The PCI Payment Ecosystem

In-person Transactions

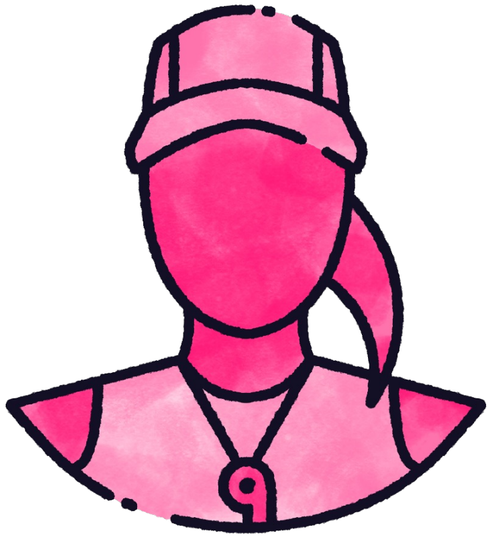


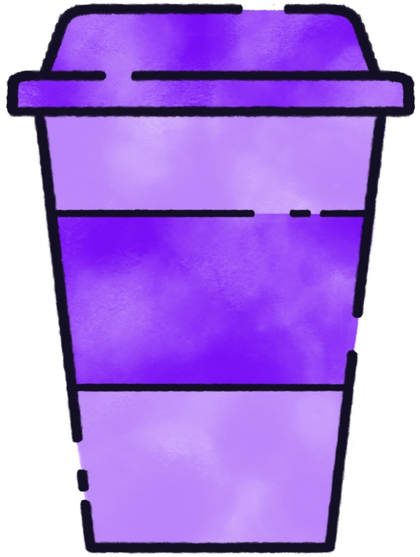
John Elliott

Payments, Security, Privacy, and Risk Specialist

@ withoutfire | pci.rocks

Have You Ever Wondered?





Card Statement
4687 38 **** 7980**

Pizza	$13.20
Rail fare	$56.87
Wired Brain Coffee	$ 5.10
Pluralsight	$29.99
Web hosting	$ 9.99
Total	$115.15

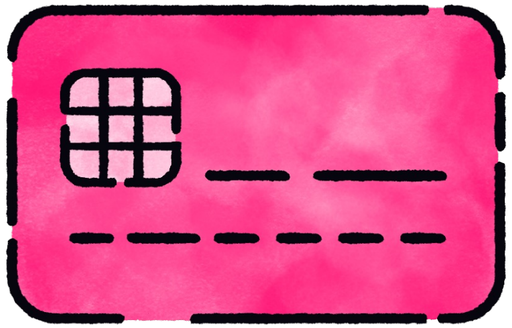
Ordering Coffee



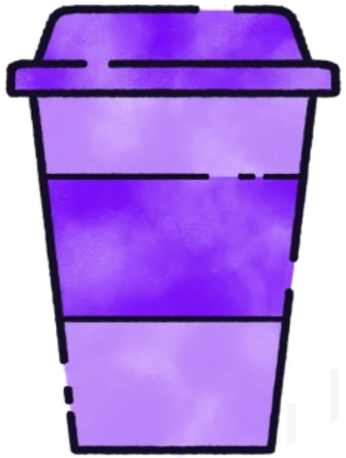
“I’ll have a large latte to go, please”



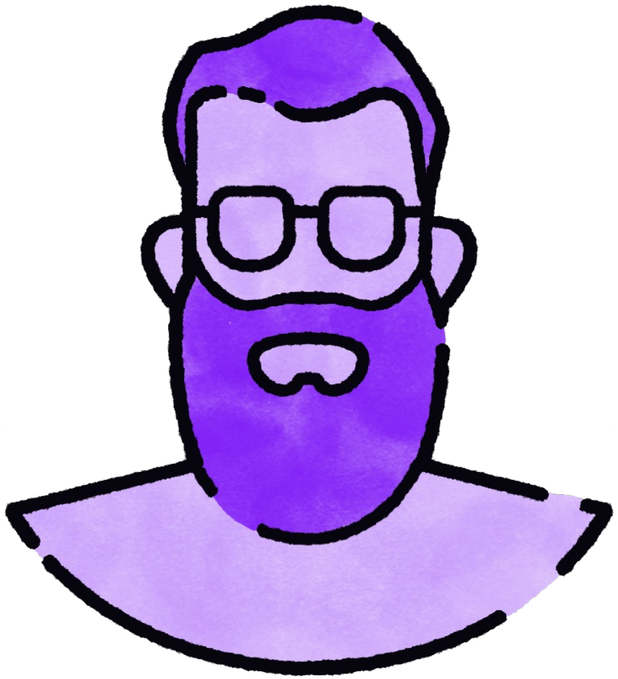
“That will be $5.10”



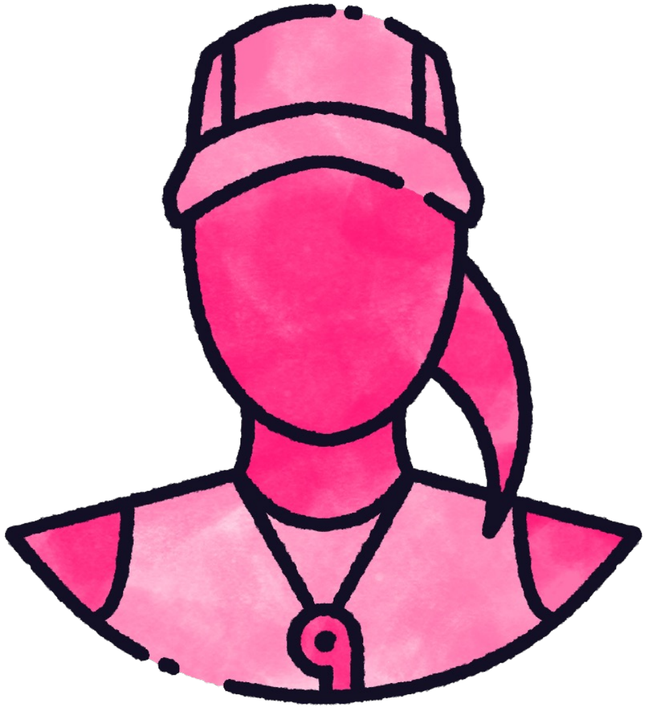
“I’ll pay by card...”



“Here you go”



Will Wired Brain Coffee be paid for this?



I need coffee
before starting work



1. Is it really Alice making the transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization



"Hello, it's Wired Brain Coffee here"

"Here is some data from one of your cards"

"Will you give me $5.10 later?"



"OK, here's our answer"

Will Wired Brain Coffee be paid for this?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization



Authorization request

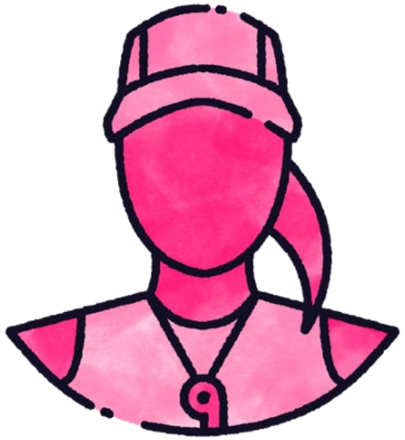
Authorization response



Will Wired Brain Coffee be paid for this?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Payment Ecosystem Terms



Cardholder

(Alice)



Issuer
or Issuing Bank

(Alice's bank)



Merchant

(Wired Brain Coffee)

Ways to Use the Card

Swipe

Dip

Tap

Who Has What?





