

Payment Card Security, Processing, and the PCI Standards

Discovering How Card Payments Work



John Elliott

Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire



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



Time for Coffee



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



**“That will be
\$5.10”**



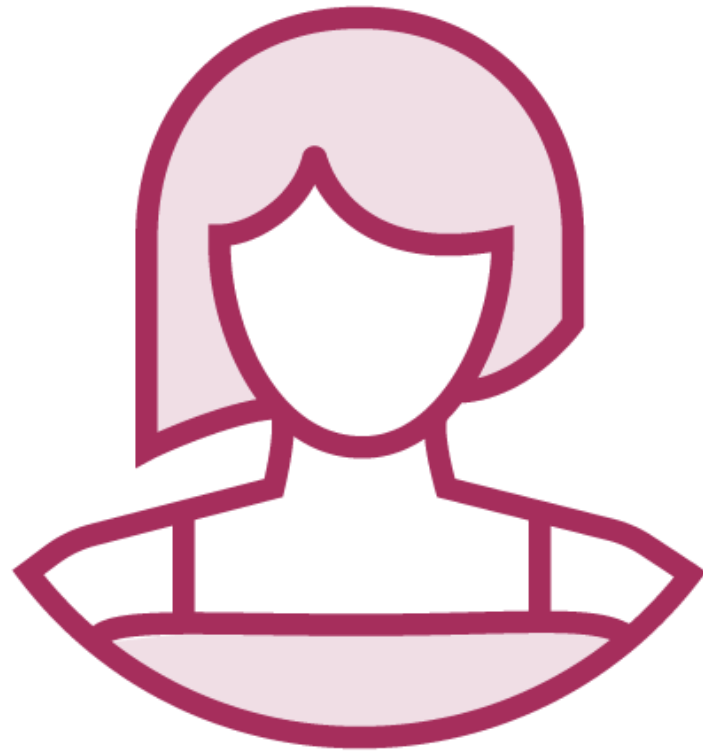
“I’ll pay by card...”



“Here you go”



What Are People Thinking?



Wanda Wired-Brain

Will I get paid?



Ann Cardholder

Can I have that latte?

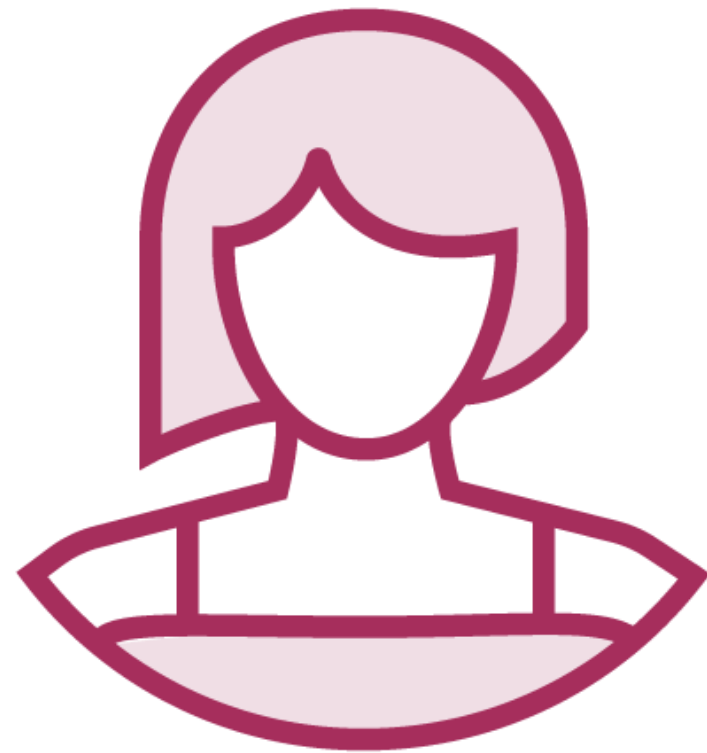


Ann's Bank

**Is this really Ann,
or is it fraud?
Does Ann have enough
cash or credit?**



The Purpose of Authorization



**Wanda Wired-Brain
(Merchant)**

Will I get paid?

