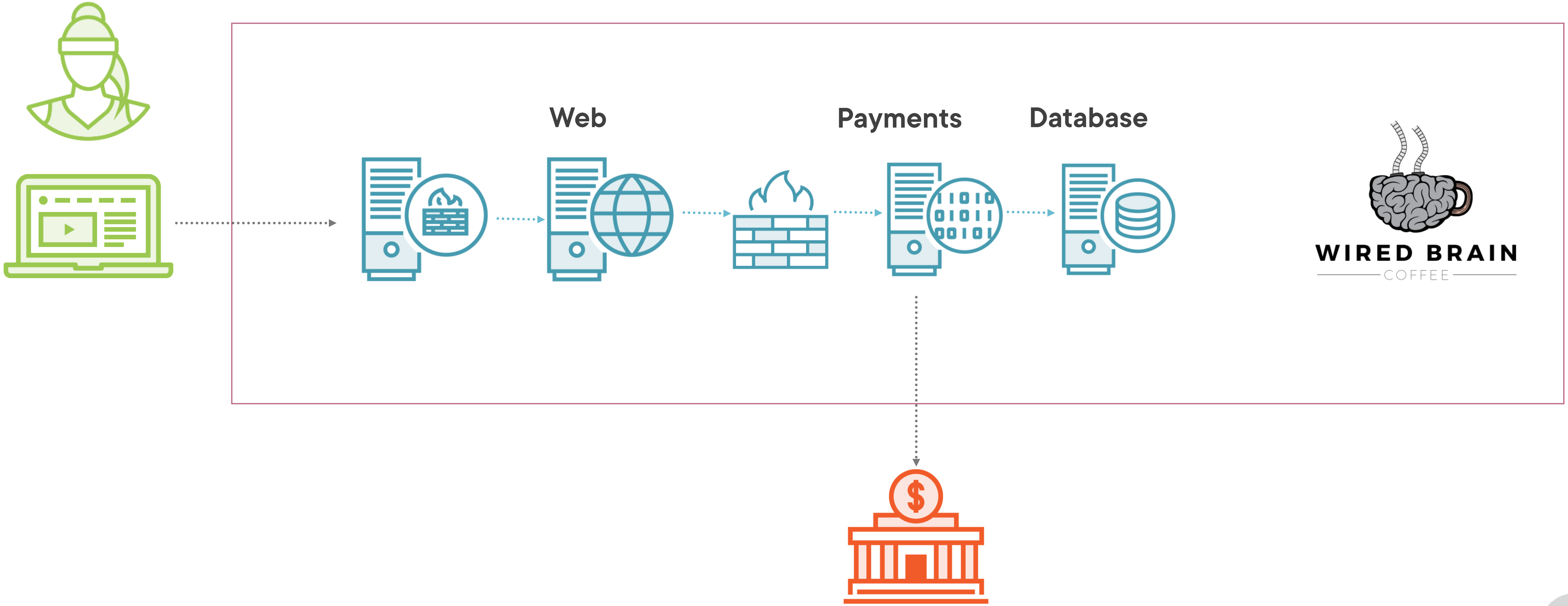
E-commerce



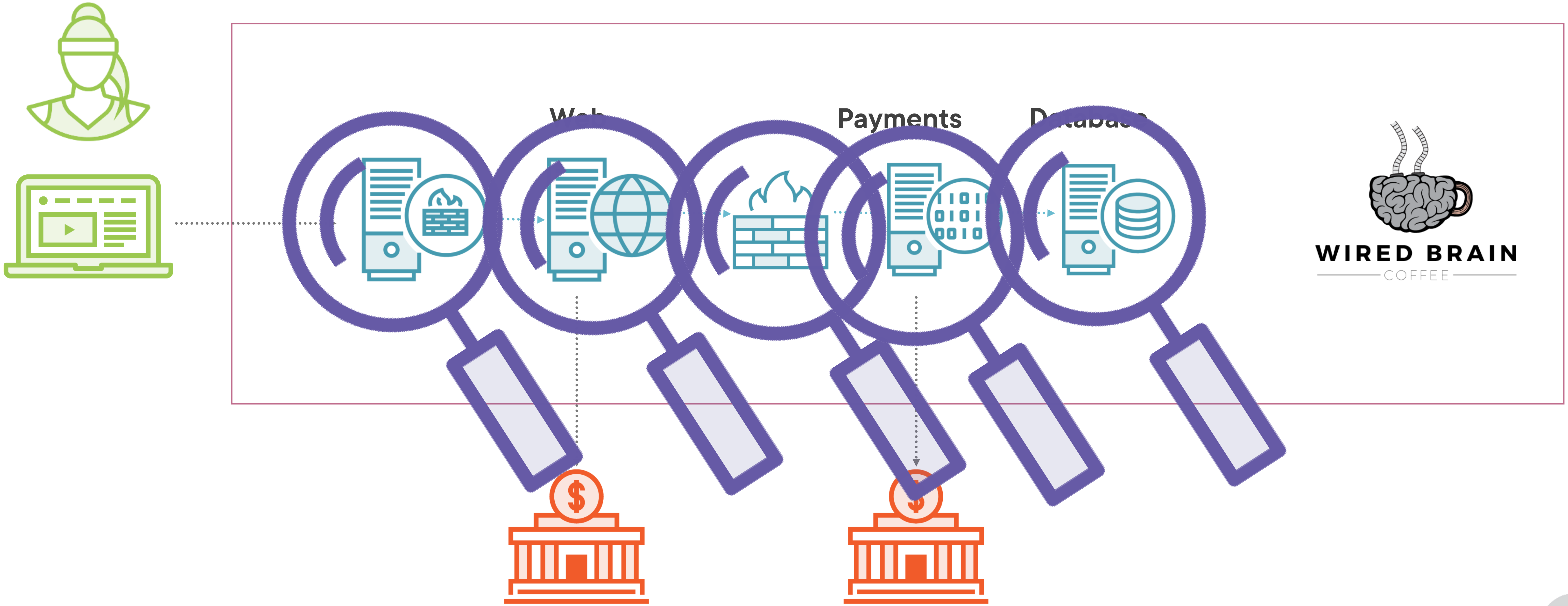
E-commerce



E-commerce



E-commerce



Who Wants Authorization Data?

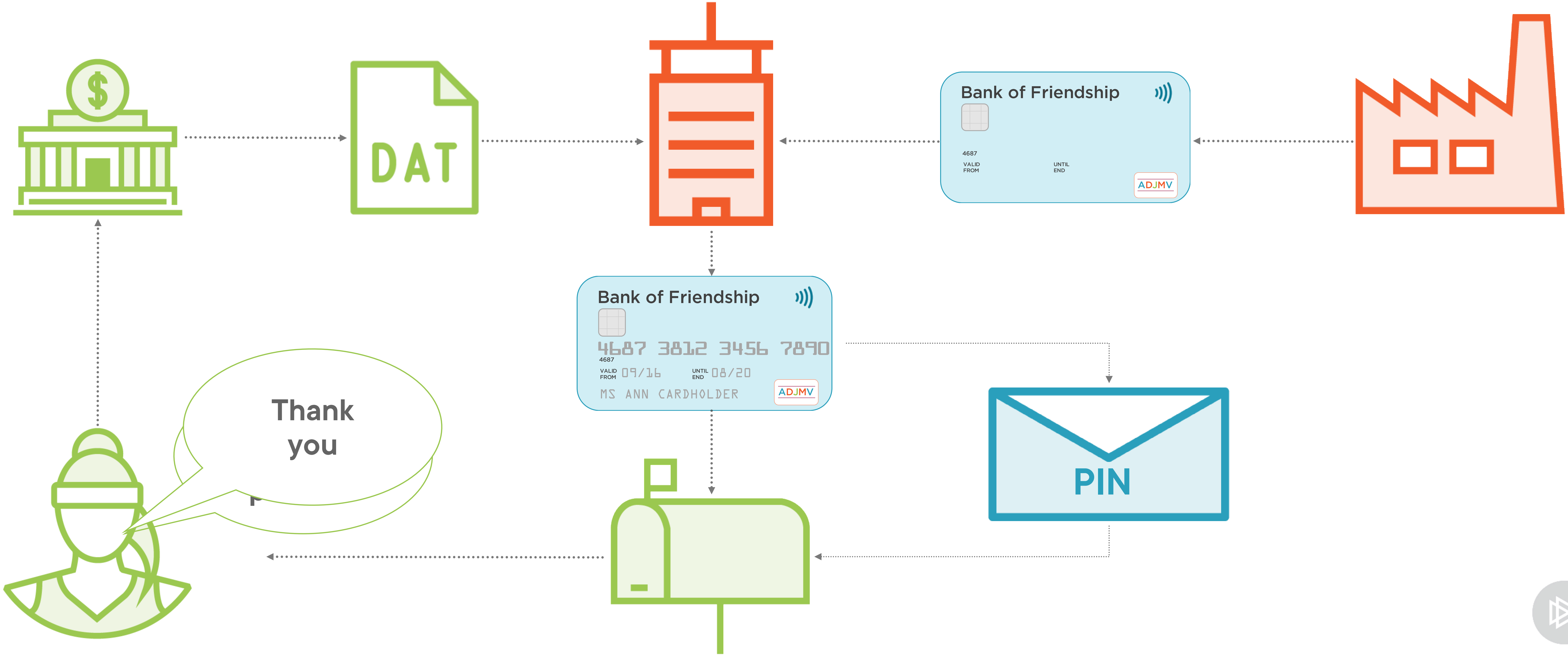
Criminals

Want to steal authorization data

But What Would a Criminal Like More?