Cardholder

(Alice)



We owe you $5.10

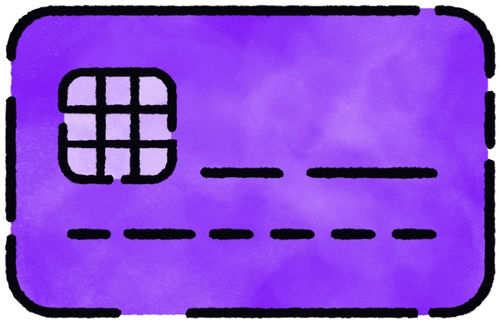


Alice’s bank

Merchant

(Wired Brain Coffee)

No Longer Just Cards



Traditional cards



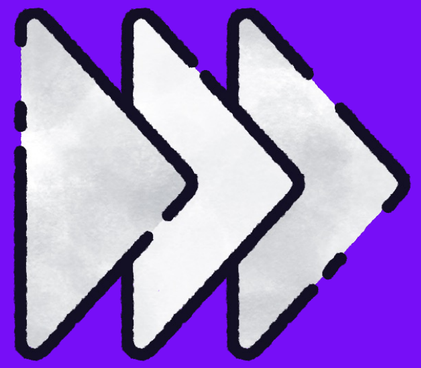
Smartphones



Smart devices



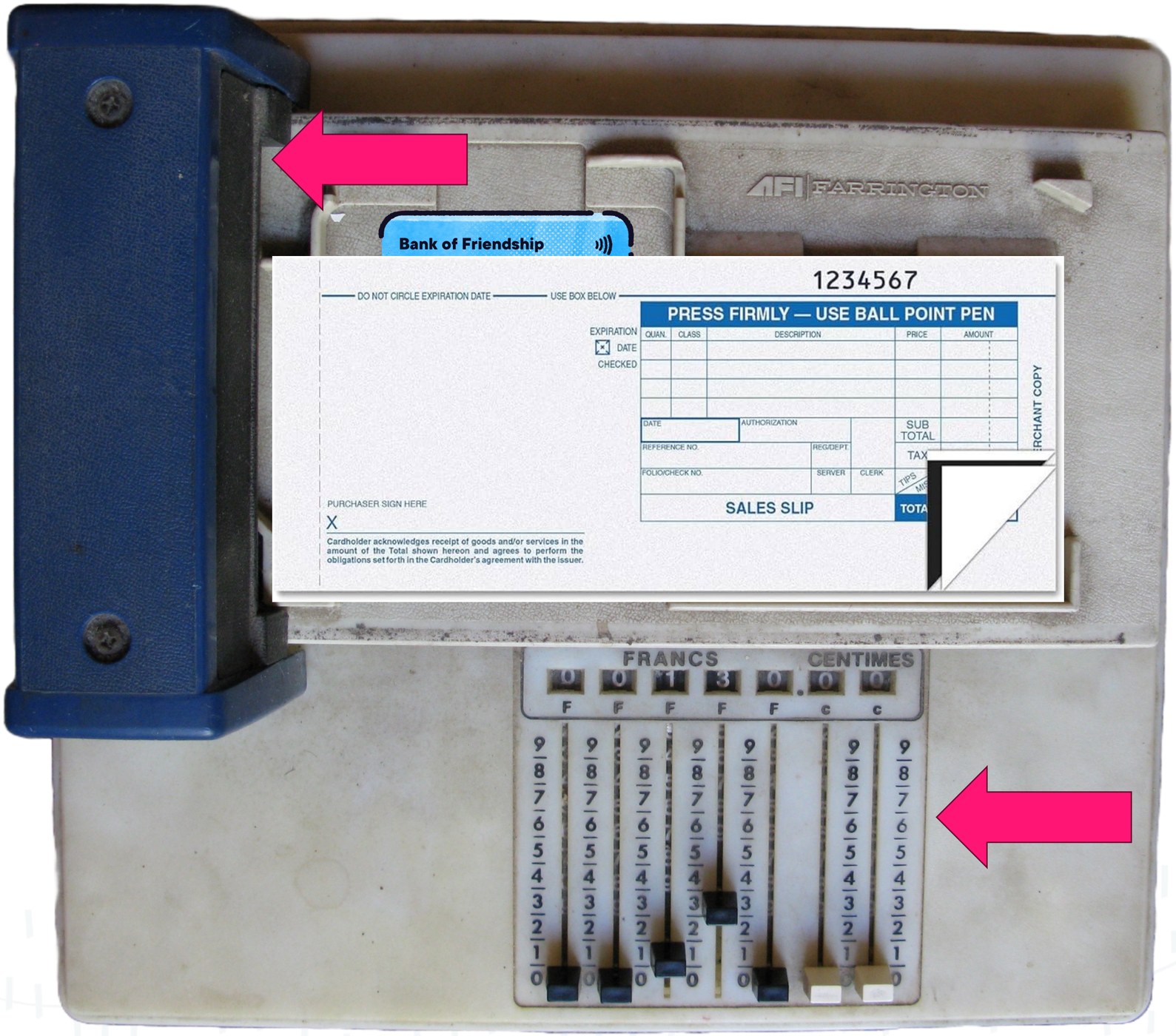
Things Are Different



Pace of Change

The Data on a Traditional Payment Card




AFI FARRINGTON
Bank of Friendship
1234567
DO NOT CIRCLE EXPIRATION DATE
USE BOX BELOW
PRESS FIRMLY — USE BALL POINT PEN
EXPIRATION DATE
CHECKED
QUAN.
CLASS
DESCRIPTION
PRICE
AMOUNT
DATE
AUTHORIZATION
SUB TOTAL
REFERENCE NO.
REG/DEPT.
TAX
FOLIO/CHECK NO.
SERVER
CLERK
TIPS
SALES SLIP
PURCHASER SIGN HERE
X
Cardholder acknowledges receipt of goods and/or services in the amount of the Total shown hereon and agrees to perform the obligations set forth in the Cardholder's agreement with the issuer.
MERCHANT COPY
FRANCS
CENTIMES
0 0 1 3 0 . 0 0
F F F F F C C

The Data on a Traditional Payment Card



The Data on a Modern Payment Card



The Data on a Modern Payment Card



And in the Future



The magnetic stripe will be removed by 2030 for most cards

Authorization



Authorization request

Authorization response

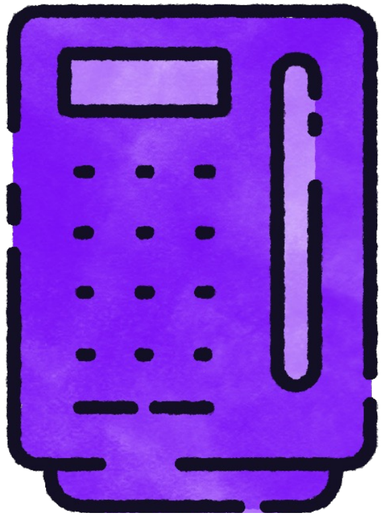


Will Wired Brain Coffee
be paid for this?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

The Chip and Terminal Exchange Data

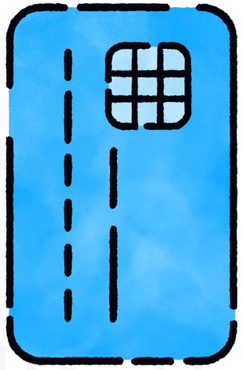
Here's some data for you



Sends authorization request

Receives authorization response

Thanks, here's some data you need to add to the authorization request



Authorization Request



Authorization Request

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	Encrypted PIN?

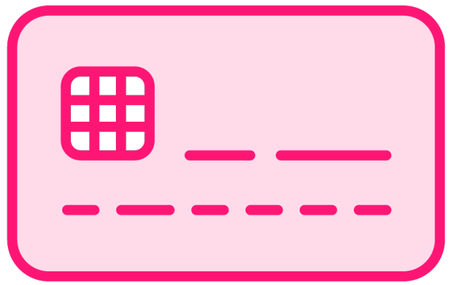
1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization Request

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	Encrypted PIN?

1. Is it really Alice making that transaction?

Authentication of a Chip Transaction by the Cardholder



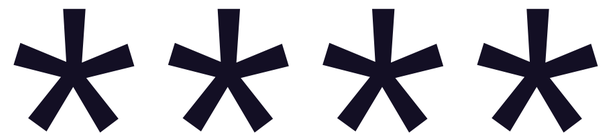
****

The chip: something Alice has

(which can not be copied)

The PIN: something Alice knows

(which is a shared secret between Alice and the card issuer)



Some transactions don’t require a PIN

- Depends on location
- Depends on card brand

Balances

- Ease of use of card payments
- Risk of fraudulent use (e.g. a stolen card)

Authorization Request

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	Encrypted PIN?

1. Is it really Alice making that transaction?
2. Is it the real card?

Authorization Request – Offline PIN

							PIN verified

1. Is it really Alice making that transaction?
2. Is it the real card?

Authorization Request

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	Encrypted PIN?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?

Authorization Request

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	Encrypted PIN?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization Request – Chip with PIN

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	Encrypted PIN

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization Request – Chip without PIN

PAN	Exp. Date	iCVV	Amount	Merchant Code & ID	Terminal ID	Cryptogram	

1. Is it really Alice making that transaction?	
2. Is it the real card?	
3. Does Alice have enough money or credit?	
4. Is it an allowed transaction?	