**“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”



Ann’s Bank

**Is this really Ann,
or is it fraud?**

**Does Ann have enough
cash or credit?**



The Purpose of Authorization



Steps in the Transaction



A

**Authorization
(auth)**



C

Clearing



S

Settlement



U

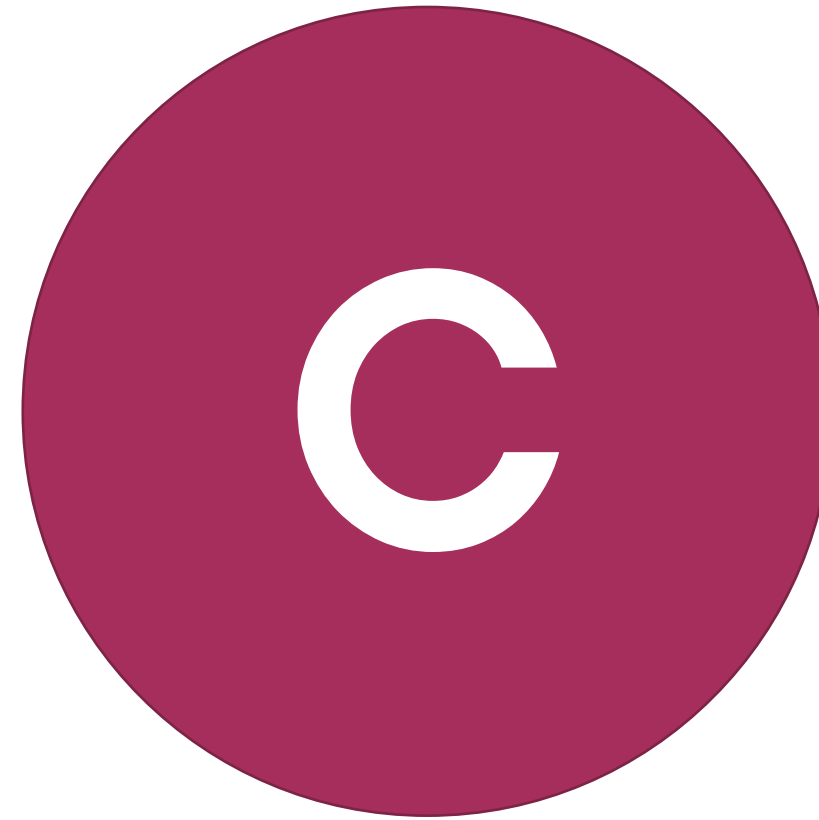
**Undo:
Chargeback and
Refunds**



Steps in the Transaction



**Authorization
(auth)**



Clearing



Settlement



**Undo:
Chargeback and
Refunds**



Steps in the Transaction



A

**Authorization
(auth)**



C

Clearing



S

Settlement

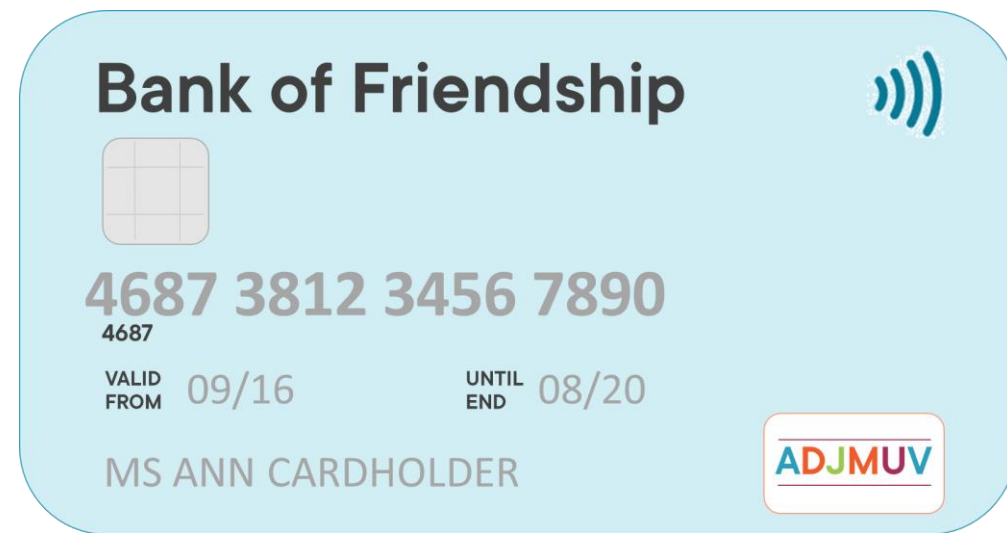


U

**Undo:
Chargeback and
Refunds**



No Longer Just Cards



Traditional Cards