And the PIN

Making Payment Cards



Personalization File

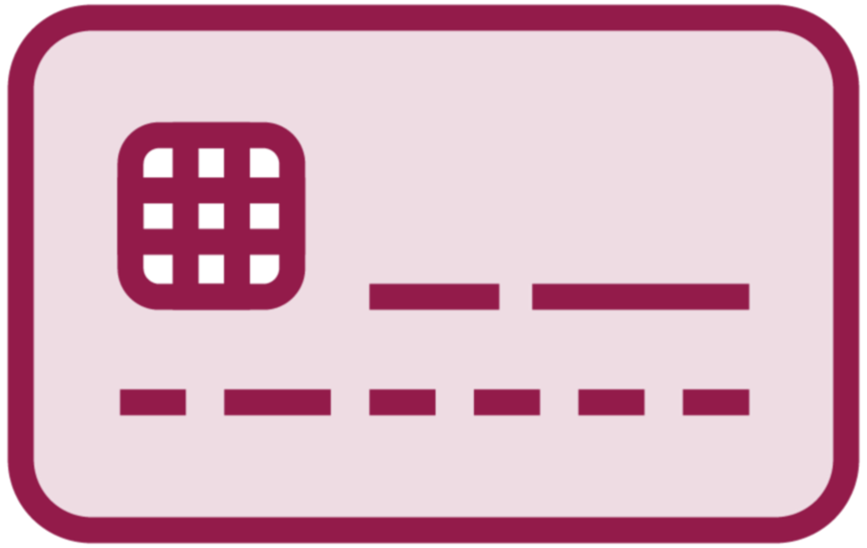
Personalization Bureau

Blank Card

Card Manufacturer

Secure Payment Technologies

Secure Payment Technologies



EMV Chip

4258 7896 2476 7852

↓

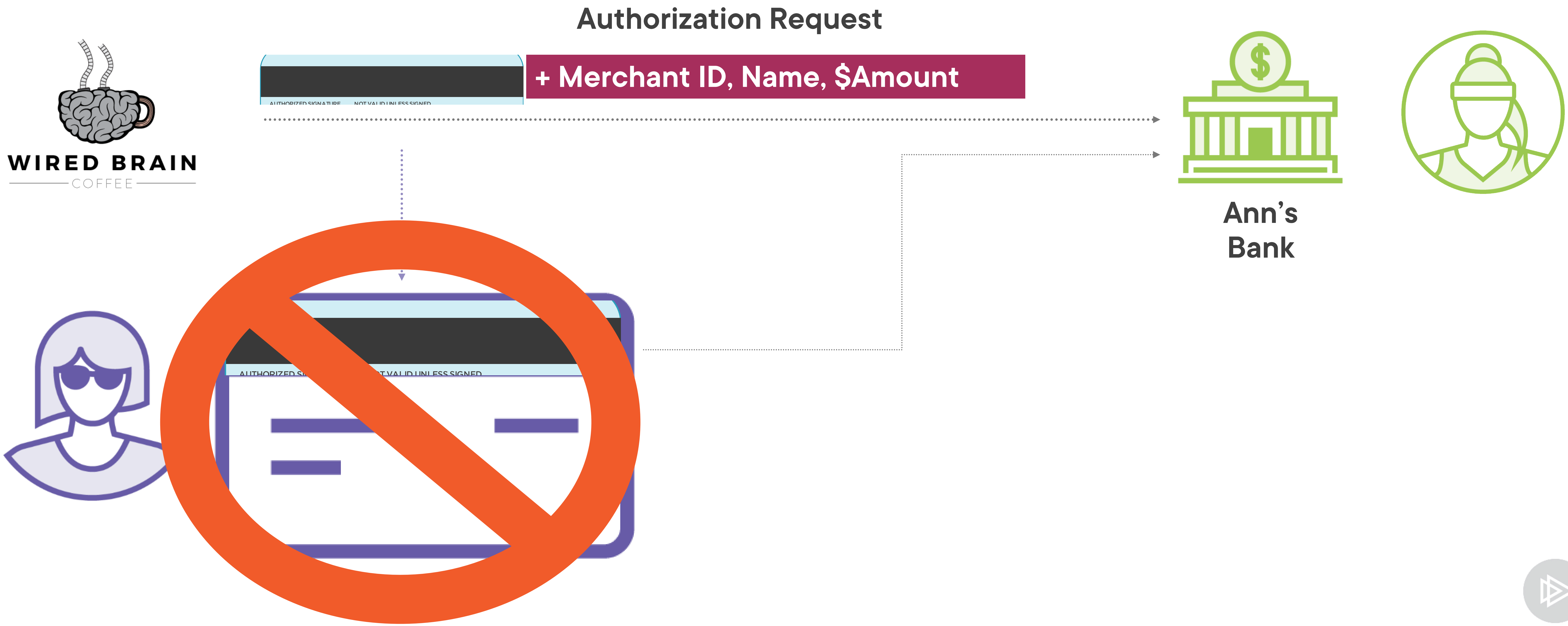
4987 2175 6187 1111

EMV Tokenization

3DS

EMV 3 Domain Security

Magnetic Stripe Authorization

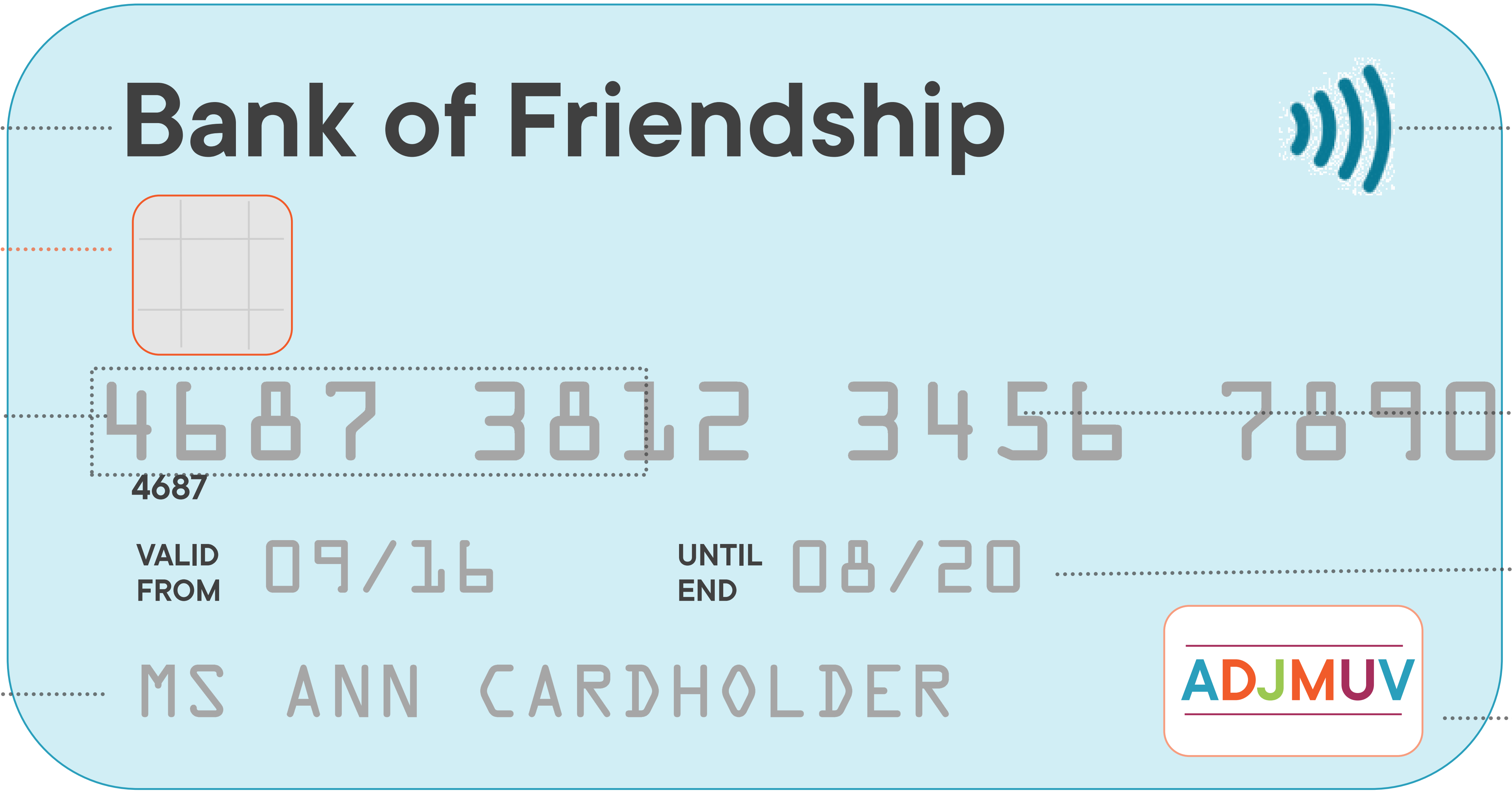


Authorization Request

+ Merchant ID, Name, $Amount

Ann's Bank

The Data on a Payment Card



Issuer Name

EMV Chip

Bank Identification Number (BIN)

Cardholder Name

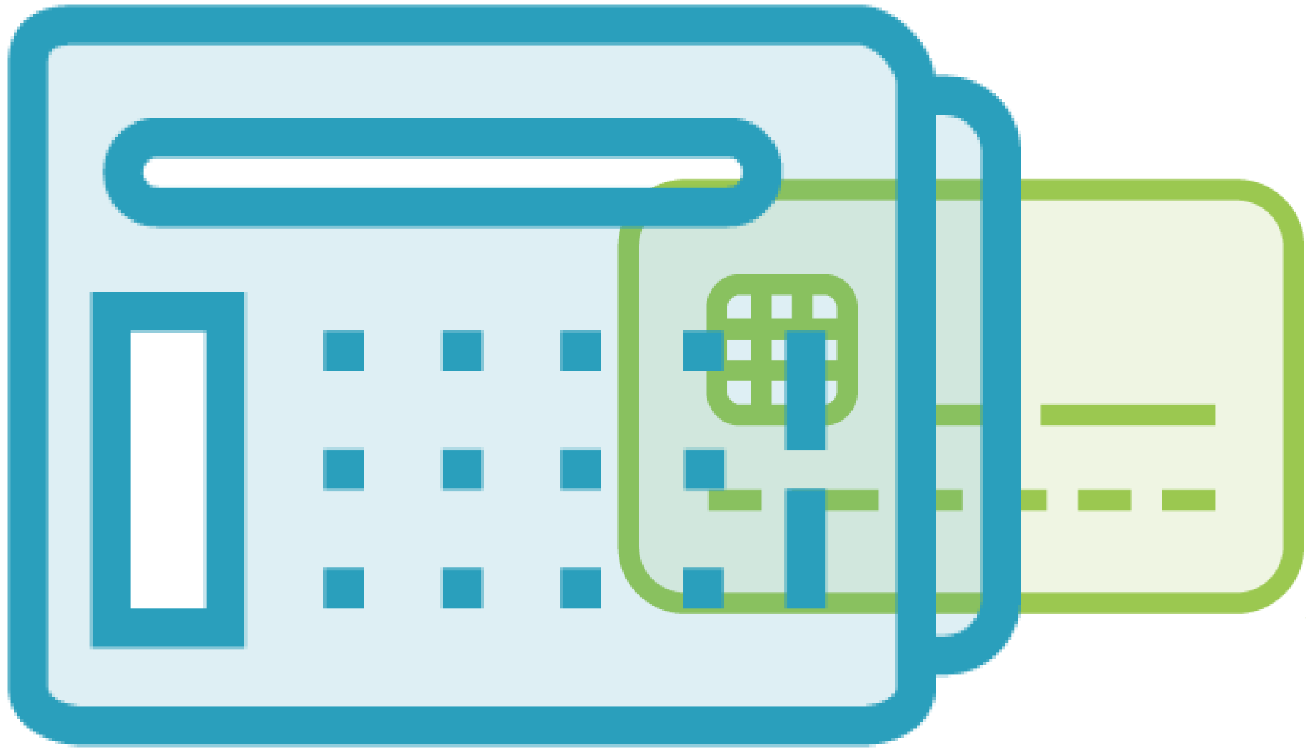
Contactless Indicator

Primary Account Number (PAN)

Expiration Date

Card Brand

How an EMV Card Works



Hello

Hello. Can I have a PIN?

Here's a PIN – is it correct?

Yes (offline)

Here's some data

Brilliant! Here's a cryptogram and something that looks like a mag stripe

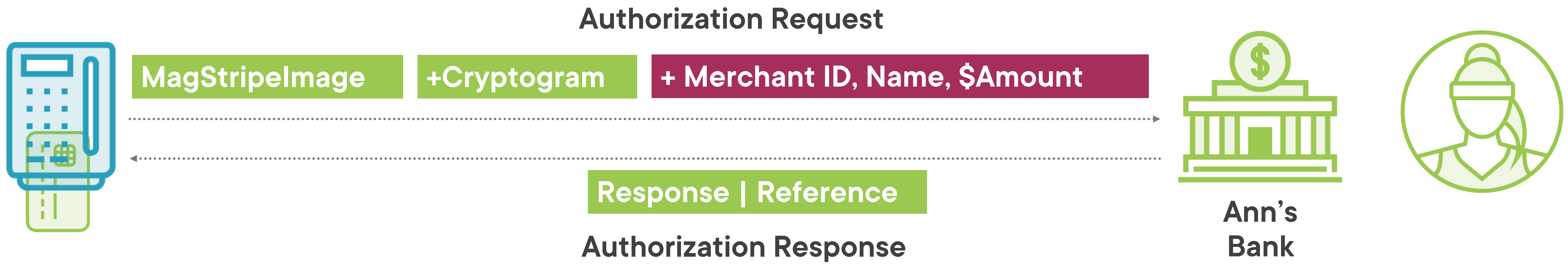
OK, I'm going for authorization, hang on

Can you send it off to my issuing bank please?