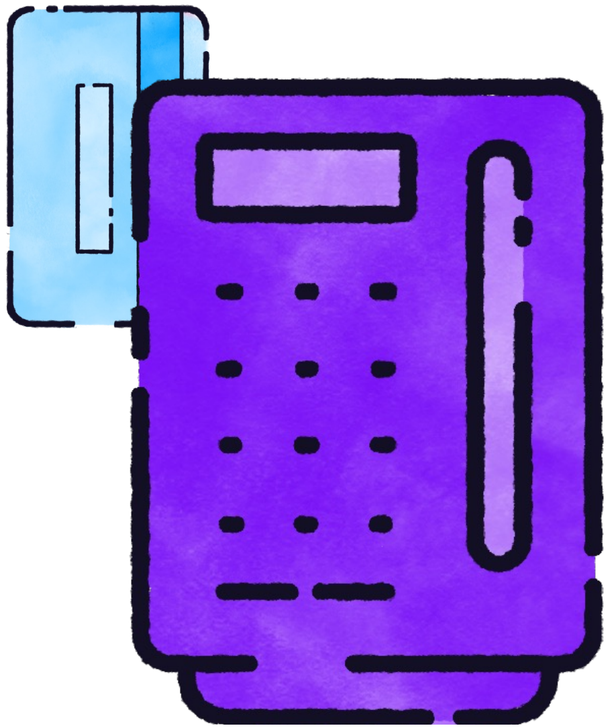
Authorization Response



Response	Reference	Cryptogram

1. Was it really authorized?

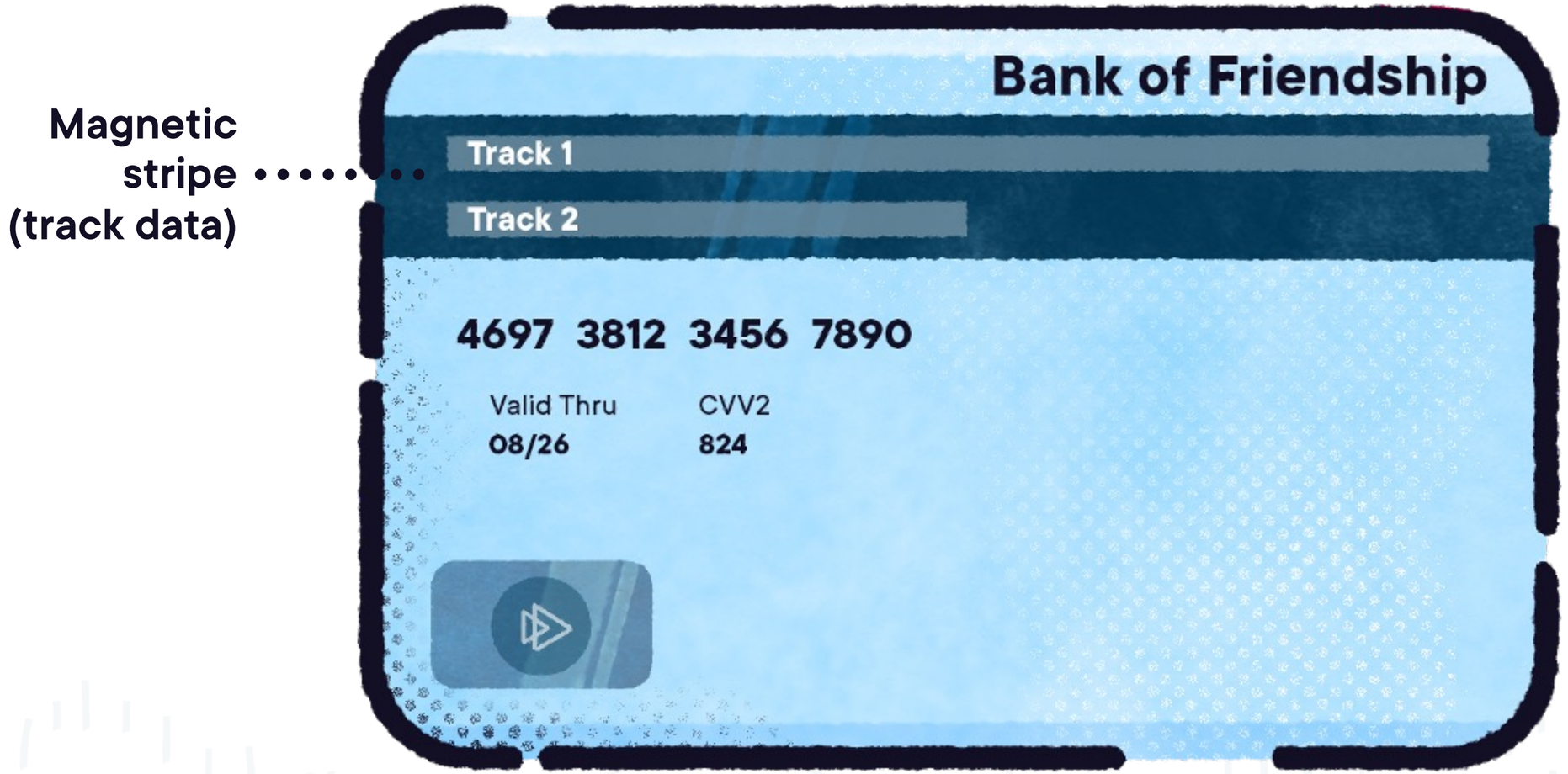
The Terminal Reads the Magnetic Stripe



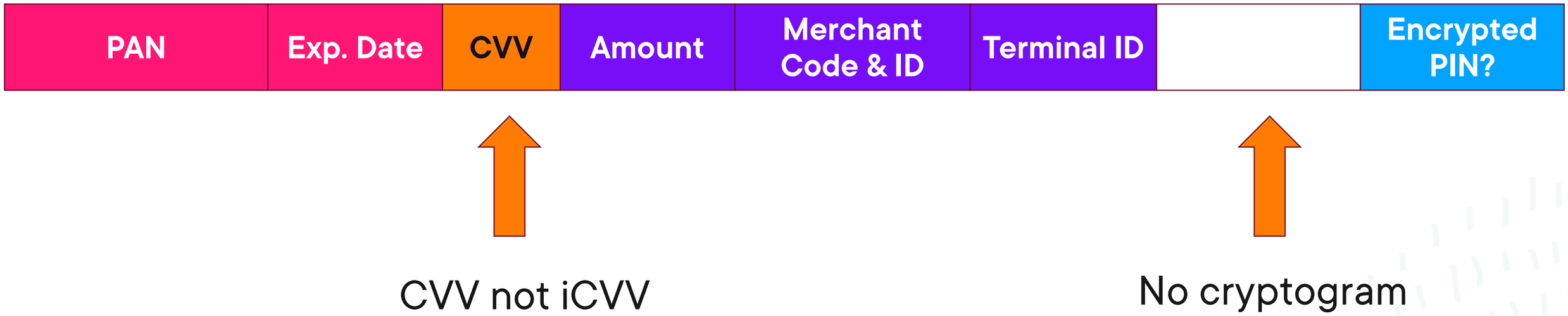
Sends authorization request

Receives authorization response

What About Magnetic Stripe Transactions?



Authorization Request

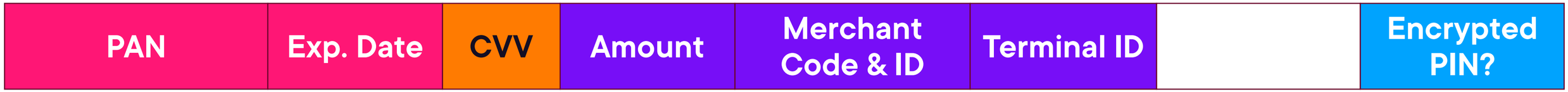


Authorization Request

PAN	Exp. Date	CVV	Amount	Merchant Code & ID	Terminal ID		Encrypted PIN?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization Request



1. Is it really Alice making that transaction?

Authorization Request

PAN	Exp. Date	CVV	Amount	Merchant Code & ID	Terminal ID		Encrypted PIN?

1. Is it really Alice making that transaction?
2. Is it the real card?

Authorization Request

PAN	Exp. Date	CVV	Amount	Merchant Code & ID	Terminal ID		Encrypted PIN?