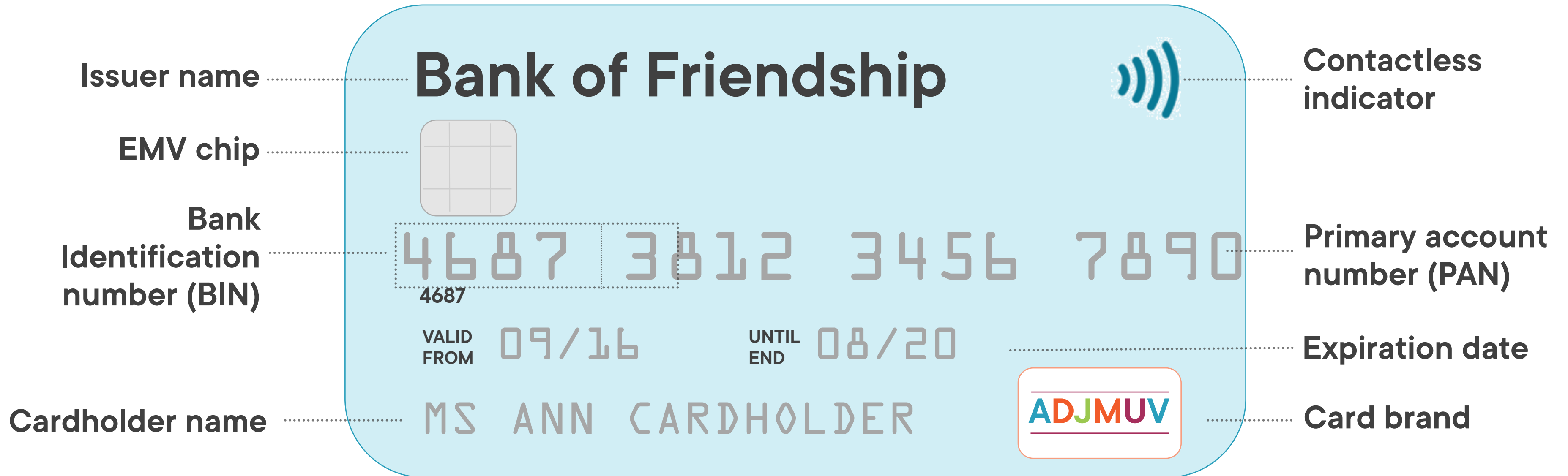
Smartphones



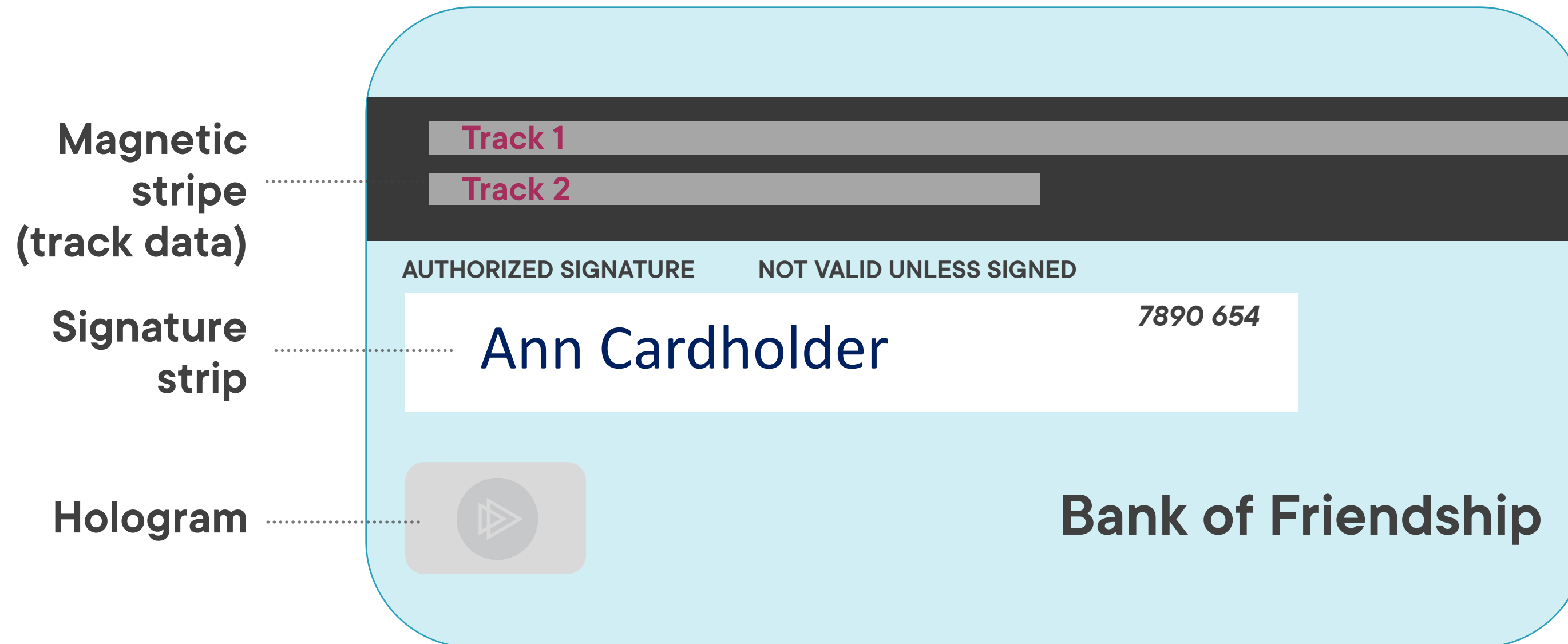
Smart Devices



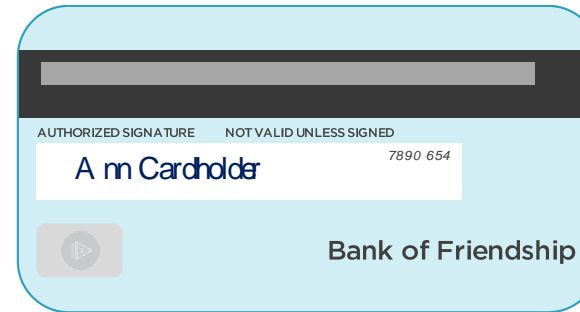
The Data on a Payment Card



The Data on a Payment Card



Cardholder Data: Track 1

[illegible]

Primary Account Number

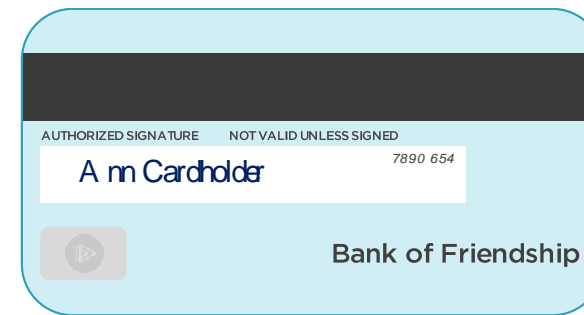
Card holder's name

Expiration date

Service code



Sensitive Authentication Data (SAD)



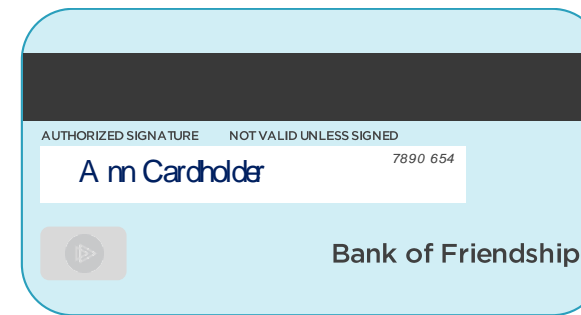
1 2 3 4 5 6 7 8
01234567890123456789012345678901234567890123456789012345678901234567890

%B4687381234567890^CARDHOLDER/ANN MS^20081010045600000000000000000000000000000000?Q

Card Verification Value (CVV)



What Can Be Stored: Track 1?