Awesome, the transaction was authorized, here's the data

Well thank you

EMV Authorization



Authorization Request

MagStripeImage

+Cryptogram

+ Merchant ID, Name, $Amount

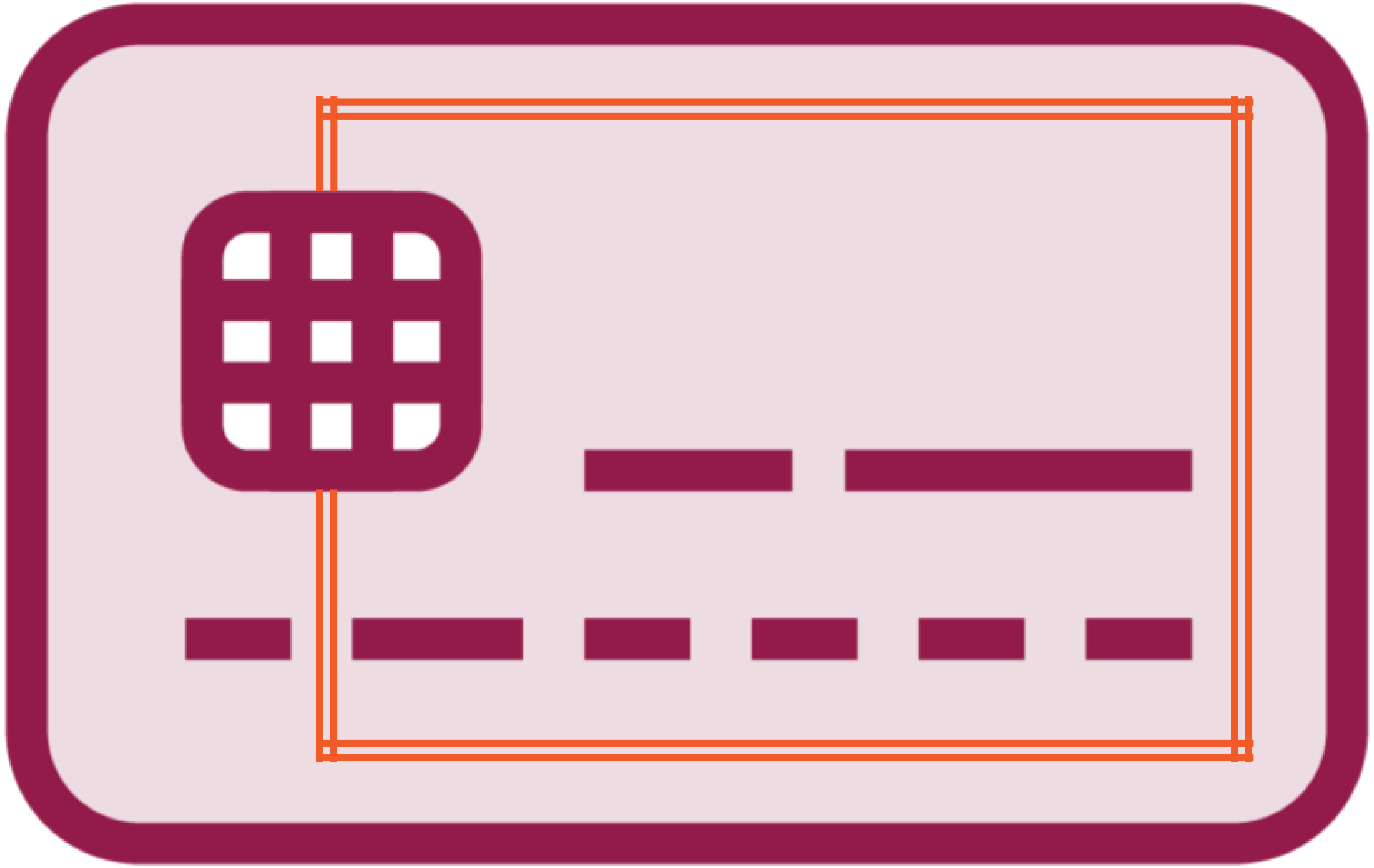
Response | Reference

Authorization Response

Ann's Bank

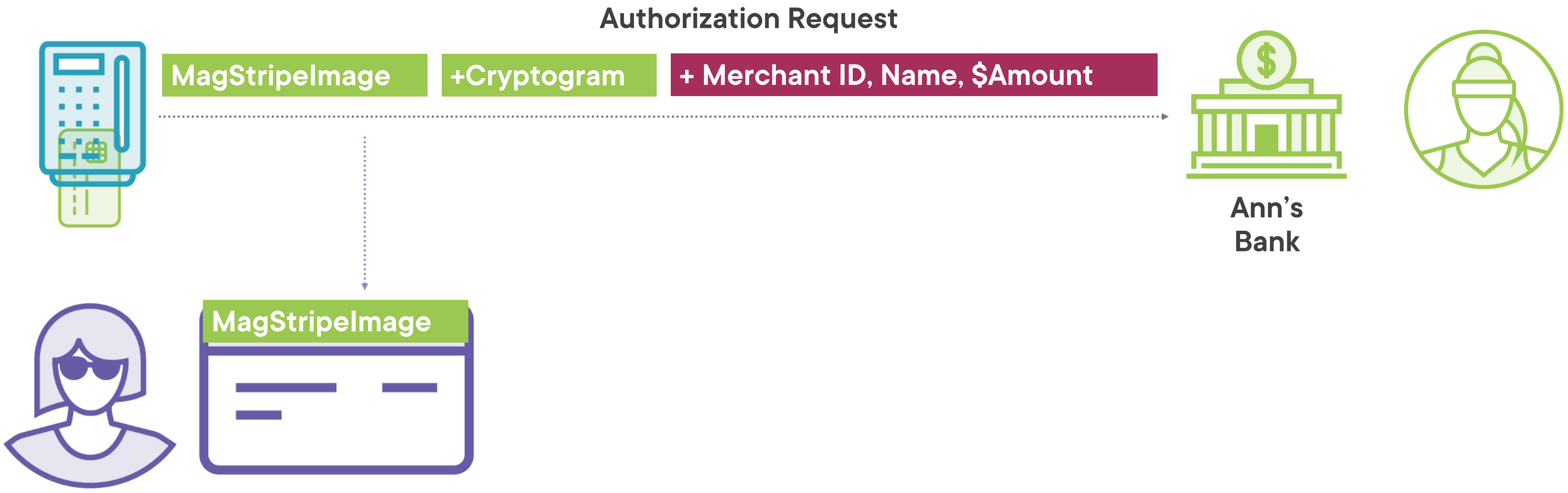
1. Validate mag stripe data
2. Generate cryptogram
3. Verify cryptograms match
4. Check balance

Contactless EMV



An antenna embedded in the card uses the magnetic field created by a contactless card reader to create an electrical current to power up the chip.