1. Is it really Alice making that transaction?
2. Is it the real card?
3. Does Alice have enough money or credit?
4. Is it an allowed transaction?

Authorization Request – Magnetic Stripe with PIN

PAN	Exp. Date	CVV	Amount	Merchant Code & ID	Terminal ID		Encrypted PIN

1. Is it really Alice making that transaction?	✓
2. Is it the real card?	✗
3. Does Alice have enough money or credit?	✓
4. Is it an allowed transaction?	✓

Authorization Request – Magnetic Stripe without PIN

PAN	Exp. Date	CVV	Amount	Merchant Code & ID	Terminal ID		

1. Is it really Alice making that transaction?	
2. Is it the real card?	
3. Does Alice have enough money or credit?	
4. Is it an allowed transaction?	

Authorization Response



Response	Reference	

1. Was it really authorized?

Authorization Request

Chip	vs	Magnetic Stripe
iCVV Cryptogram May have: Encrypted PIN May have: Confirmation of correct PIN		CVV May have: Encrypted PIN

What Data Is Used For

PAN	Exp. Date	Cardholder name

Data used to identify the cardholder

Account Data

iCVV	iCVV	CVV2



Data used to authenticate the card

Encrypted PIN

Data used to authenticate the cardholder

Sensitive Authentication Data (SAD)

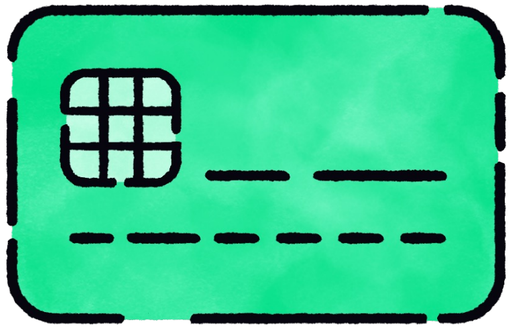
Chad Orders a Tea



“I’d like a cup of tea”



“That will be $4.50”



“I’ll pay by card...”



“Here you go”

Authorization



"Hello, it's Wired Brain Coffee here"

"Here is some data from one of your cards"

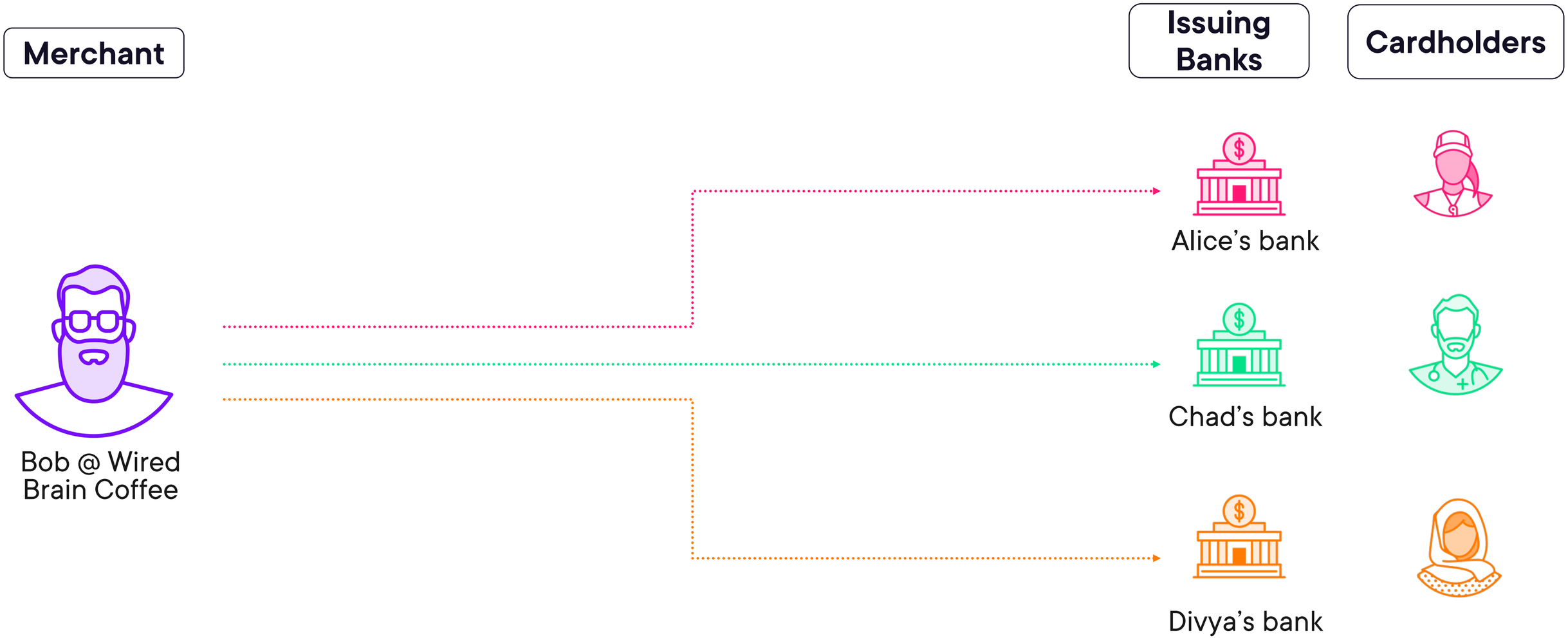
"Will you give me $4.50 later?"



"OK, here's our answer"

1. Is it really Chad making that transaction?
2. Is it the real card?
3. Does Chad have enough money or credit?
4. Is it an allowed transaction?