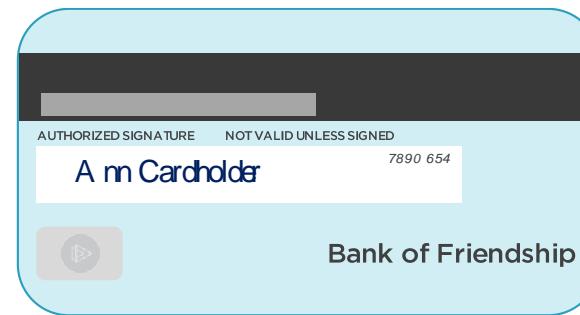
[illegible]

You can store all this up to the service code

You cannot store any of this after authorization



Cardholder Data : Track 2



1										2										3										4									
01234567890123456789012345678901234567890																																							
;4687381234567890=2008101004560000000000?Z																																							

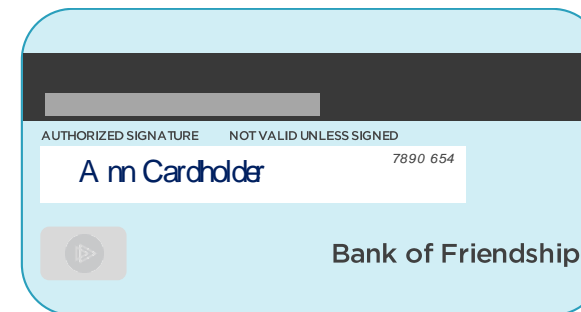
Primary
Account
Number

Expiration
date

Service
code



Cardholder Data : Track 2



1	2	3	4
01234567890123456789012345678901234567890			
;4687381234567890=2008101004560000000000?Z			

You can store all this up
to the service code

You cannot store any of this
after authorization



Reading Card Data for Authorization

**What data is
present on the card**

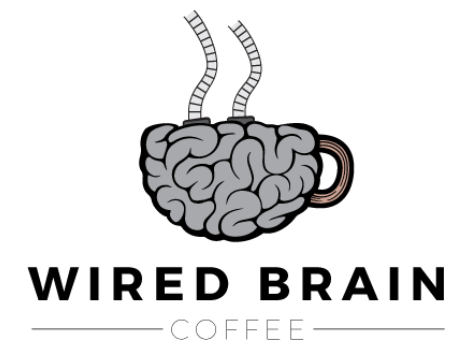
**What the merchant's
systems can read**