EMV Attack



Authorization Request

MagStripeImage

+Cryptogram

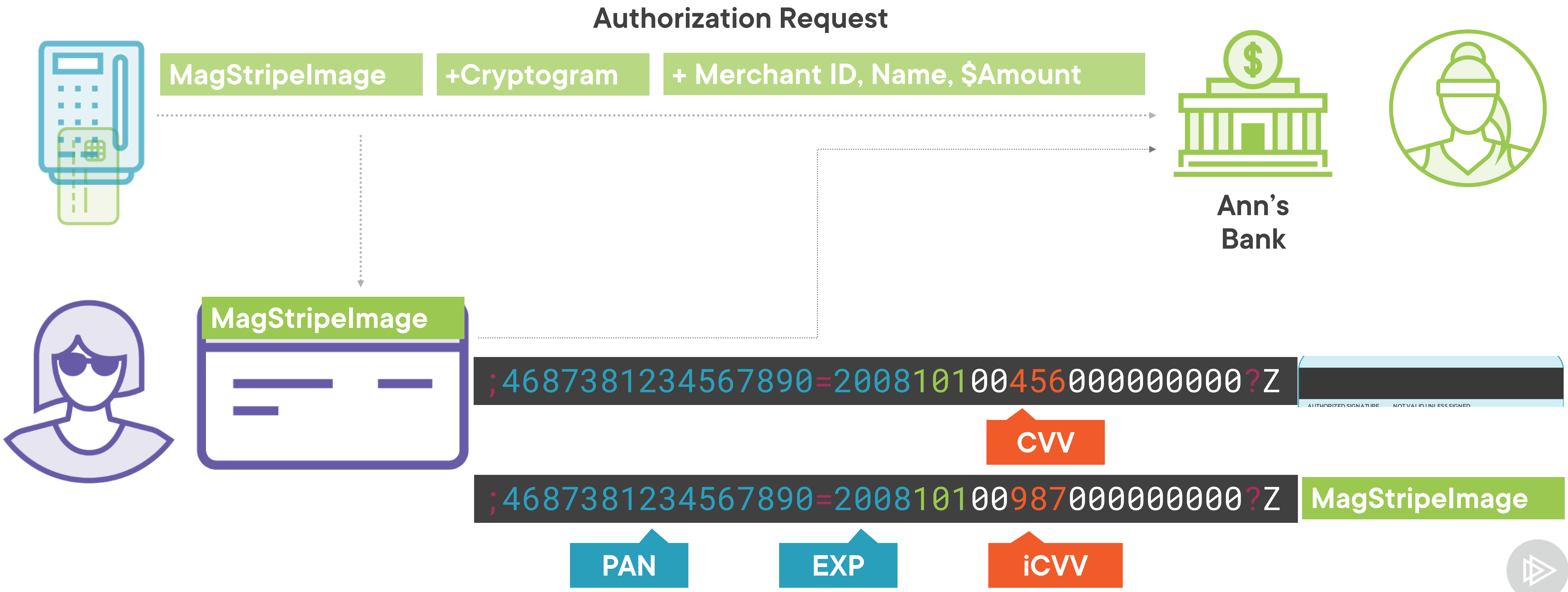
+ Merchant ID, Name, $Amount

Ann's Bank

MagStripeImage

EMV Attack

WIRED BRAIN
COFFEE



Authorization Request

MagStripeImage | +Cryptogram | + Merchant ID, Name, $Amount

Ann's Bank

MagStripeImage

`;4687381234567890=200810100456000000000?Z`

CVV

`;4687381234567890=200810100987000000000?Z`

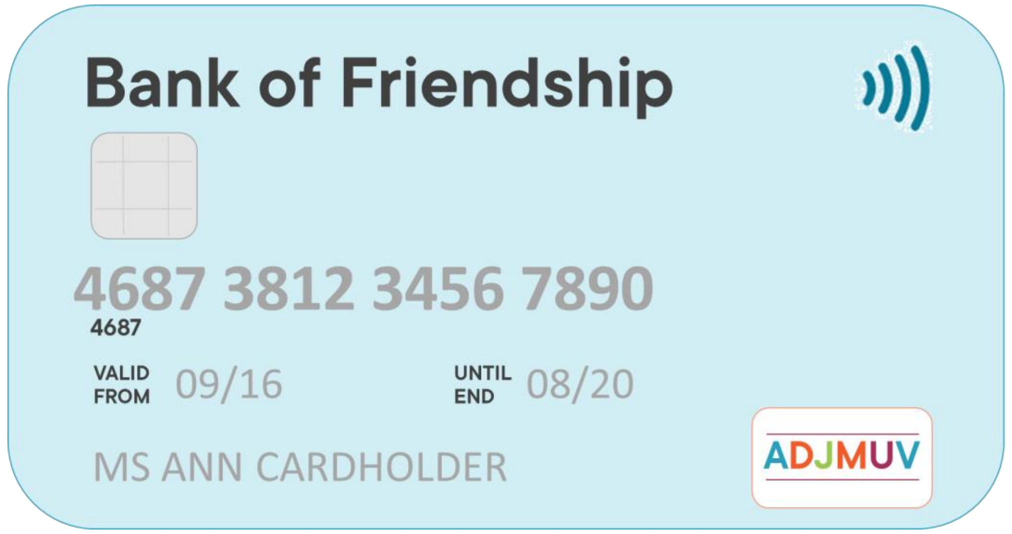
MagStripeImage

PAN

EXP

iCVV

No Longer Just Cards

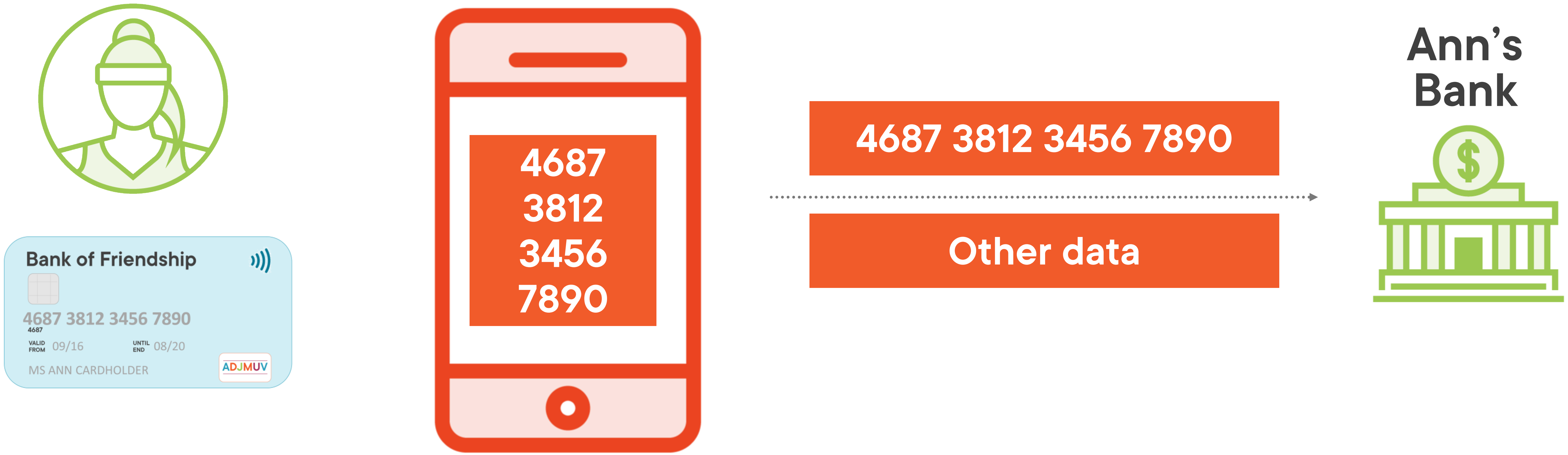


Traditional Cards

Smartphones

Smart Devices

Add a Card to a Device



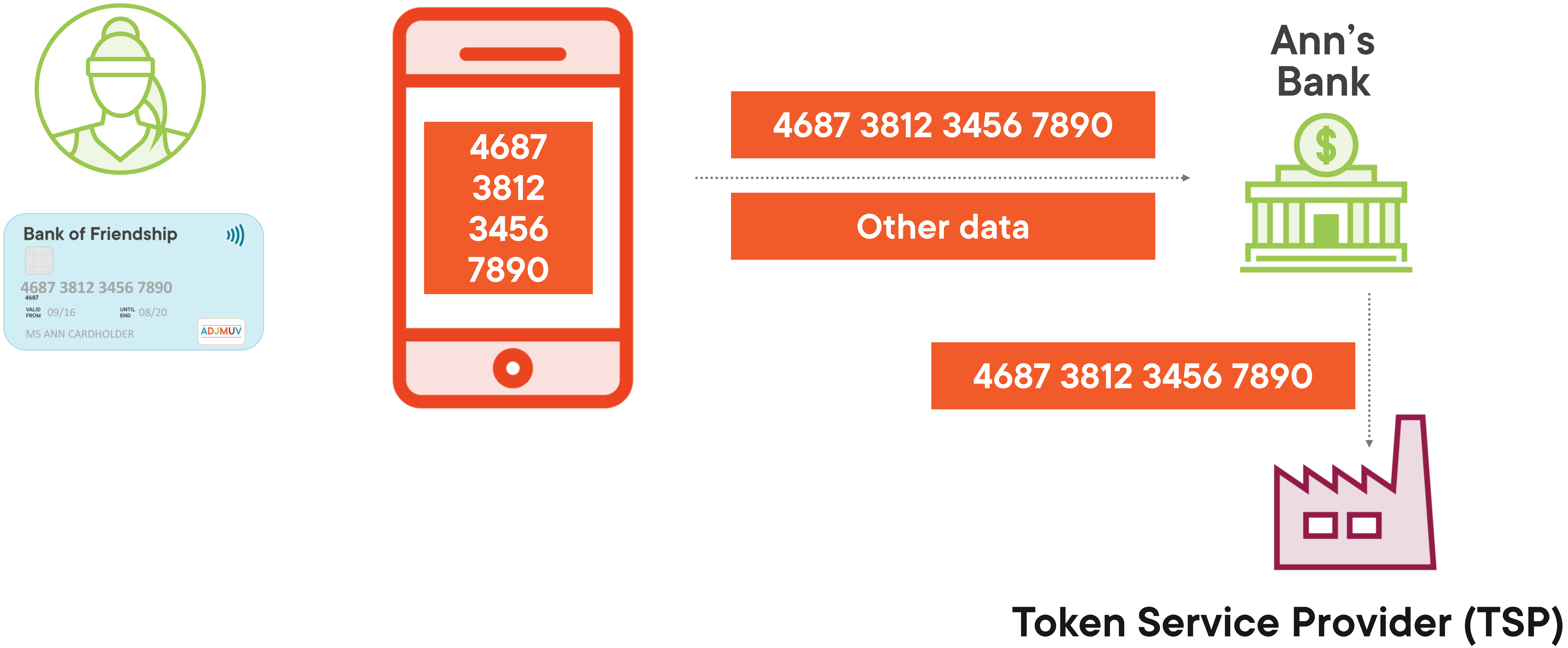
4687
3812
3456
7890

4687 3812 3456 7890

Other data

Ann's Bank

Add a Card to a Device



Ann's Bank

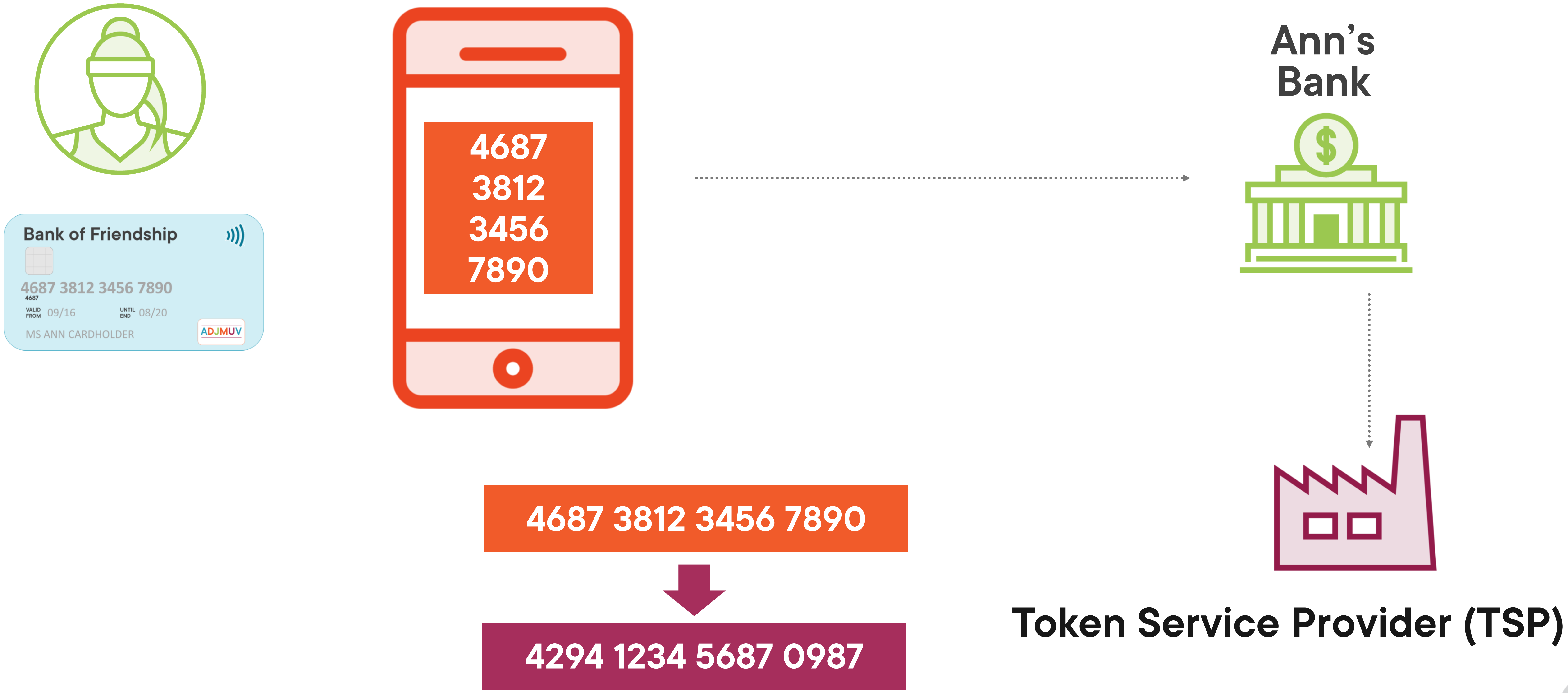
4687 3812 3456 7890

Other data

4687 3812 3456 7890

Token Service Provider (TSP)

Add a Card to a Device



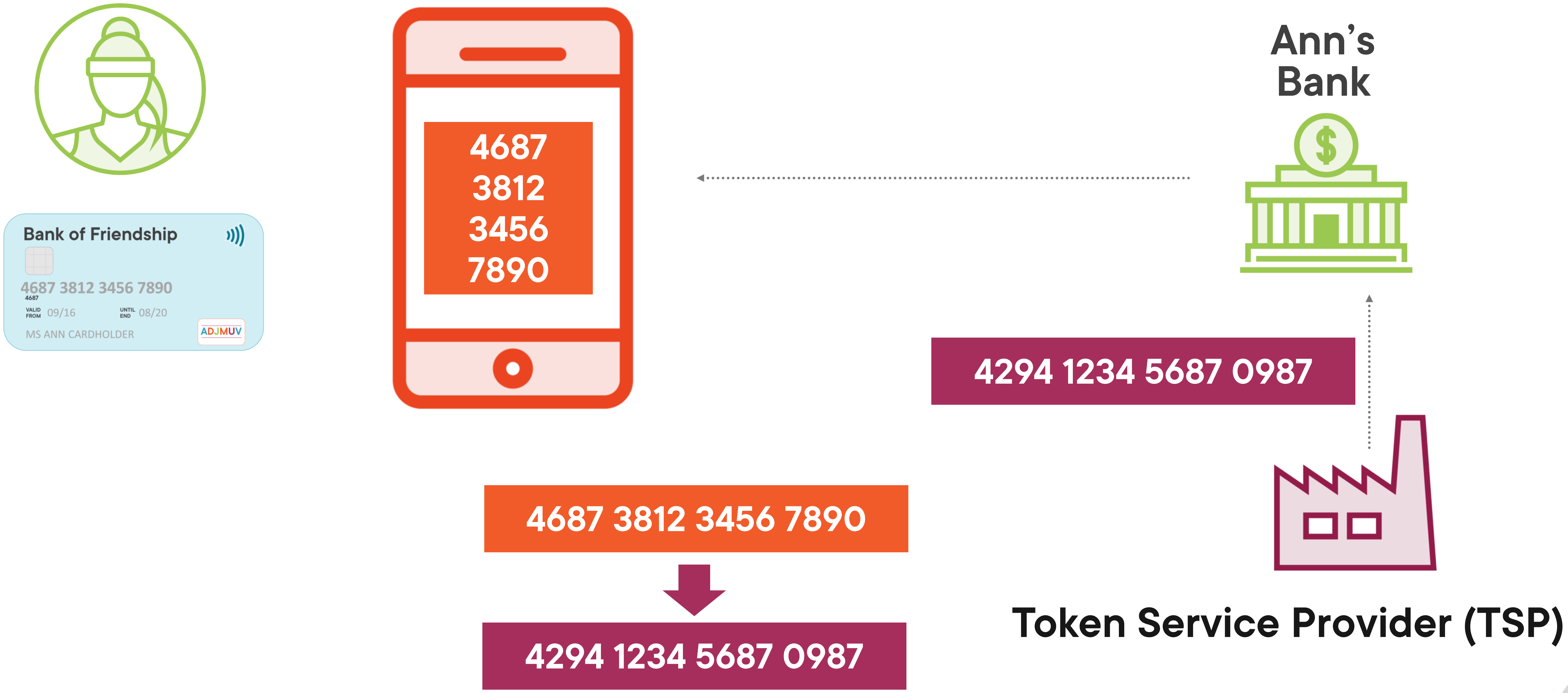
Ann's Bank

Token Service Provider (TSP)

4687 3812 3456 7890

4294 1234 5687 0987

Add a Card to a Device



Ann's Bank

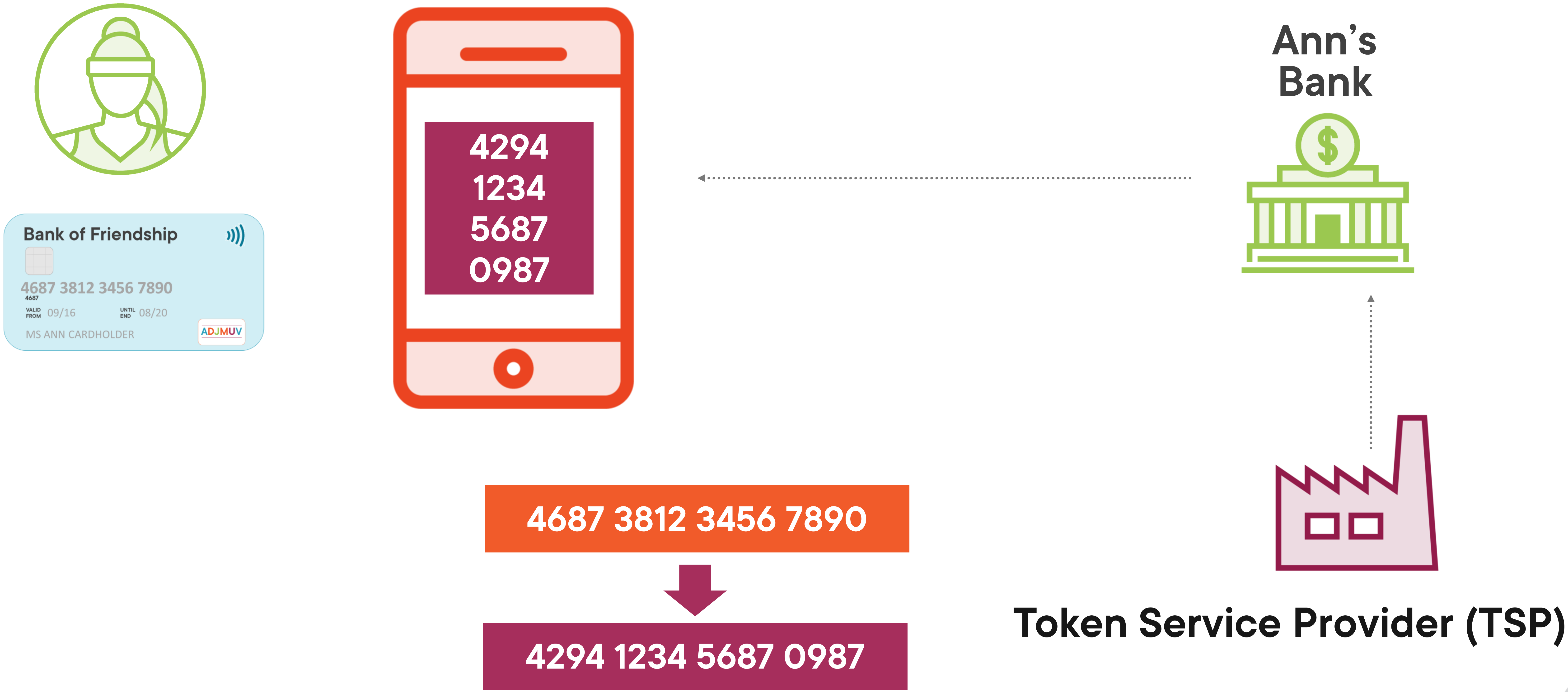
4294 1234 5687 0987

4687 3812 3456 7890

4294 1234 5687 0987

Token Service Provider (TSP)