Authorization in Practice



Authorization in Practice

Merchant

Acquirer

Issuing Banks

Cardholders



Bob @ Wired Brain Coffee



Acquirer
Acquiring Bank
Merchant Acquirer
Merchant Processor



Alice's bank





Chad's bank

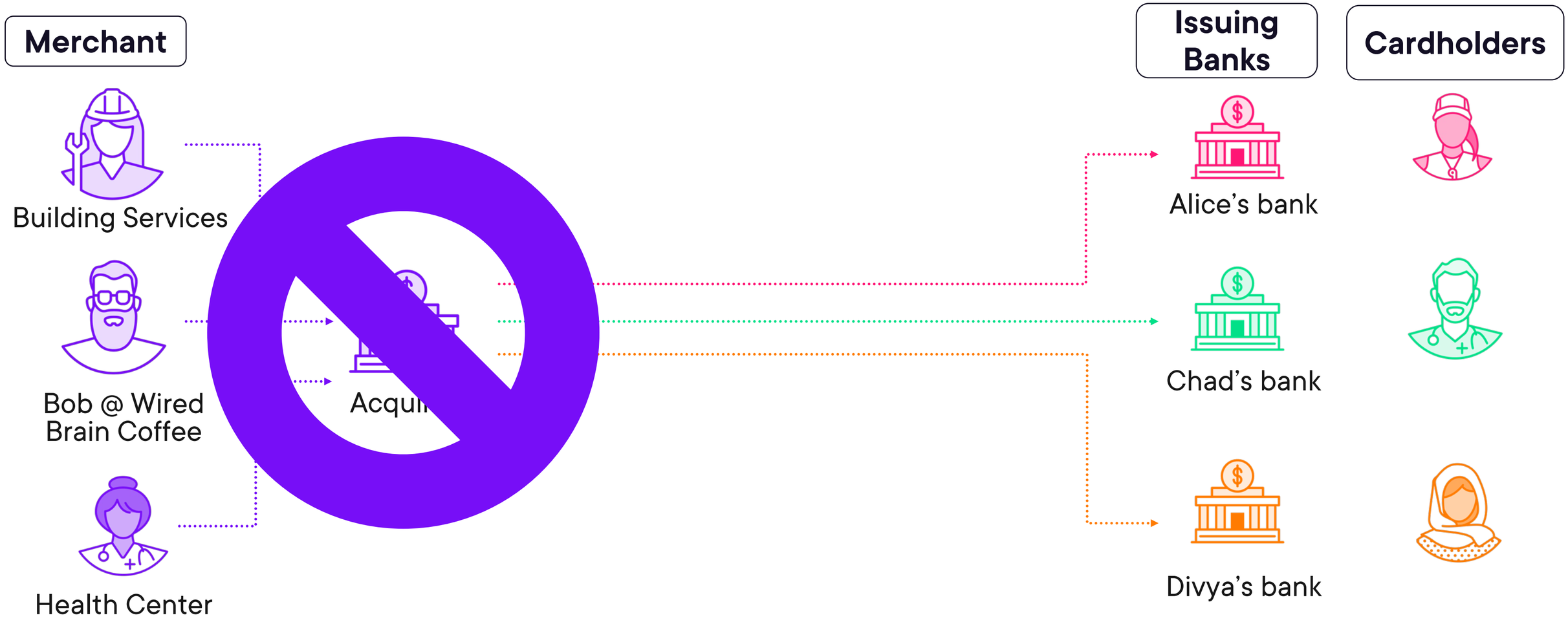




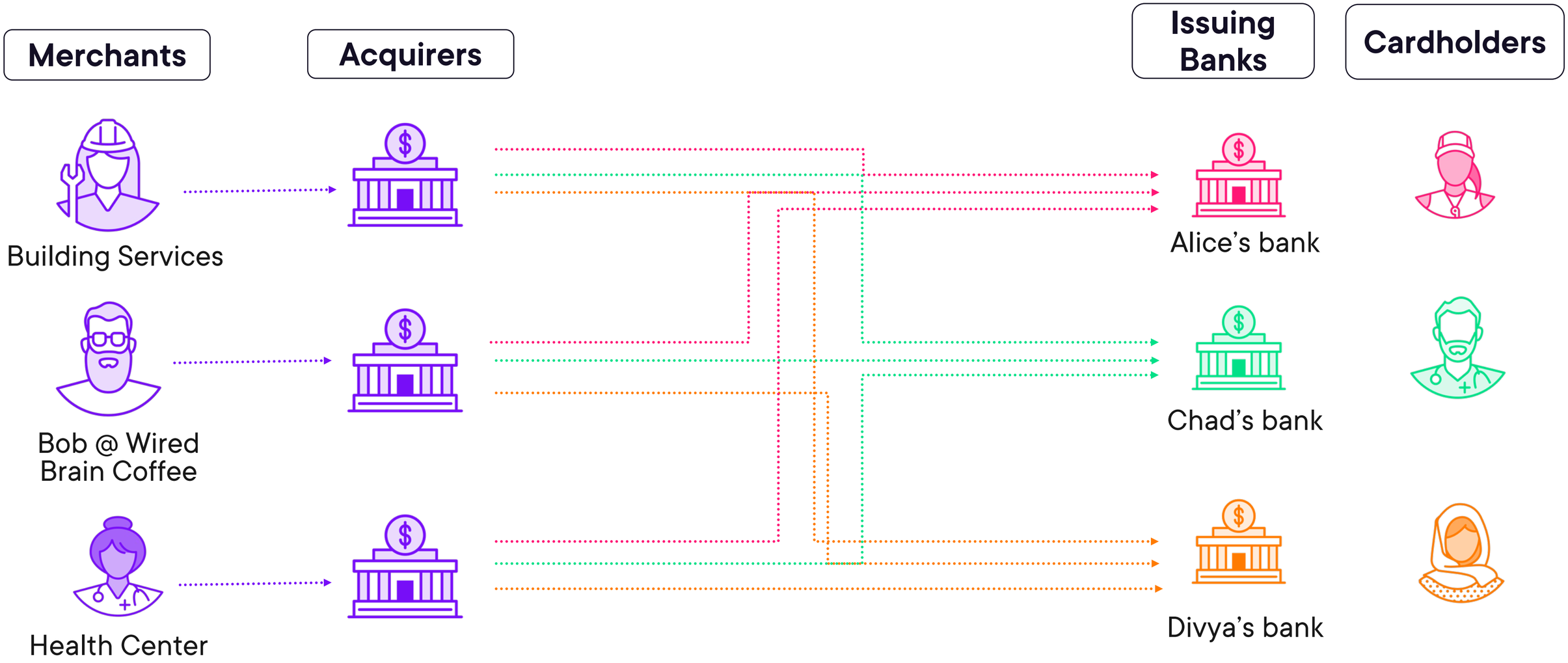
Divya's bank



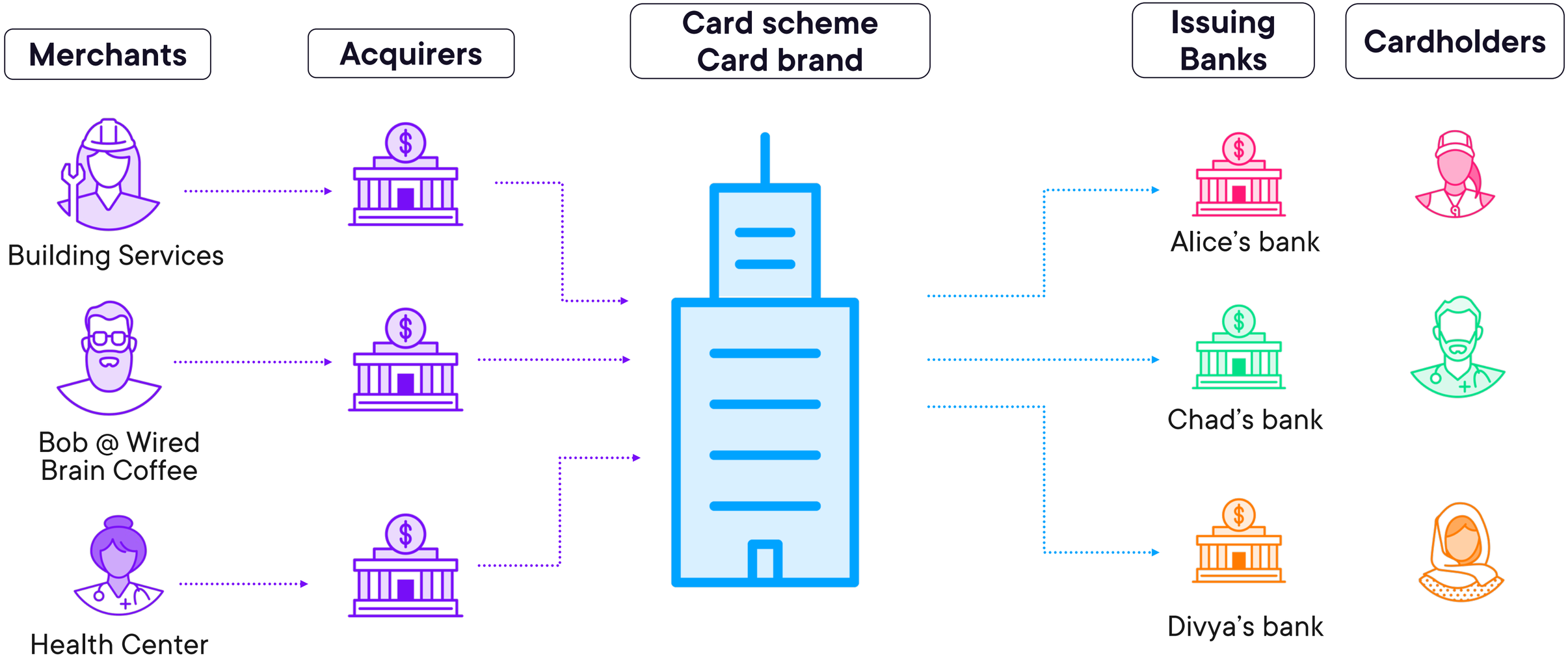
Multiple Merchants?



Multiple Merchants, Multiple Acquirers?



Card Brands / Schemes



Message Flow: Authorization



Cardholder



Merchant



Acquirer



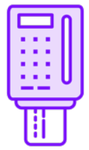
Card brand



Issuer



Taps or dips card



Authorization request

Which brand?

Authorization request

Which issuer?

Authorization request

Authorize?

Reserve funds in cardholder's account

Authorization Response

Which acquirer?

Authorization Response

Which merchant?