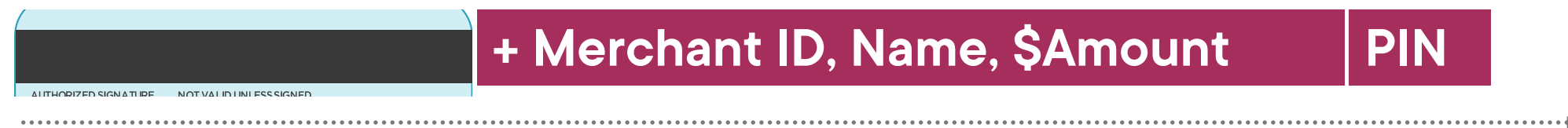
Reading Card Data



Authorization in Practice



Authorization Request



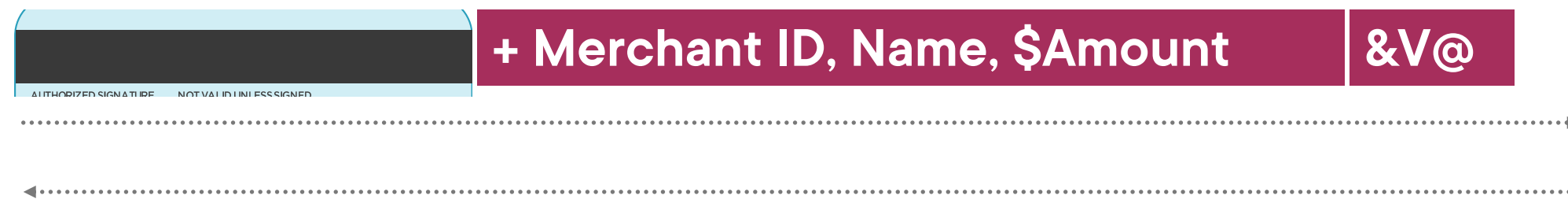
Ann's
Bank



Authorization in Practice



Authorization Request



Response | Reference

Authorization Response

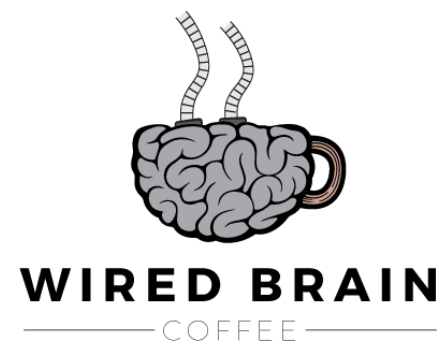


Ann's
Bank