Add a Card to a Device



Ann's Bank

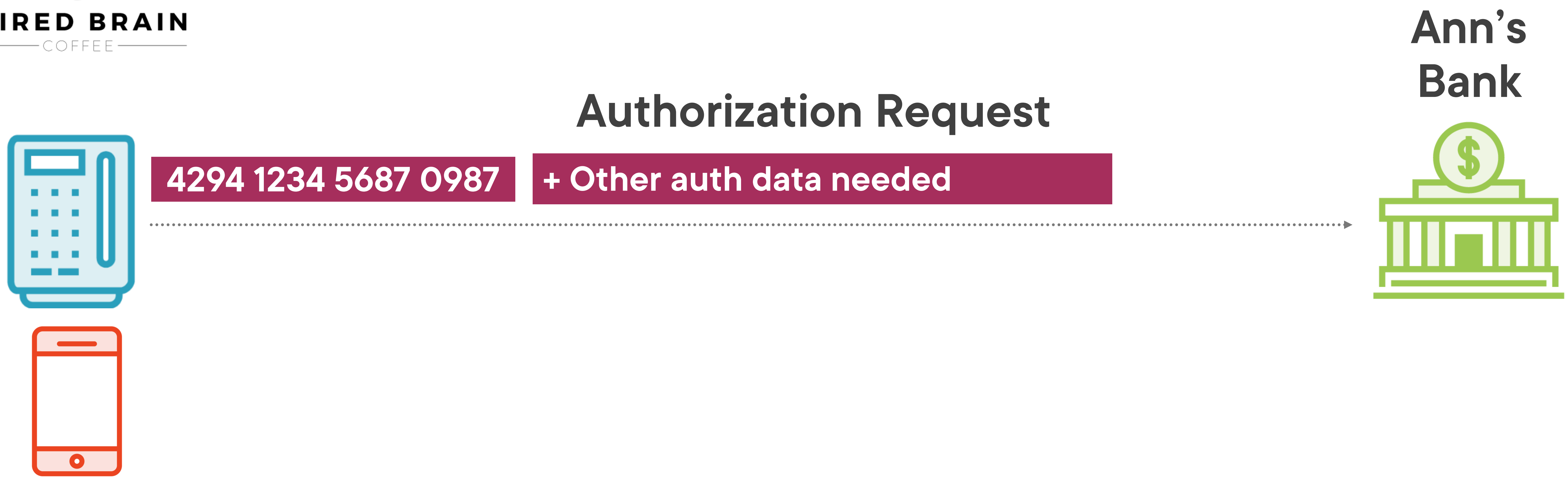
4687 3812 3456 7890

4294 1234 5687 0987

Token Service Provider (TSP)

EMV Authorization with Tokenization

WIRED BRAIN
COFFEE

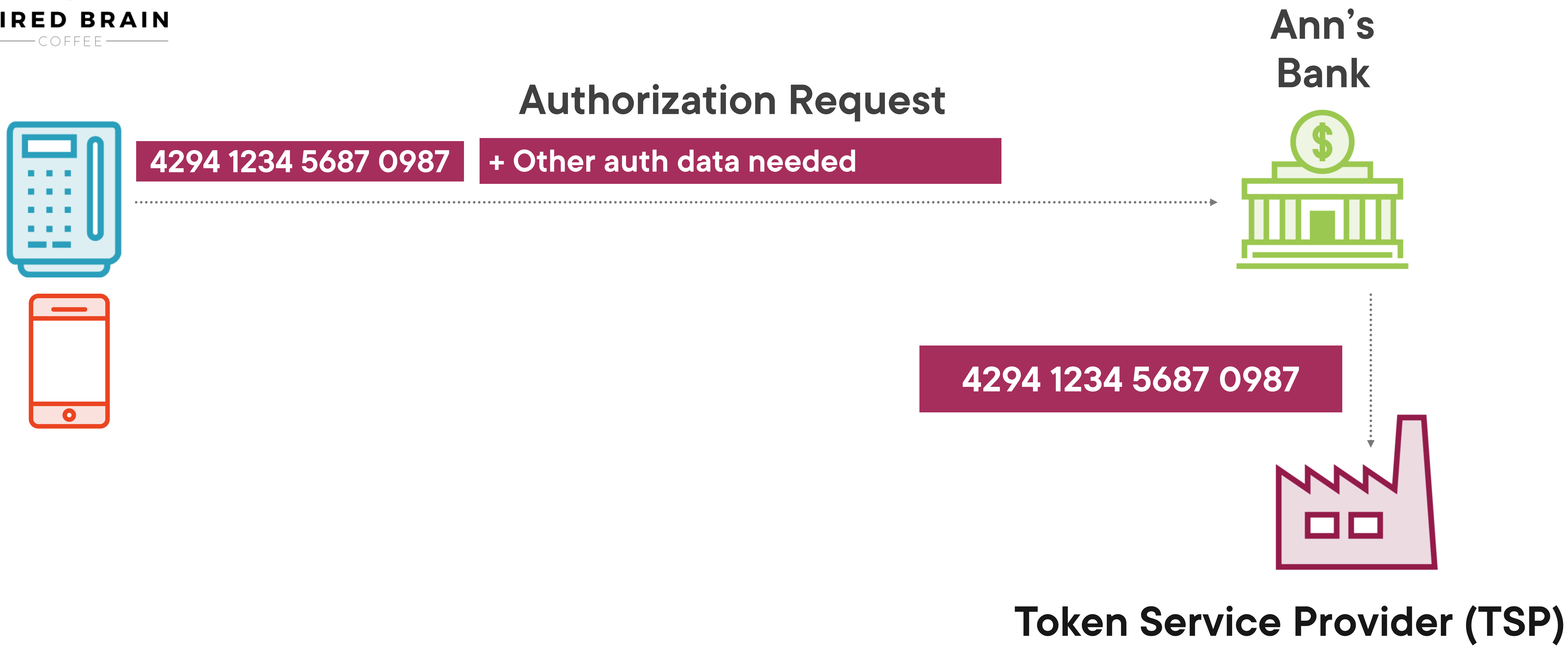


Authorization Request

4294 1234 5687 0987

+ Other auth data needed

EMV Authorization with Tokenization



Authorization Request

4294 1234 5687 0987

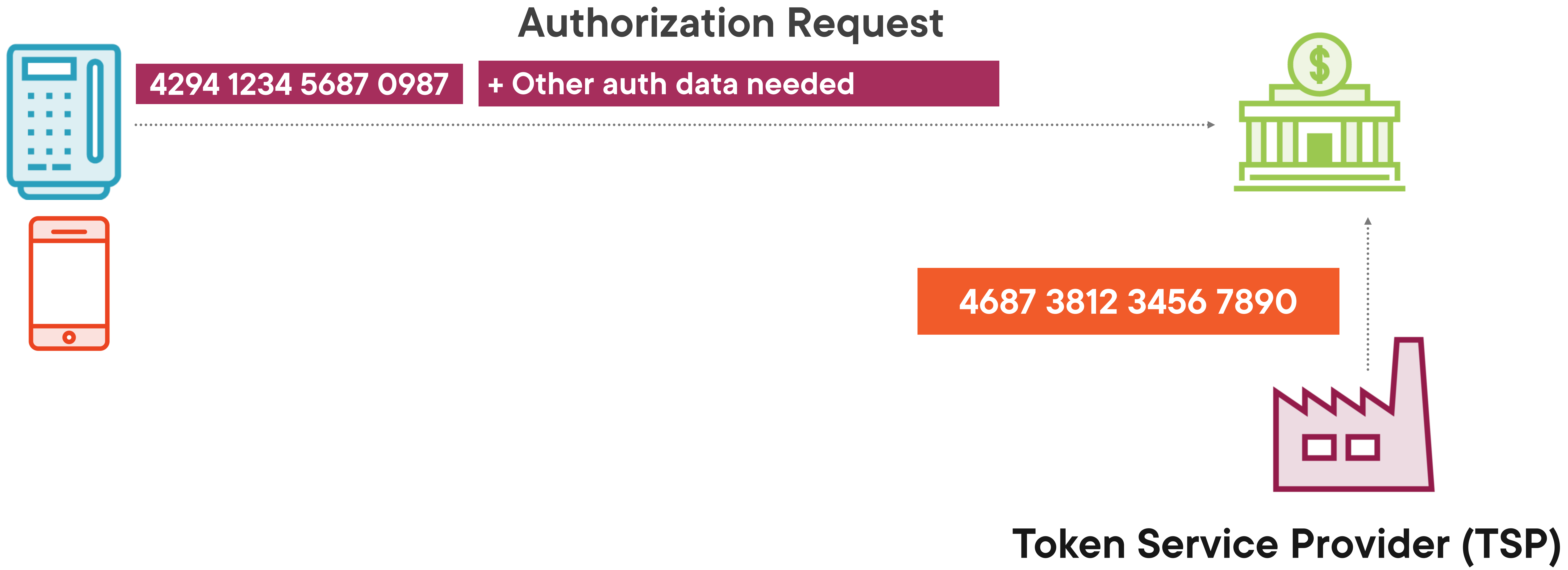
+ Other auth data needed

Ann's Bank

4294 1234 5687 0987

Token Service Provider (TSP)

EMV Authorization with Tokenization



Authorization Request

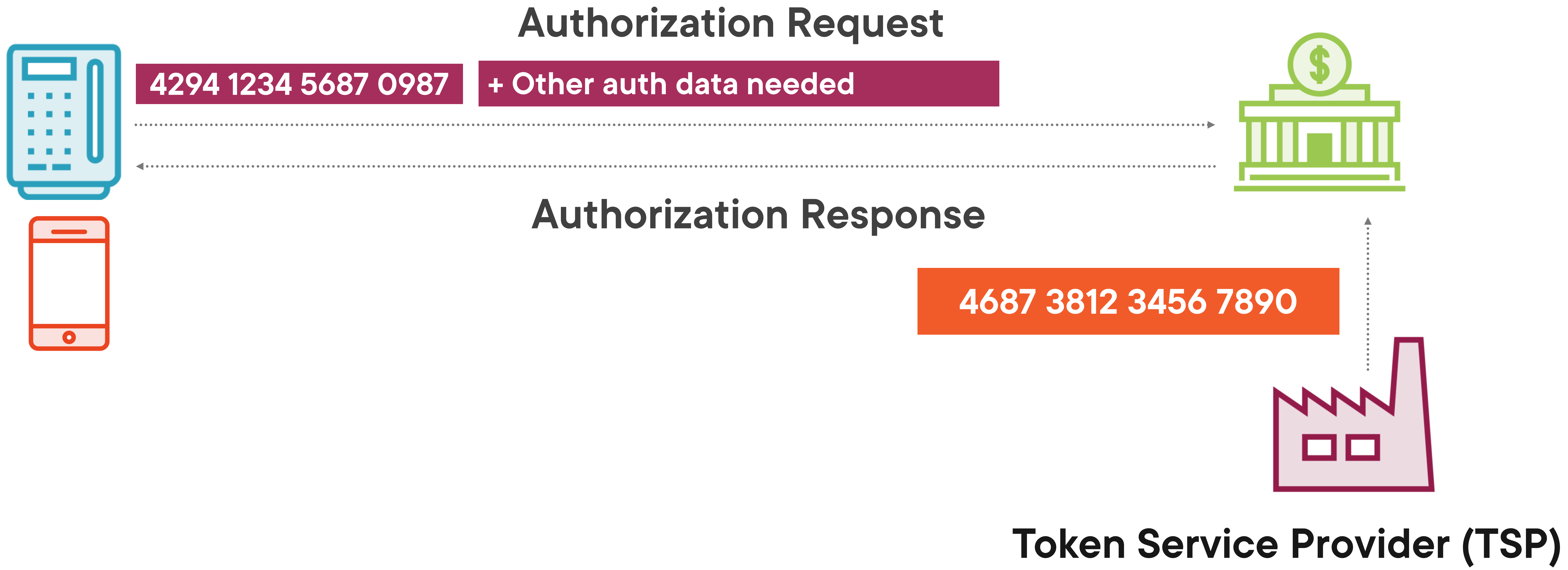
4294 1234 5687 0987

+ Other auth data needed

4687 3812 3456 7890

Token Service Provider (TSP)