Authorization Response

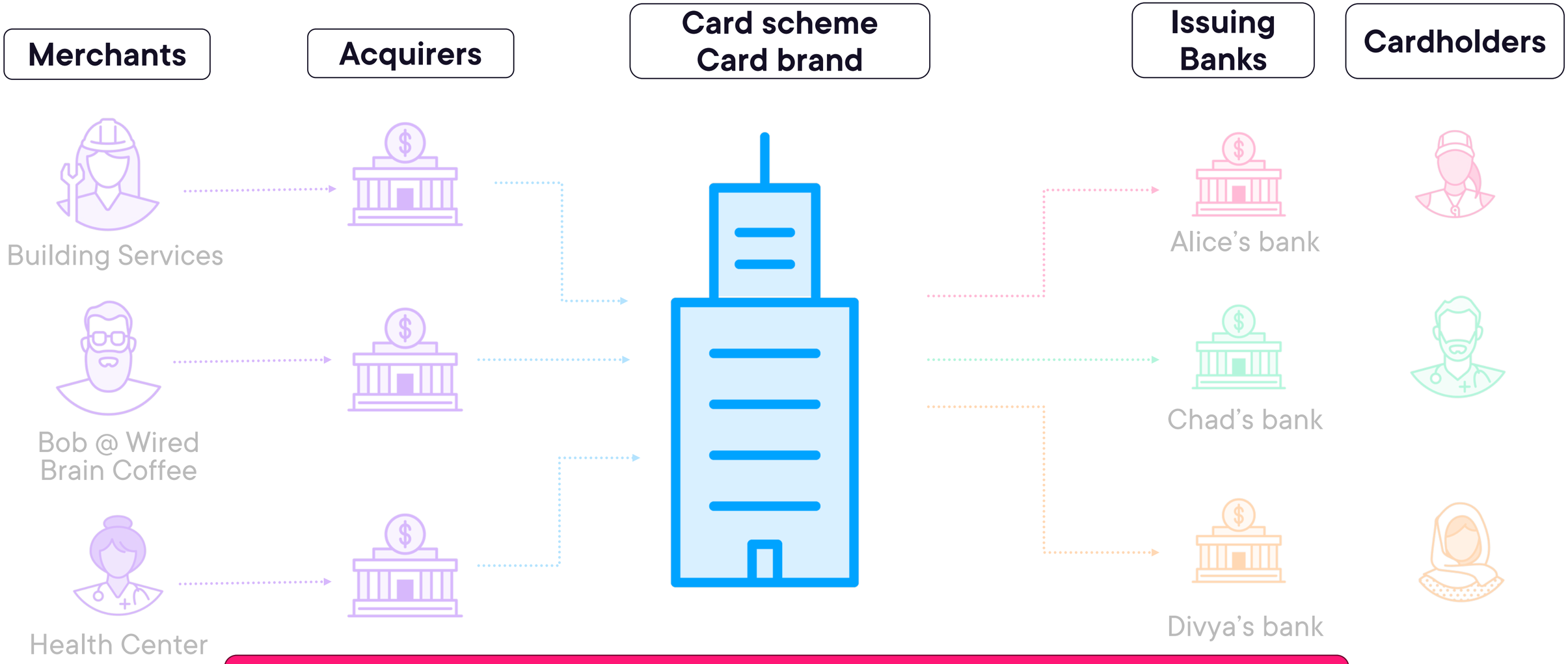


Receives coffee



Authorized

Card Brands / Schemes



Four-party model | Mastercard, Visa

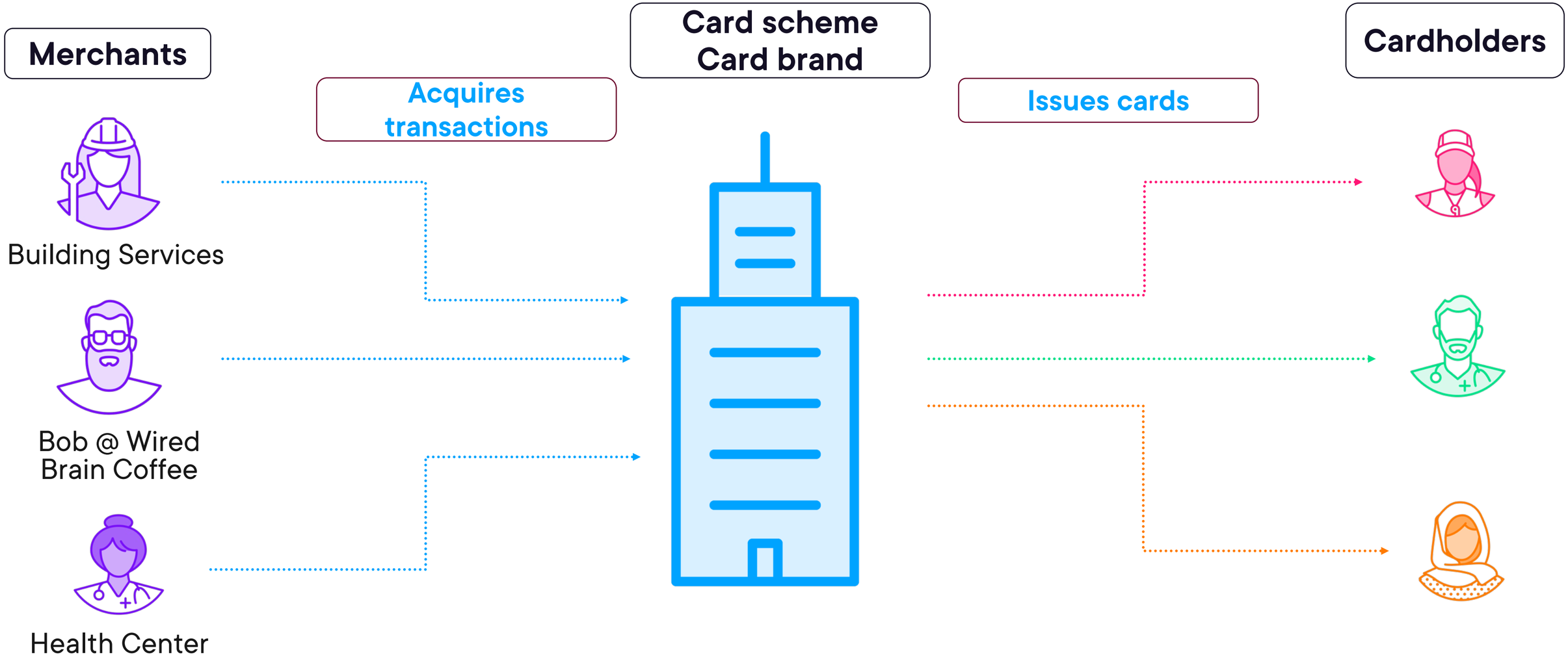


Things Are Different

Depending where you are in the world.

Depending how payment systems evolved.

Card Brands / Schemes



Three-party model | American Express

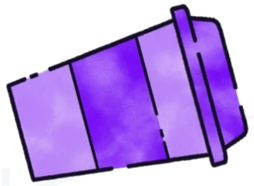
Where Did We Get To?

Alice has drunk her coffee



Cardholder

(Alice)





Merchant

(Wired Brain Coffee)

Bob has an IOU!

We owe you $5.10



Alice's bank

The Three Stages of Card Payments

Authorization

Secures funds

Clearing

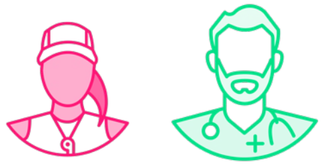
Reconciliation

Settlement

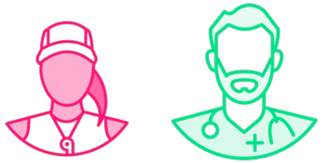
Money moves

Clearing (Four-party)

Cardholders | **Merchants** | **Acquirers** | **Card scheme Card brand** | **Issuing Banks**



Alice & Chad buy a coffee from Bob



Alice & Chad pay for parking at the health center

```
4242 4242 1234 5678   A5555  $5.55
4000 4000 9876 5432   A9999  $9.99
```



```
4242 4242 1234 5678   A1111  $11.11
4000 4000 9876 5432   A6666  $66.66
```





```
4242 4242 1234 5678  A5555  $  5.55
4242 4242 1234 5678  A1111  $11.11
```



Alice's bank

```
4000 4000 9876 5432  A9999  $  9.99
4000 4000 9876 5432  A6666  $66.66
```



Chad's bank

Message Flow: Clearing



Cardholder



Merchant



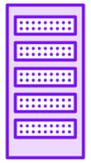
Acquirer



Card brand



Issuer



Merchant clearing file

Separate brands

Brand clearing file

Separate issuers

Issuer clearing file

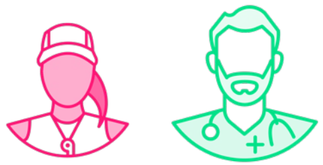
Debit funds from cardholders' accounts

Clearing (Three-party)