Authorization in Practice

Merchant



Issuing
banks

Card
holders



Anne's Bank



Bob's Bank

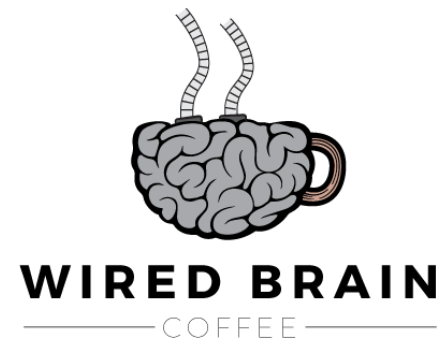


Claire's Bank



Authorization in Practice

Merchant



Acquirer



Wired Brain Coffee's
Acquiring Bank

Issuer



Anne's Bank

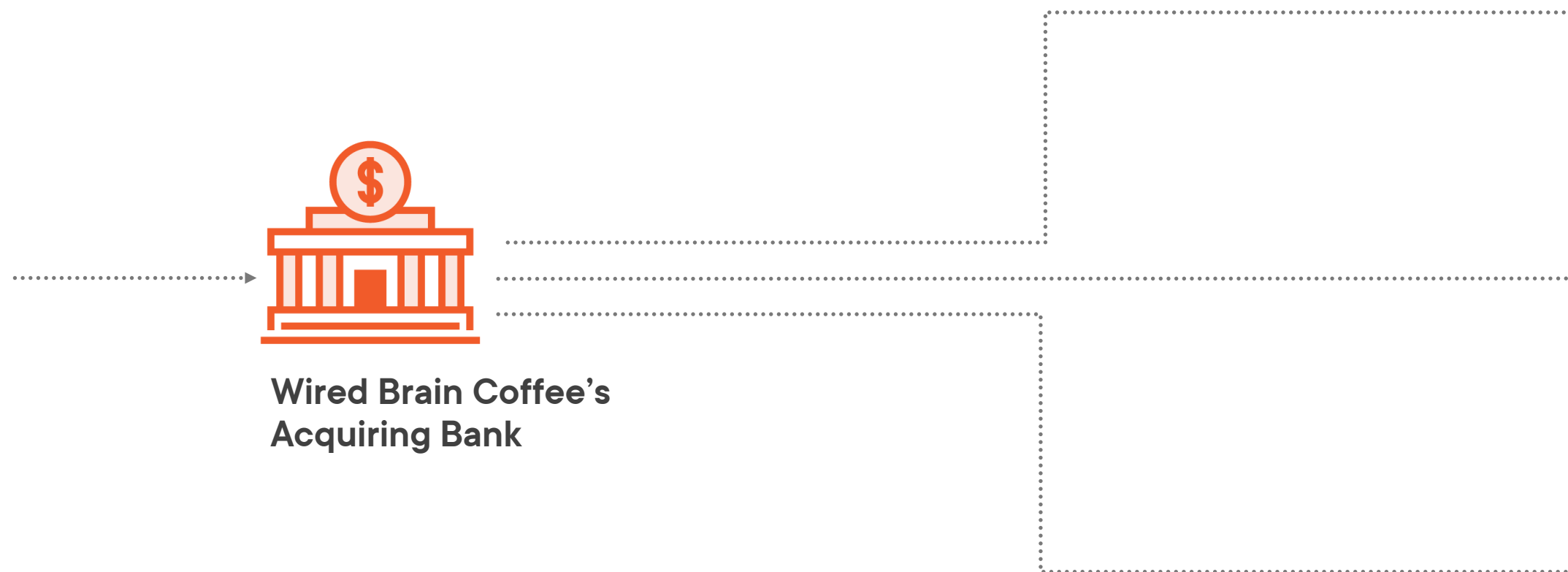


Bob's Bank