EMV Authorization with Tokenization



Authorization Request

4294 1234 5687 0987

+ Other auth data needed

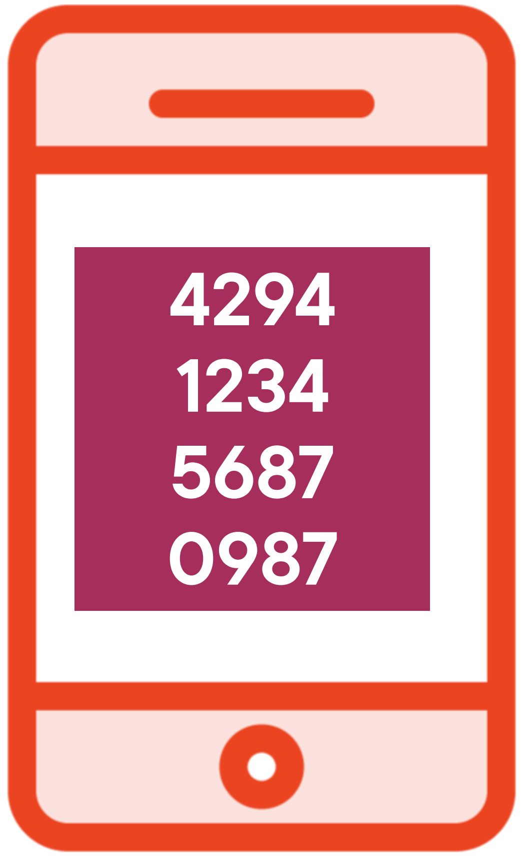
Authorization Response

4687 3812 3456 7890

Token Service Provider (TSP)

Authentication with Devices

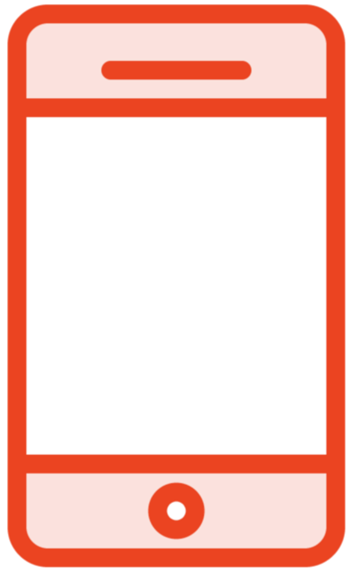
Validate the “Card”



Token
Does it match?

Chip Emulated in Device
iCVV correct?
Correct secret?

Validate the Cardholder

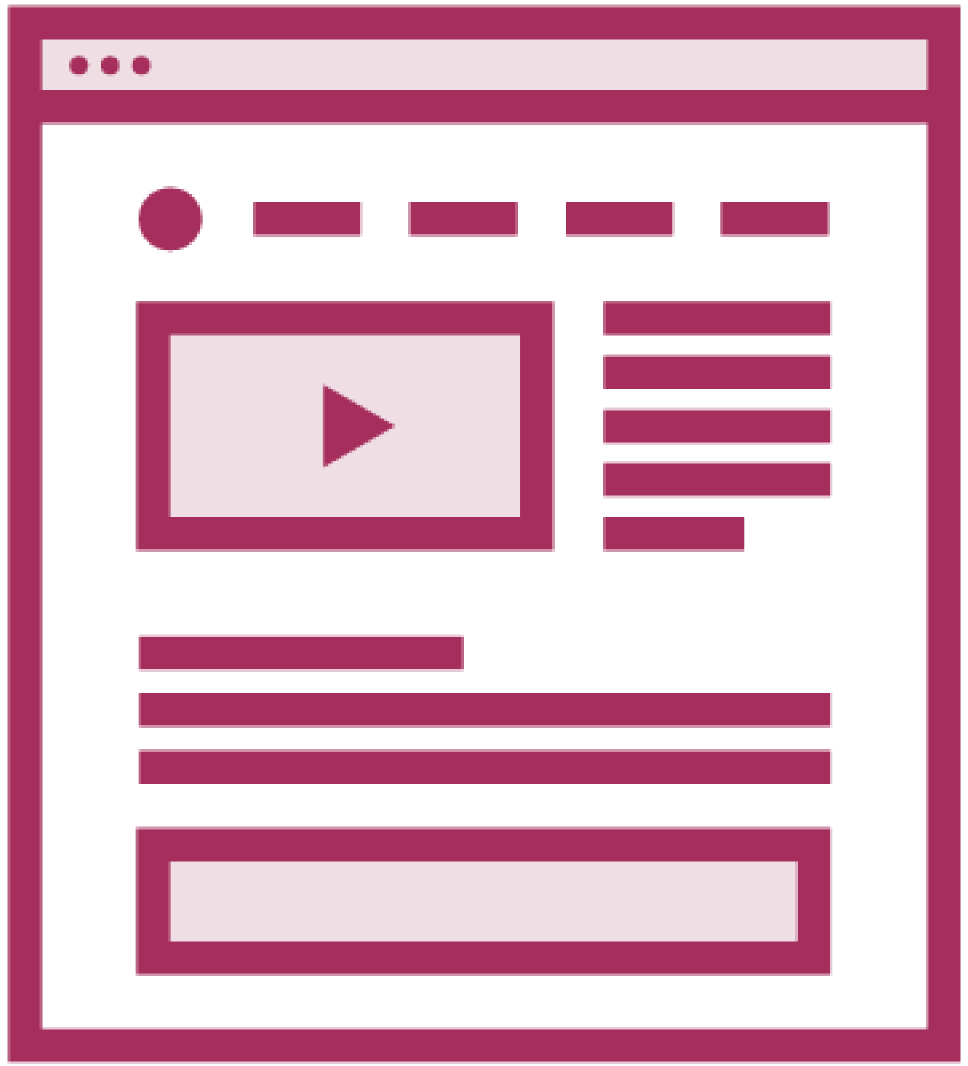


It’s OK – I’ve authenticated the human cardholder

Personal Identification Number (PIN) ****
For the device

Biometric
For the device

EMV 3 Domain Security (3DS) for E-commerce



Authenticate that the cardholder is making the transaction

Authentication happens in the issuer's domain

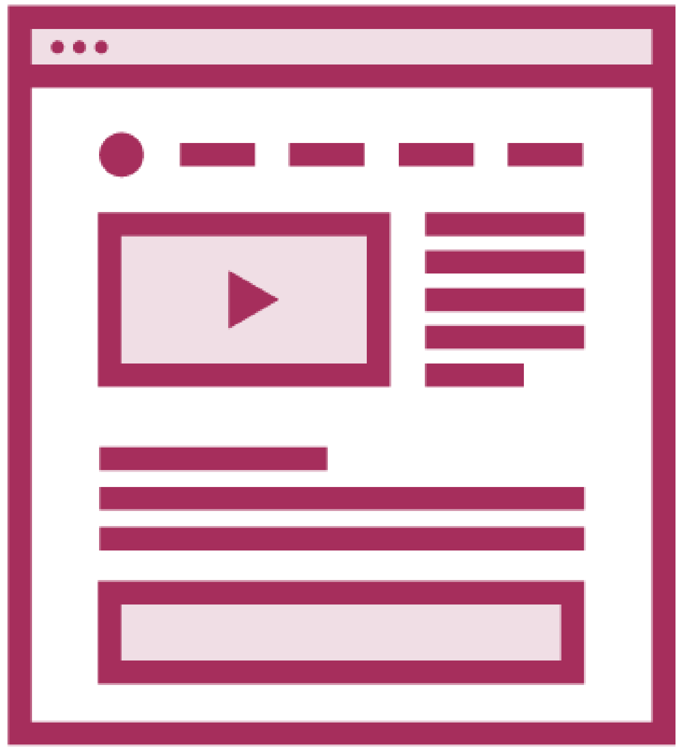
Each card brand has a different name for this:

- Mastercard: Identity Check
- Visa: Visa Secure
- American Express: SafeKey

E-commerce

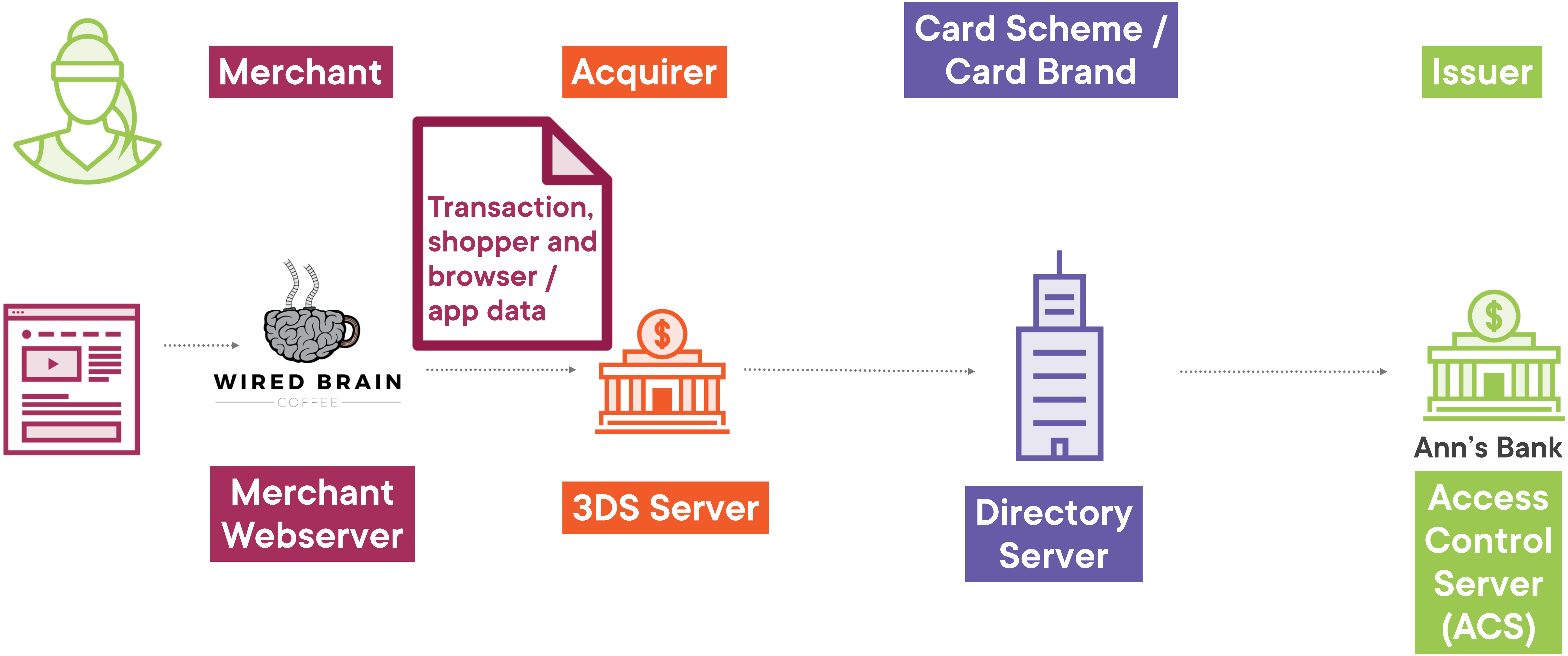
Ann Cardholder wants to buy some beans...

... using her payment card ...