Cardholders

Merchants

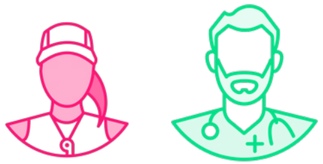
Card scheme
Card brand



Alice & Chad buy
a coffee from Bob

```
370000 12345 6789   A5555  $5.55
370000 98765 4321   A9999  $9.99
```





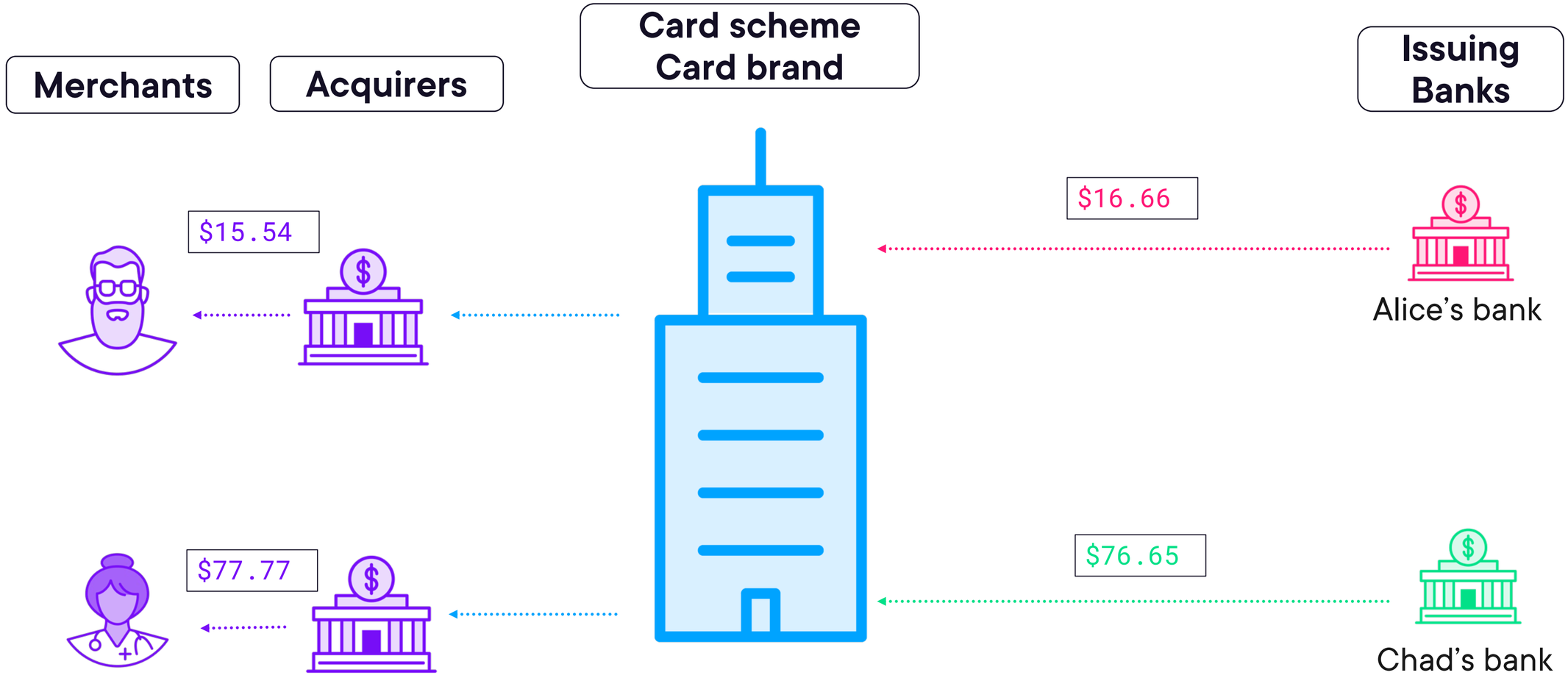
Alice & Chad pay
for parking at the
health center

```
370000 12345 6789   A1111  $11.11
370000 98765 4321   A6666  $66.66
```





Settlement (Four-party)



Message Flow: Settlement



Cardholder



Merchant



Acquirer



Card brand



Issuer

Calculate settlement amounts

Send bill

Allocate funds

Separate acquirers

Send $

Send $

Separate merchants

Credit merchants' accounts

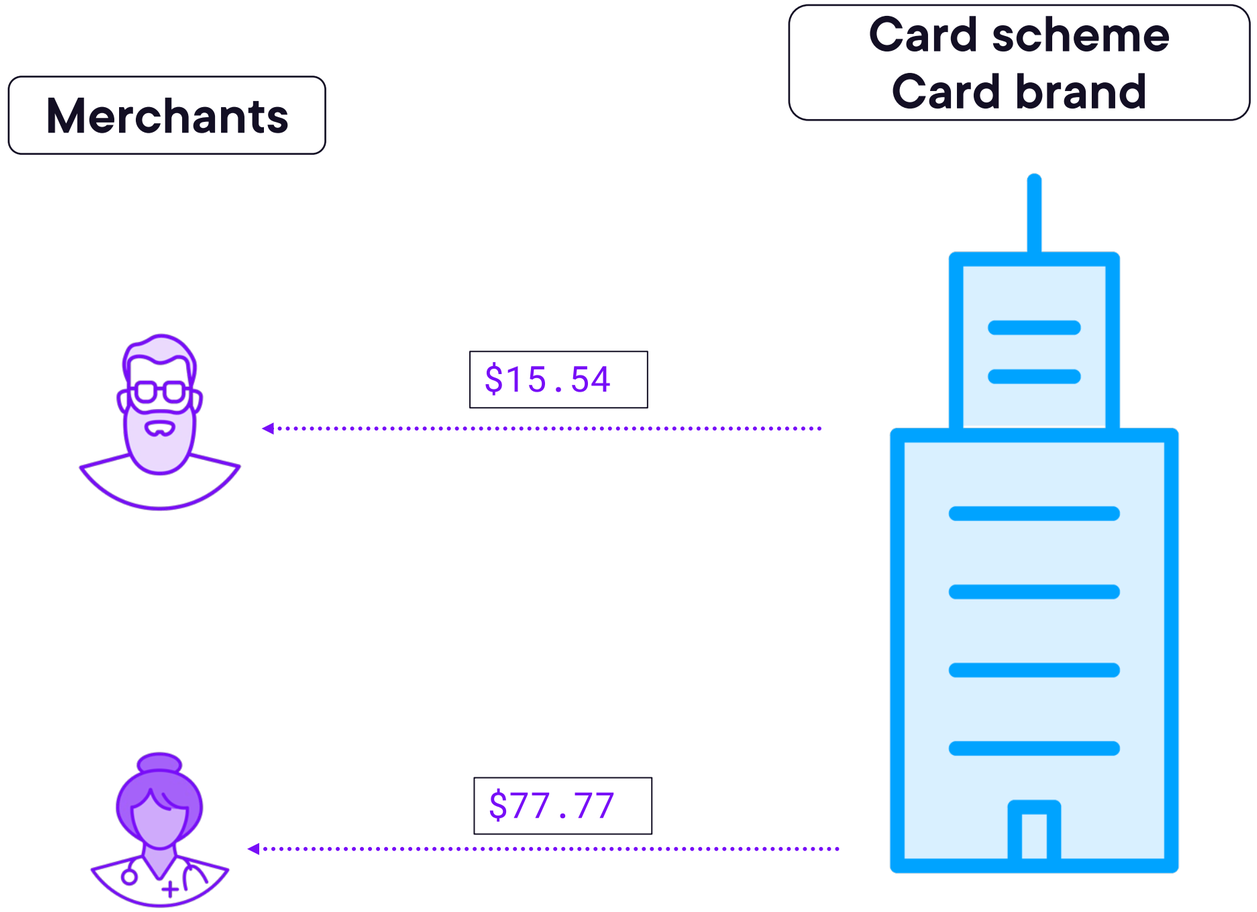


Withdraw $

Card Statement
4687 38 **** 7980**

Pizza	$13.20
Rail fare	$56.87
Wired Brain Coffee	$ 5.10
Pluralsight	$29.99
Web hosting	$ 9.99
Total	$115.15

Settlement (Three-party)



Some Irregularities (Sorry)

Not all transactions are authorized

Merchants may not send clearing files

Some merchants call their clearing flies “settlement files”