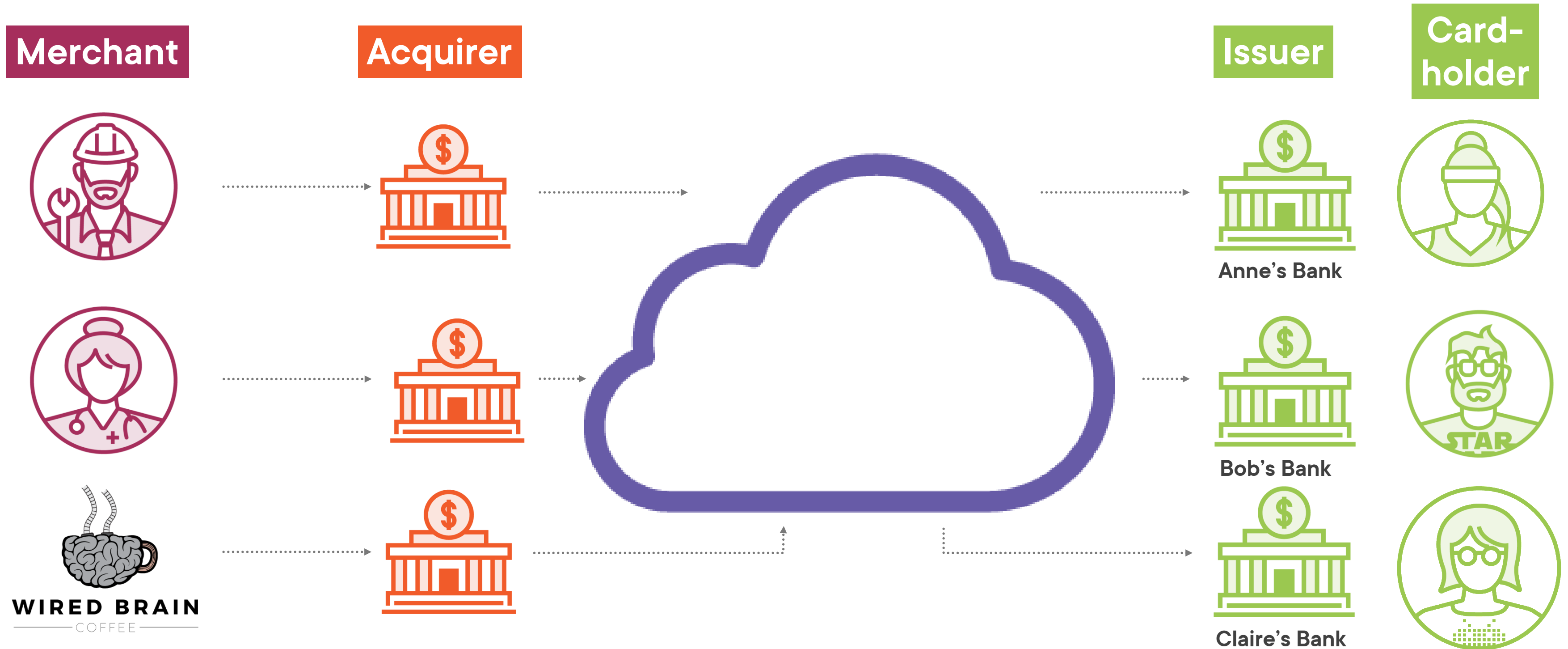


Claire's Bank

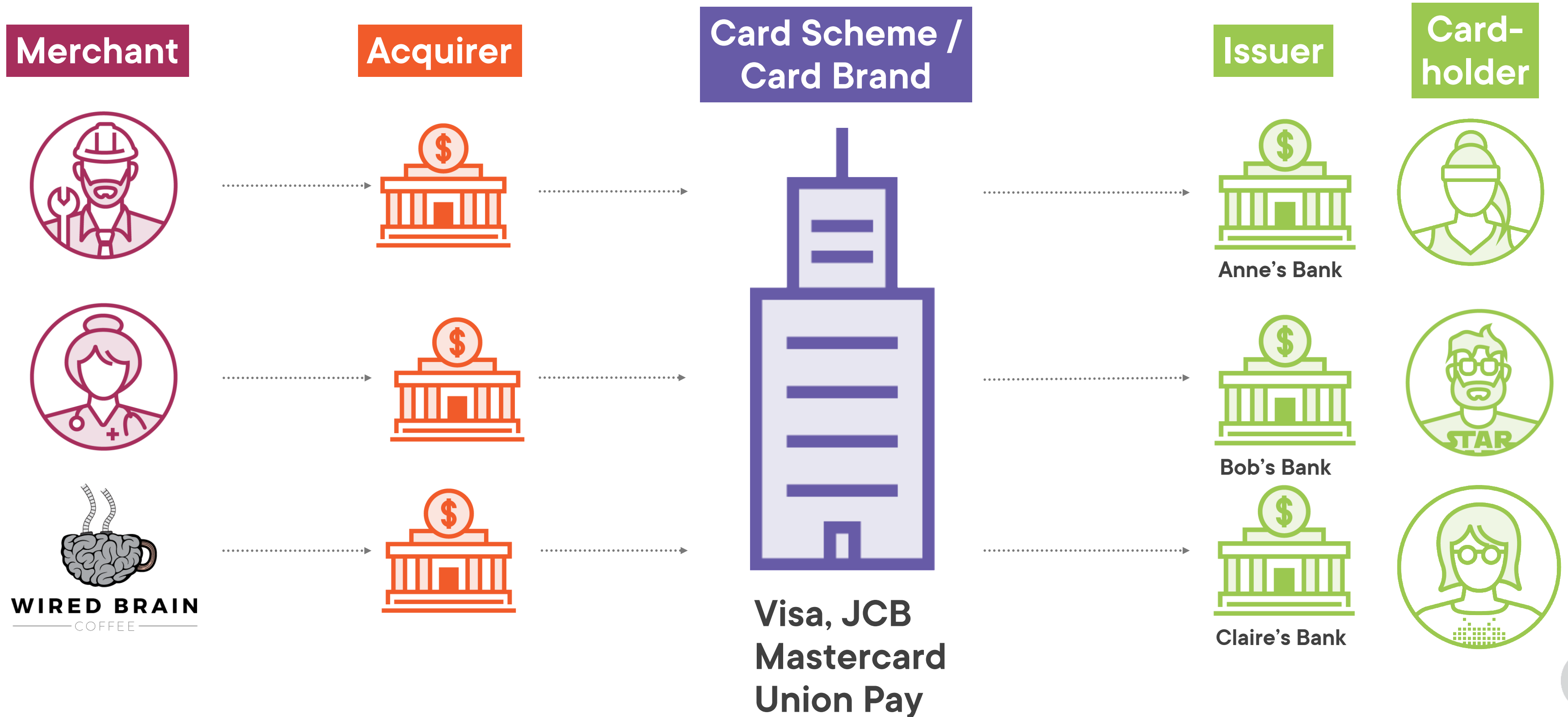
Card-
holder



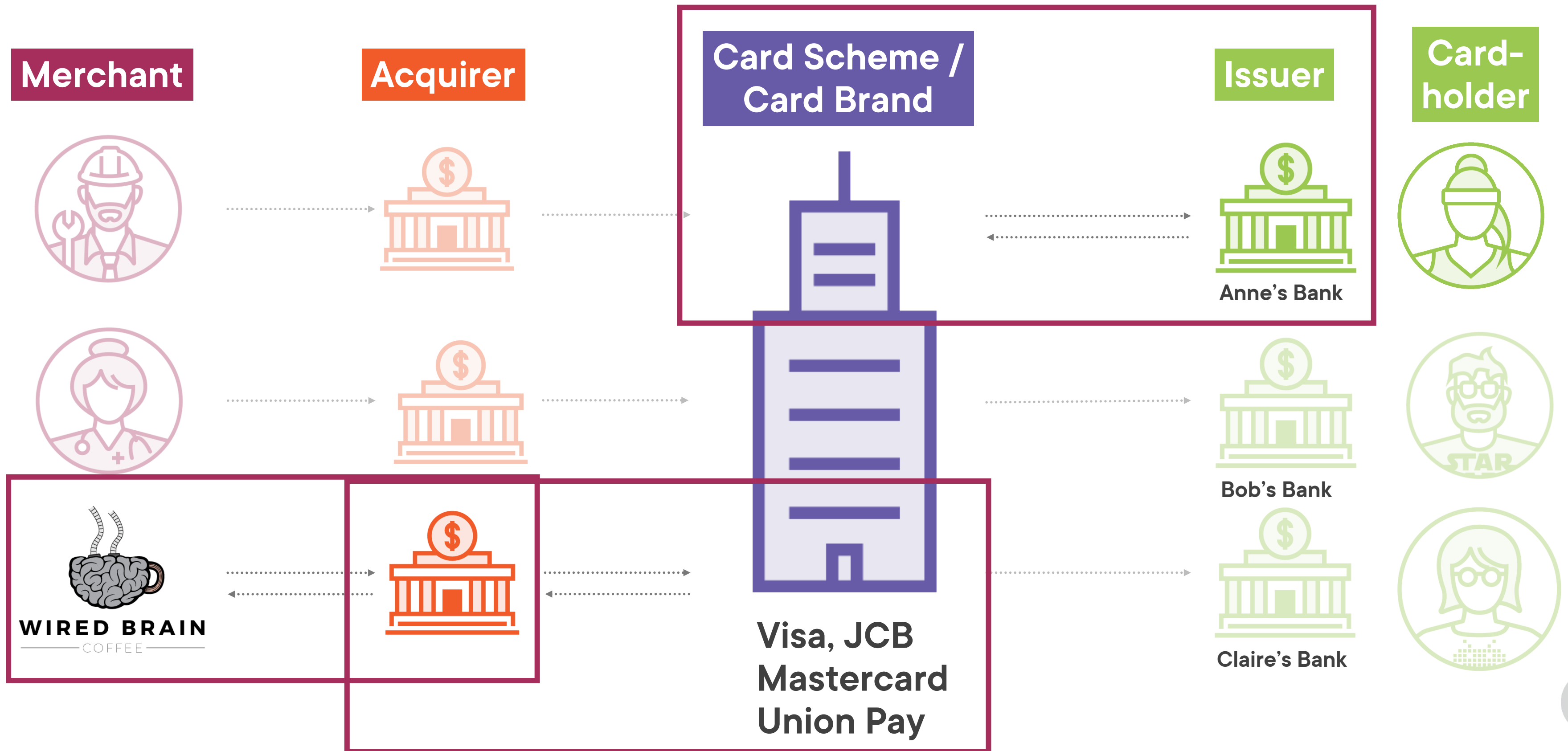
Authorization in Practice



Authorization in Practice



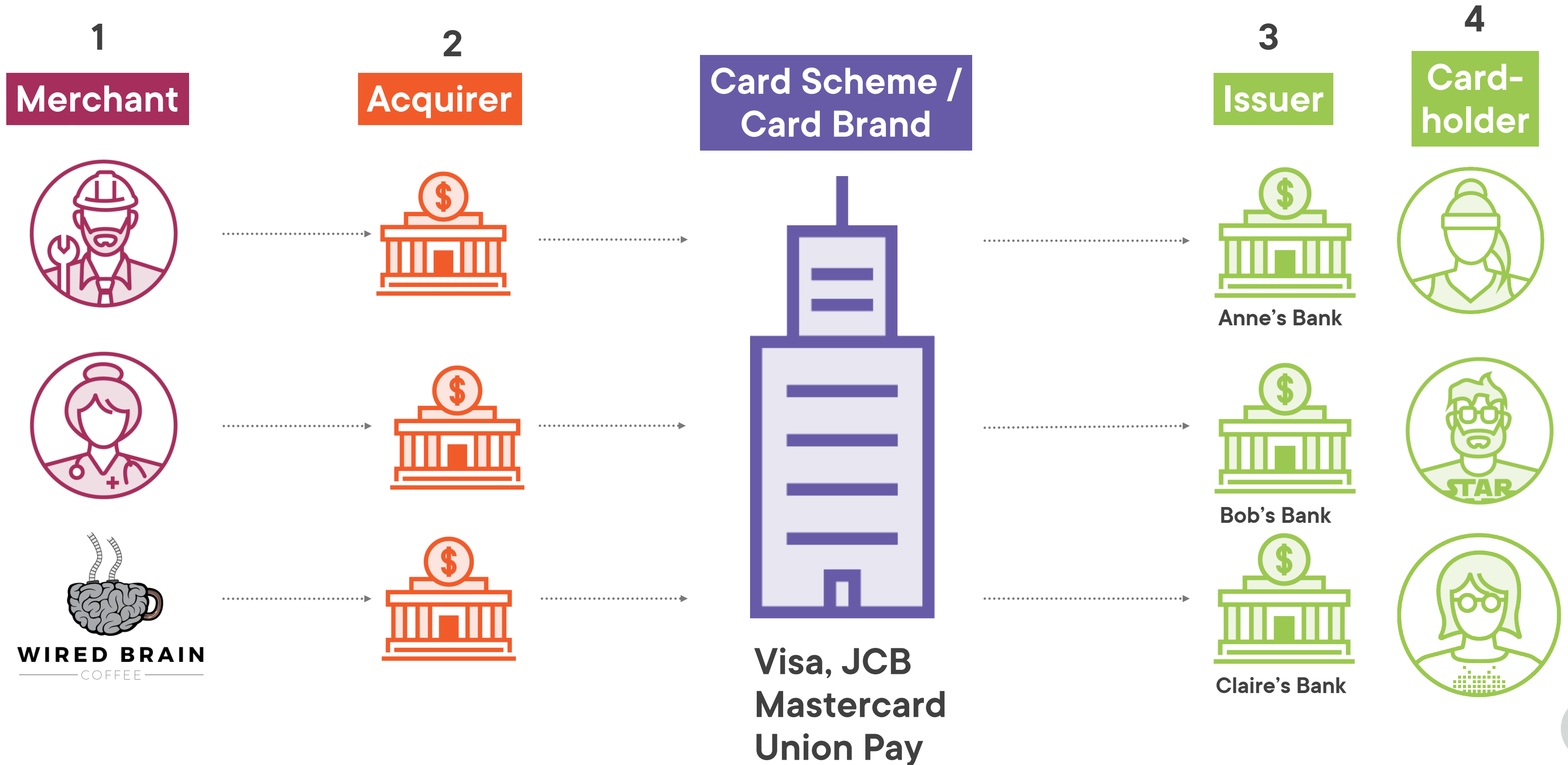
Authorization in Practice



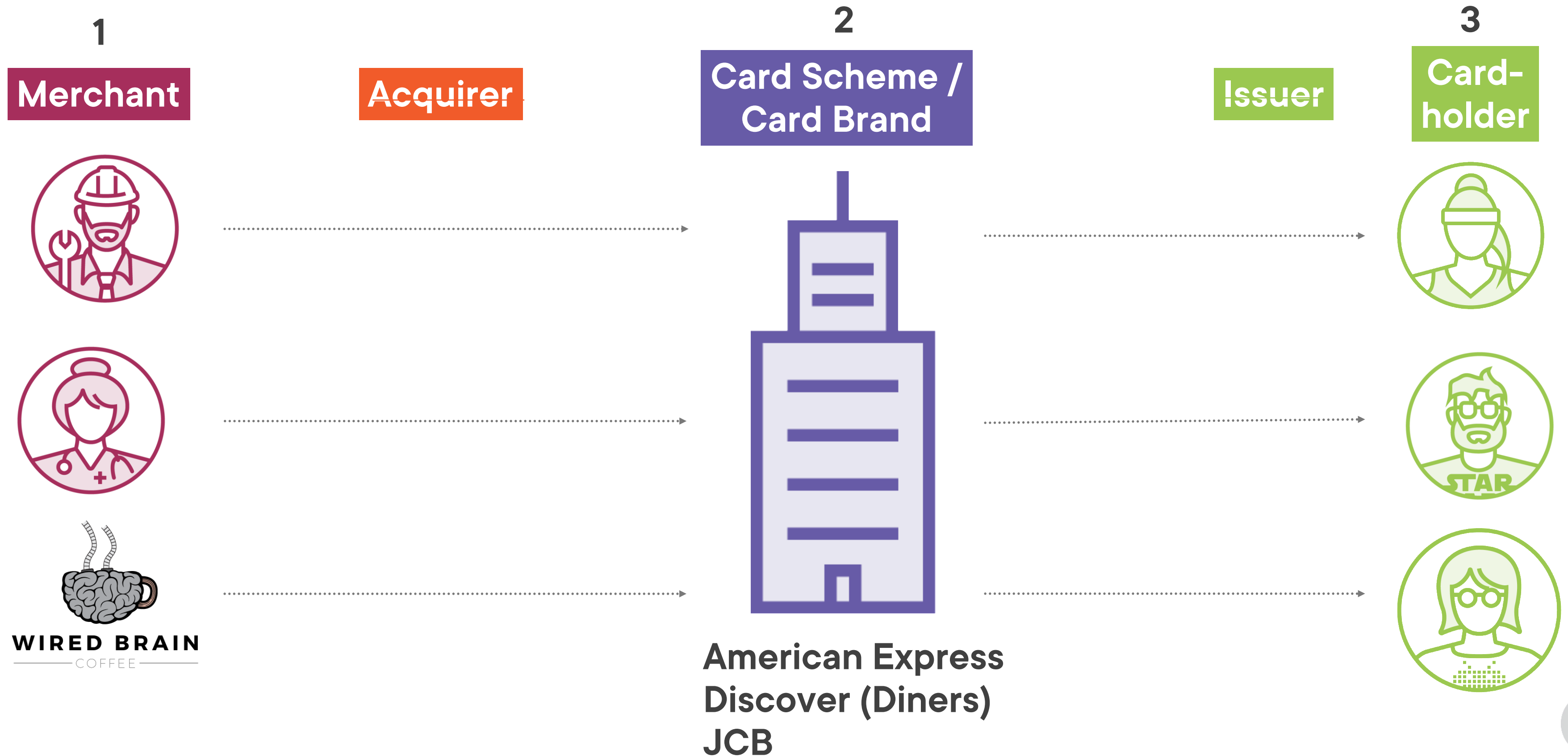