... from the **Wired Brain Coffee** website

E-commerce Authentication



Merchant

Acquirer

Card Scheme / Card Brand

Issuer

Transaction, shopper and browser / app data

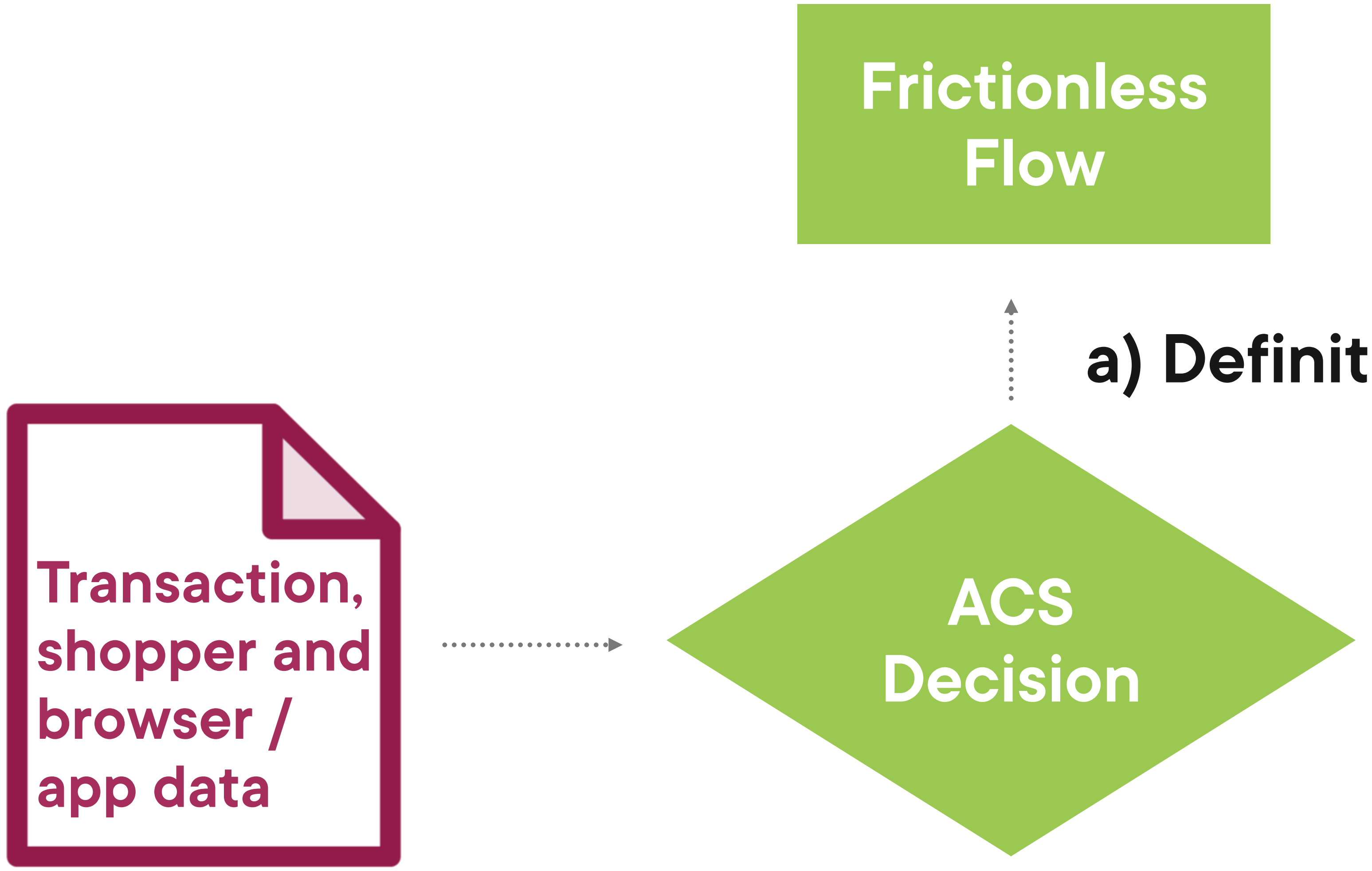
Merchant Webserver

3DS Server

Directory Server

Access Control Server (ACS)

The ACS Makes a Decision



Frictionless Flow

a) Definitely Ann

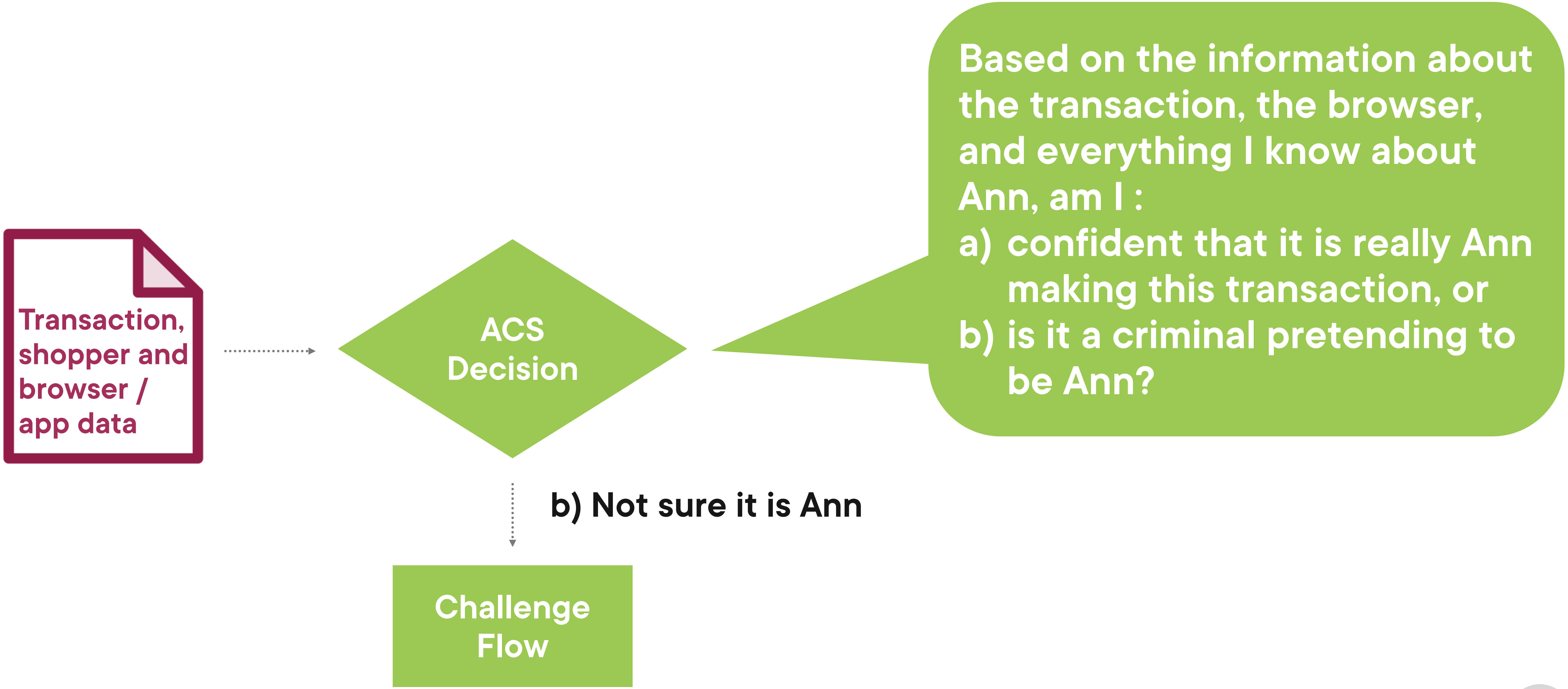
Transaction, shopper and browser / app data

ACS Decision

Based on the information about the transaction, the browser, and everything I know about Ann, am I :

a) confident that it is really Ann making this transaction, or
b) is it a criminal pretending to be Ann?

The ACS Makes a Decision



Transaction, shopper and browser / app data

ACS Decision

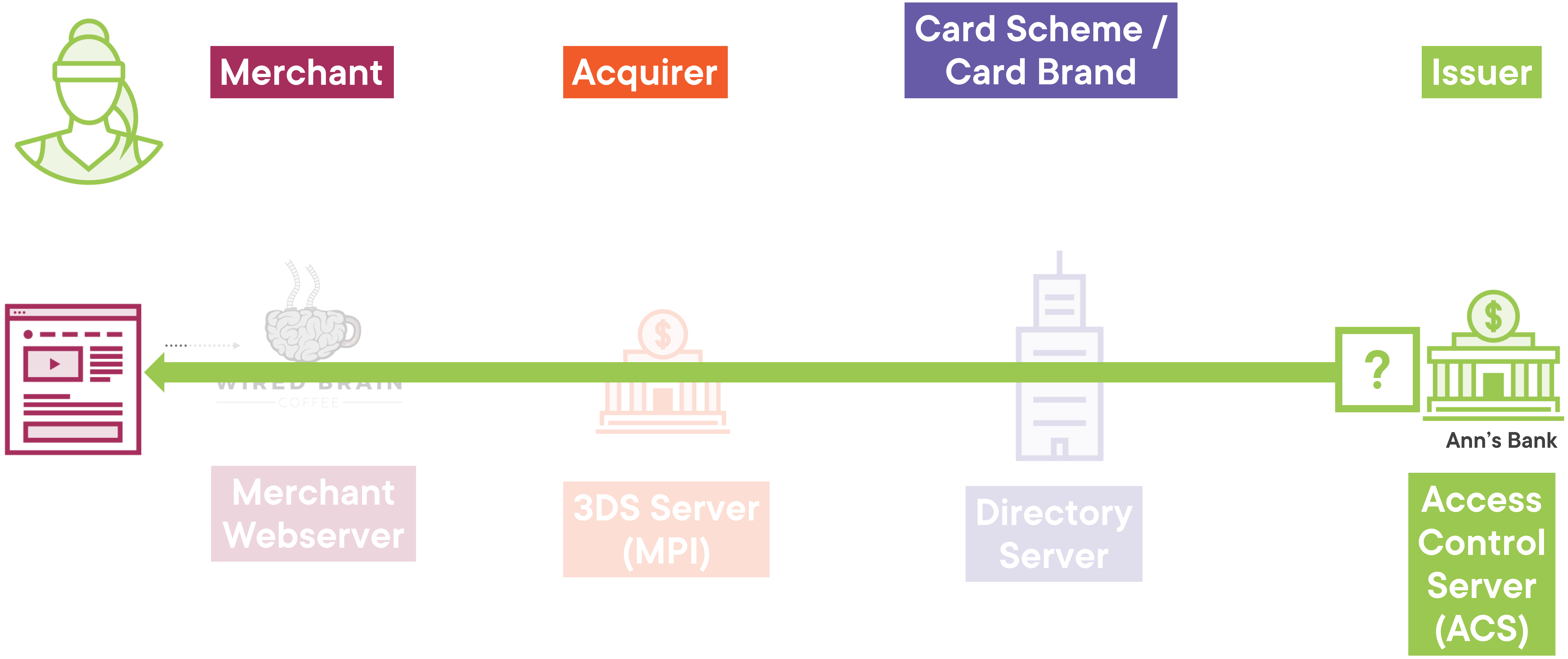
Based on the information about the transaction, the browser, and everything I know about Ann, am I :

a) confident that it is really Ann making this transaction, or
b) is it a criminal pretending to be Ann?

b) Not sure it is Ann

Challenge Flow

ACS Challenge



Merchant

Acquirer

Card Scheme / Card Brand

Issuer

Merchant Webserver

3DS Server (MPI)

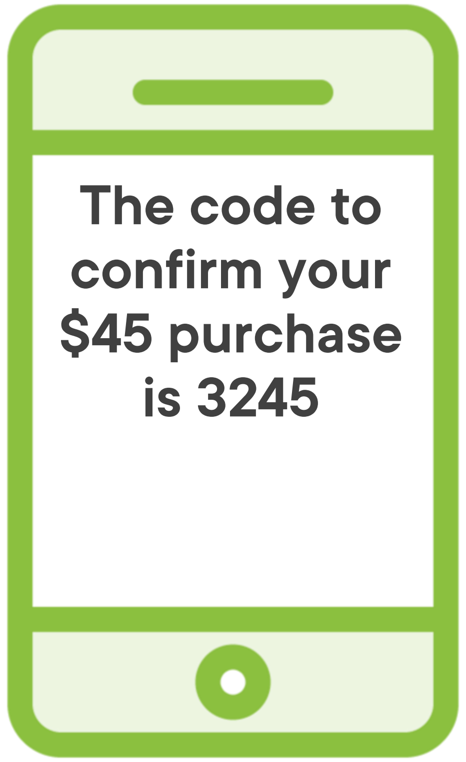
Directory Server

Access Control Server (ACS)