Messages are different based on brand and country

Some schemes of countries may not have clearing

Some 3-party brands are also 4-party brands

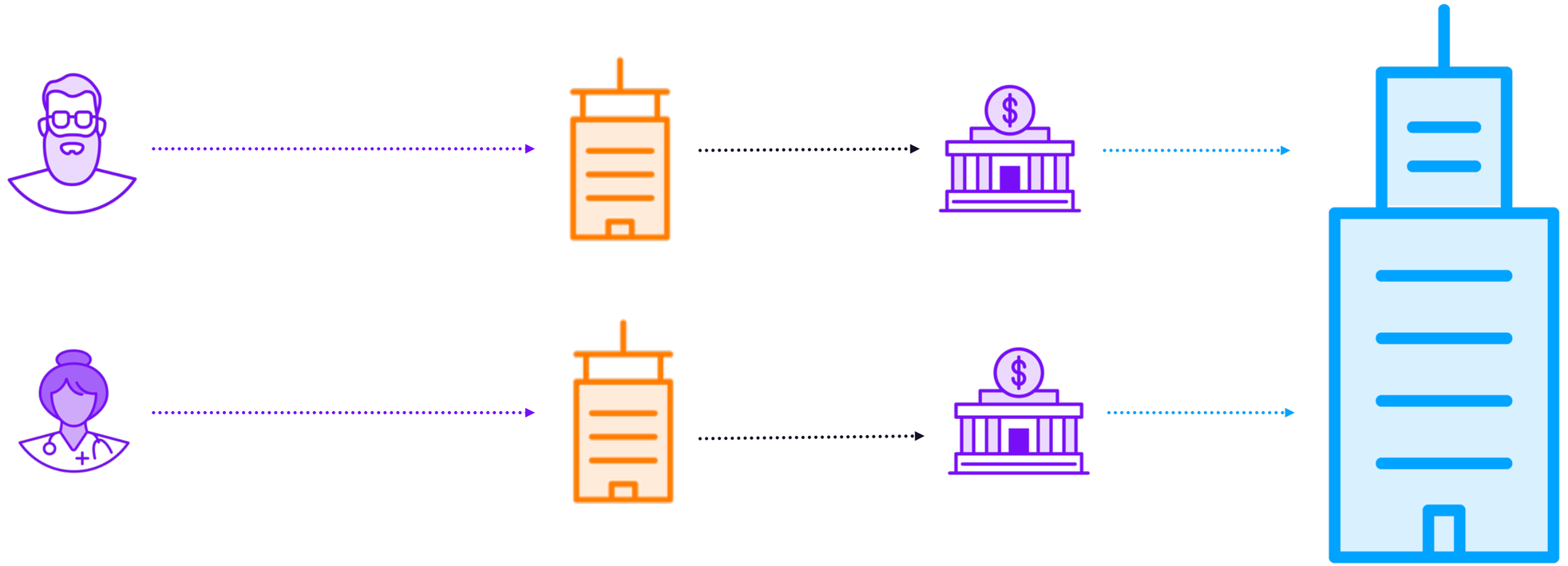
One New Ecosystem Member

Merchants

ISO
Merchant Services Provider

Acquirers

Card scheme
Card brand



Independent Sales Organization (ISO)



Merchant services provider

- (Payment services provider)

Supply payment terminals

Have arrangements with acquirers

May pass data between the merchant and acquirer

Transparent to the transaction

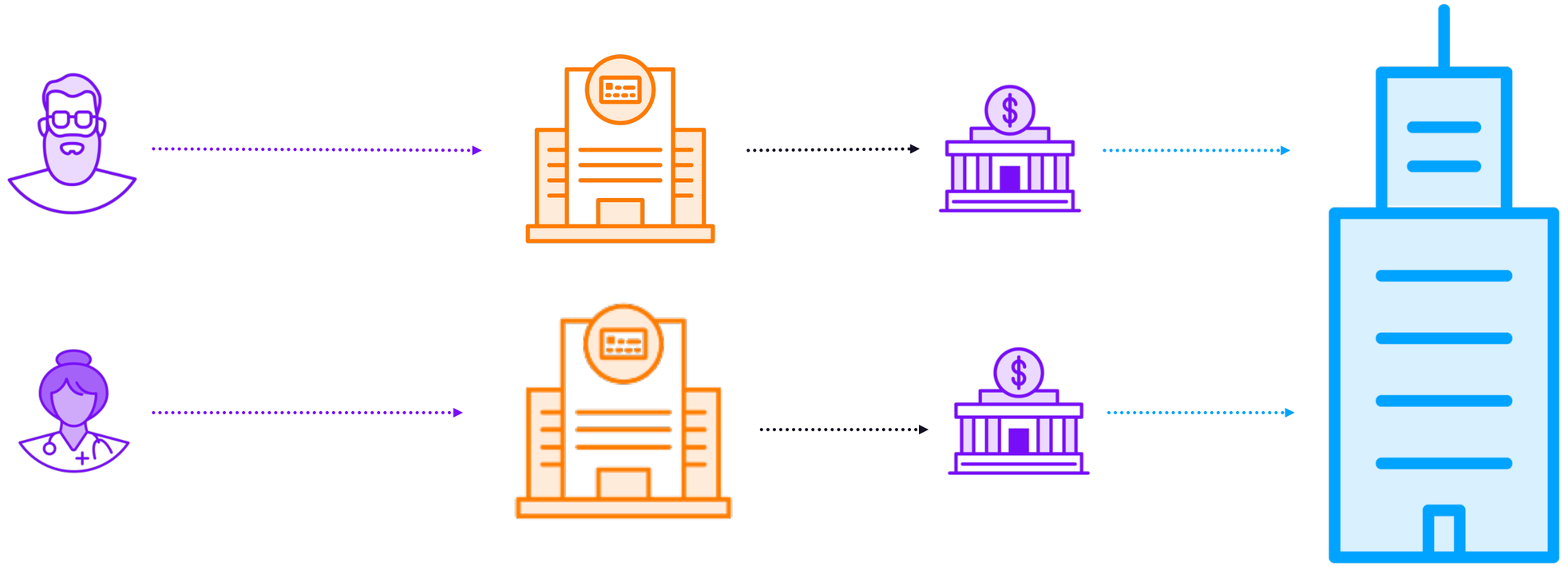
Another New Ecosystem Member

“Merchants”

Payment Facilitator (Payfac)

Acquirers

Card scheme
Card brand



Payment Facilitator



Supply payment terminals

Have arrangements with acquirers

Is the actual merchant of record

- PS*Wired Brain Coffee

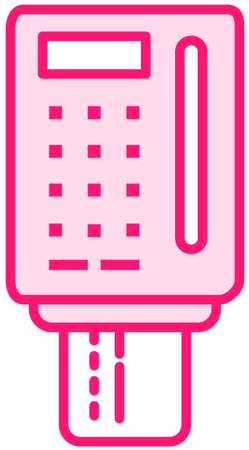
Their customers are sub-merchants

Initially targeted small merchants

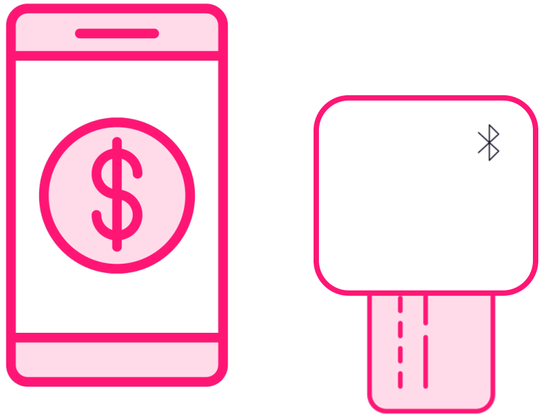
Sometimes vertical market focused

- Hospitality

Payment Terminals (Points of Interaction or POI)



Traditional payment terminal



Phone or tablet devices with external reader



Phone or tablet devices

The Three Stages of Card Payments

Authorization

Real-time

Clearing

Reconciliation

Settlement

Payment

Summary

Issuing banks (issuers) and (3-party) card brands/schemes provide cards to cardholders

Cardholders purchase goods and services from merchants

Acquiring banks (acquirers) and (3-party) card brands acquire transactions from merchants

(4-party) Card brands/schemes connect acquirers to issuers

Independent sales organizations and payment facilitators can contract with merchants to send transactions to acquirers