Typical Challenges

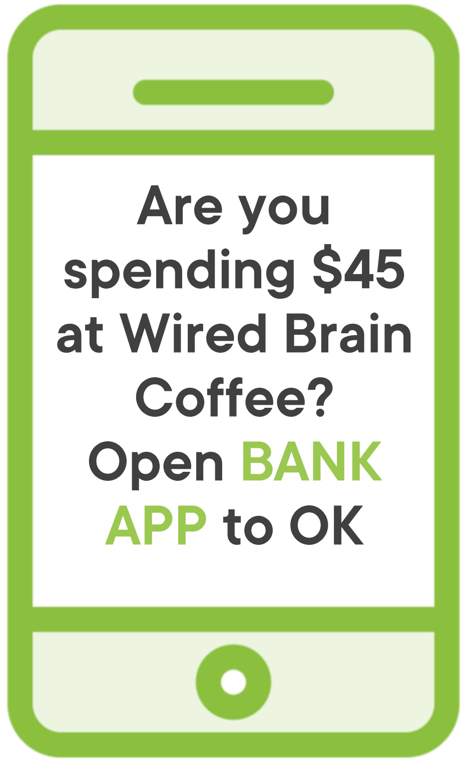
****

Memorized password



The code to confirm your $45 purchase is 3245

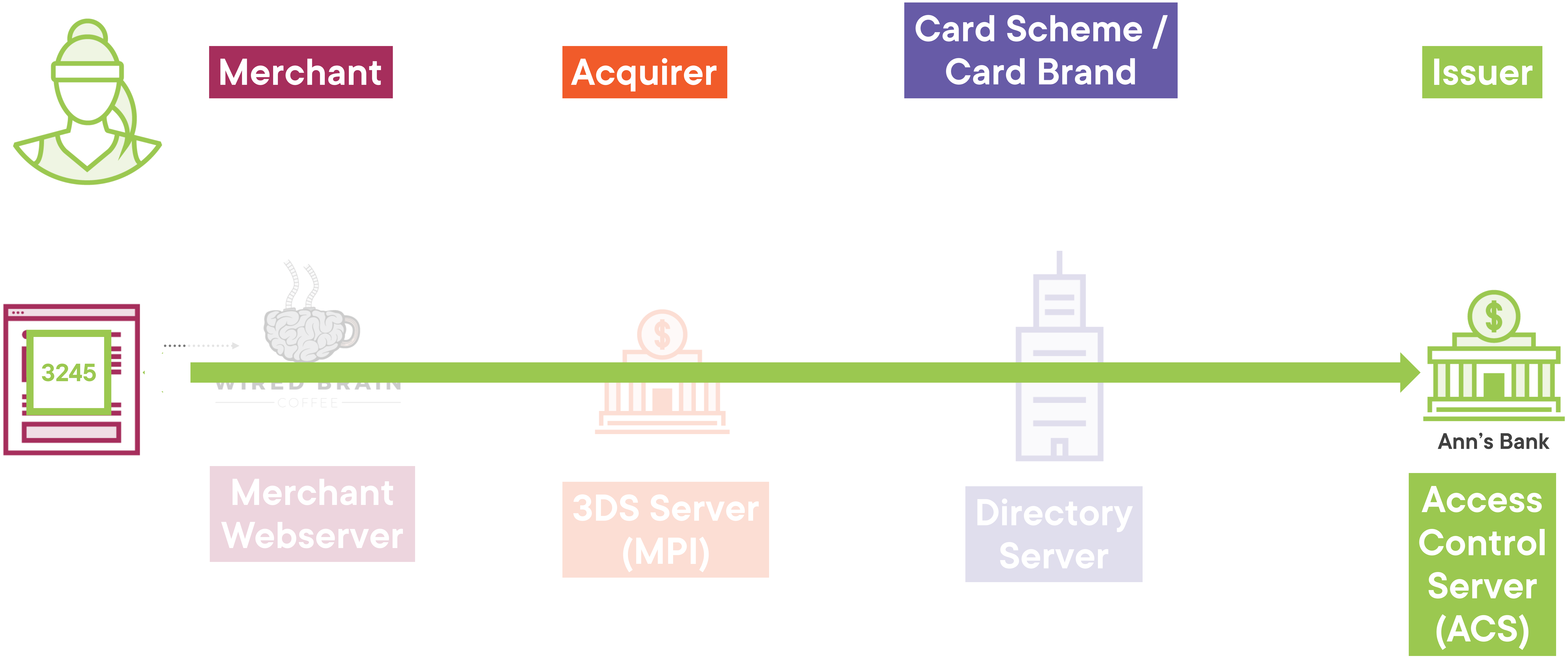
Text message to a known device



Are you spending $45 at Wired Brain Coffee? Open BANK APP to OK

Push notification to an app on a known device

ACS Challenge



Merchant

Acquirer

Card Scheme / Card Brand

Issuer

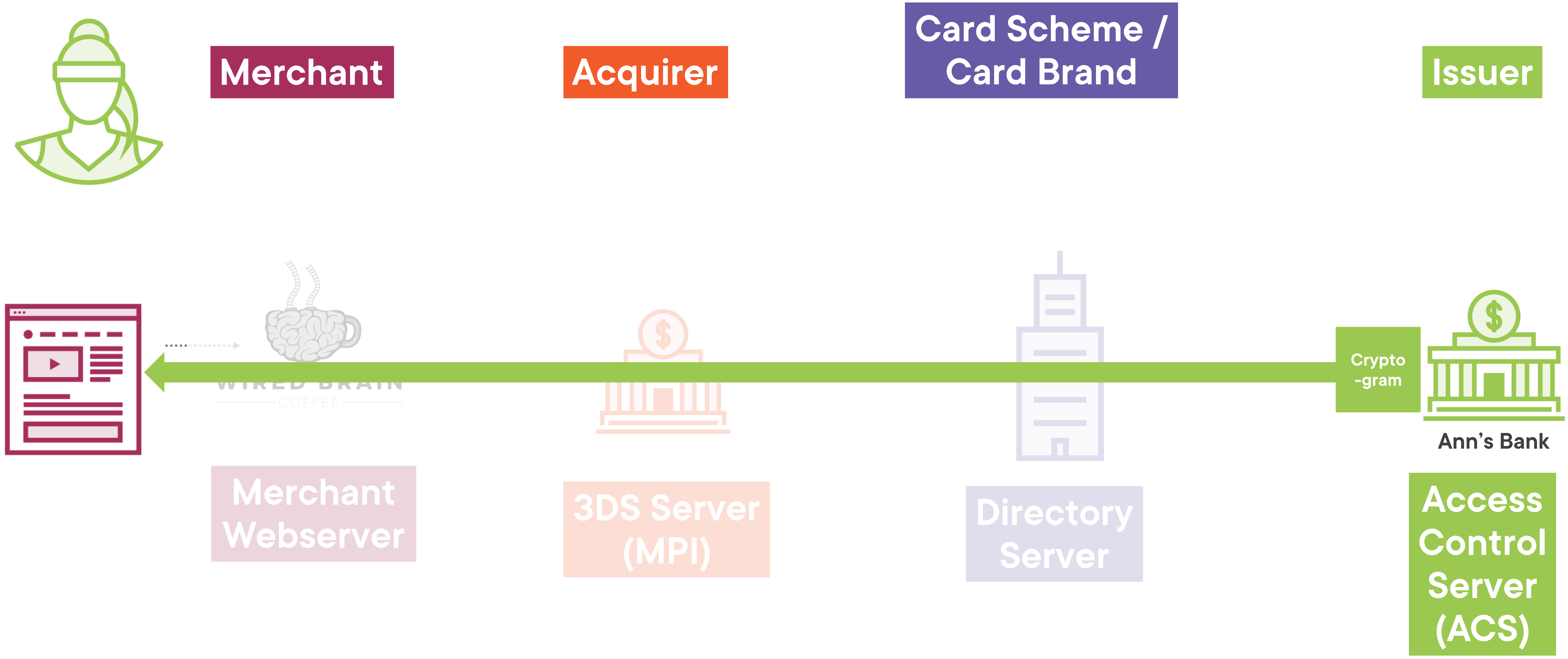
Merchant Webserver

3DS Server (MPI)

Directory Server

Access Control Server (ACS)

ACS Challenge



Merchant

Acquirer

Card Scheme / Card Brand

Issuer

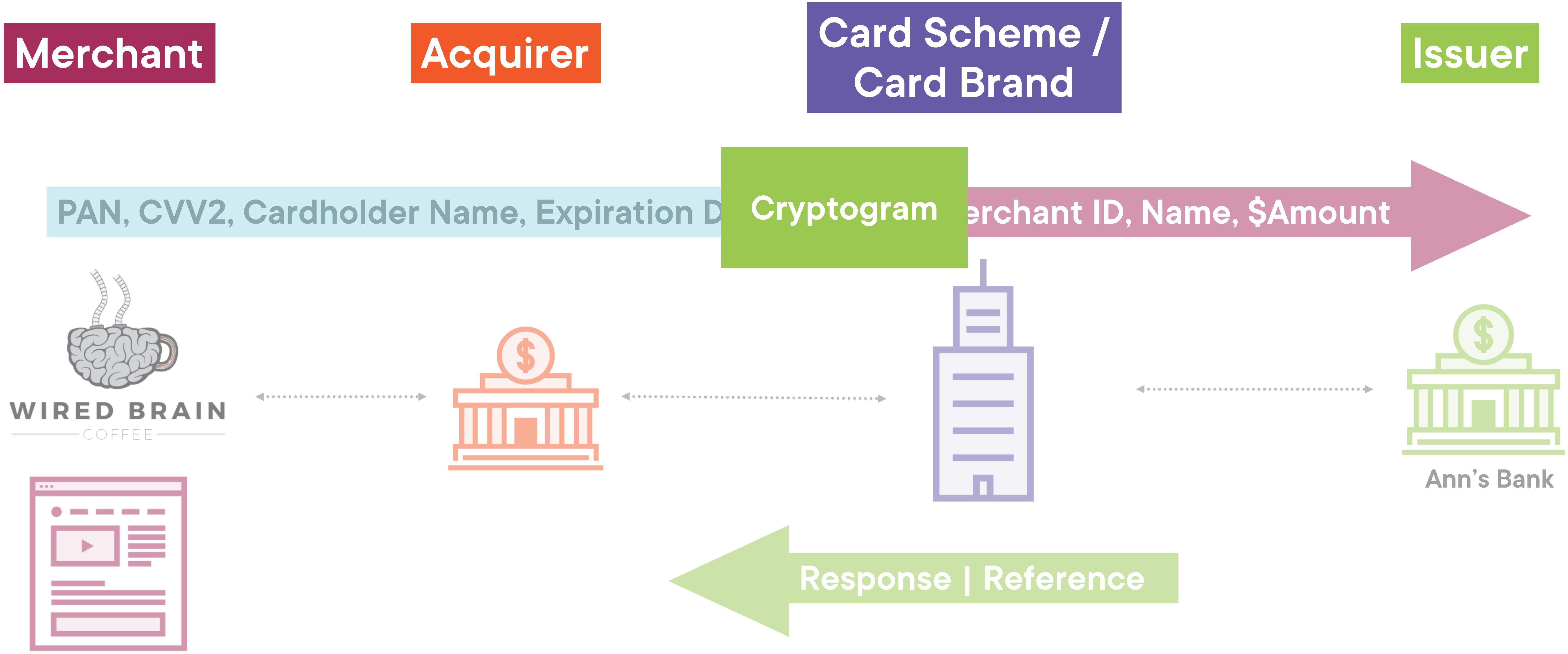
Merchant Webserver

3DS Server (MPI)

Directory Server

Access Control Server (ACS)

E-commerce Authorization After 3DS



Merchant

Acquirer

Card Scheme / Card Brand

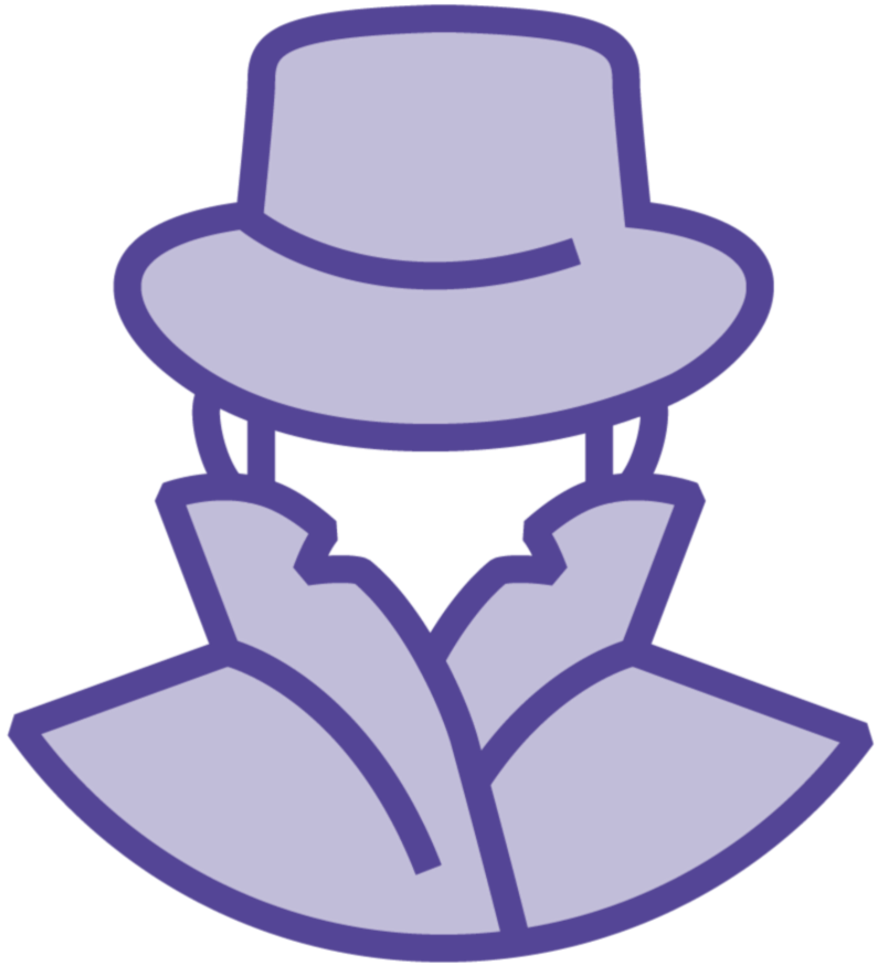
Issuer

PAN, CVV2, Cardholder Name, Expiration D

Cryptogram

erchant ID, Name, $Amount

Response | Reference



1. Physical cards and PINS
2. Fake cards made from stolen magnetic stripe data
3. Any stolen data that will get an e-commerce or MOTO transaction authorized