If the payment system were a language, it would have more irregular verbs than any other



Four-party Model



Three-party Model



Who Has What?



Wanda Wired has a “promise to pay”
from Ann’s bank



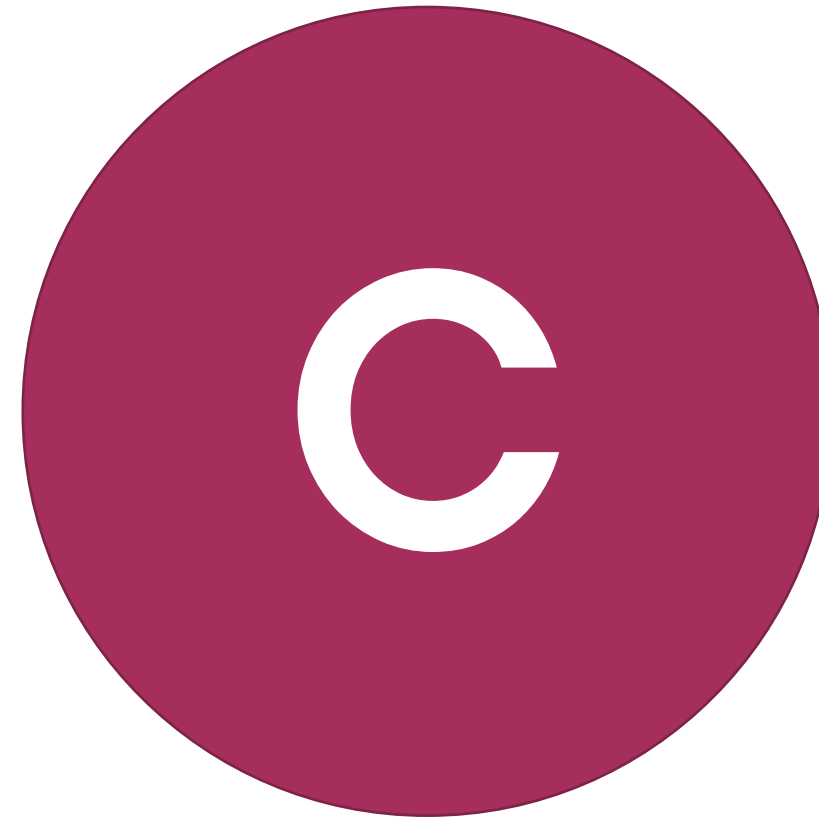
Ann Cardholder has coffee



Getting Money – Clearing and Settlement



**Authorization
(auth)**



Clearing



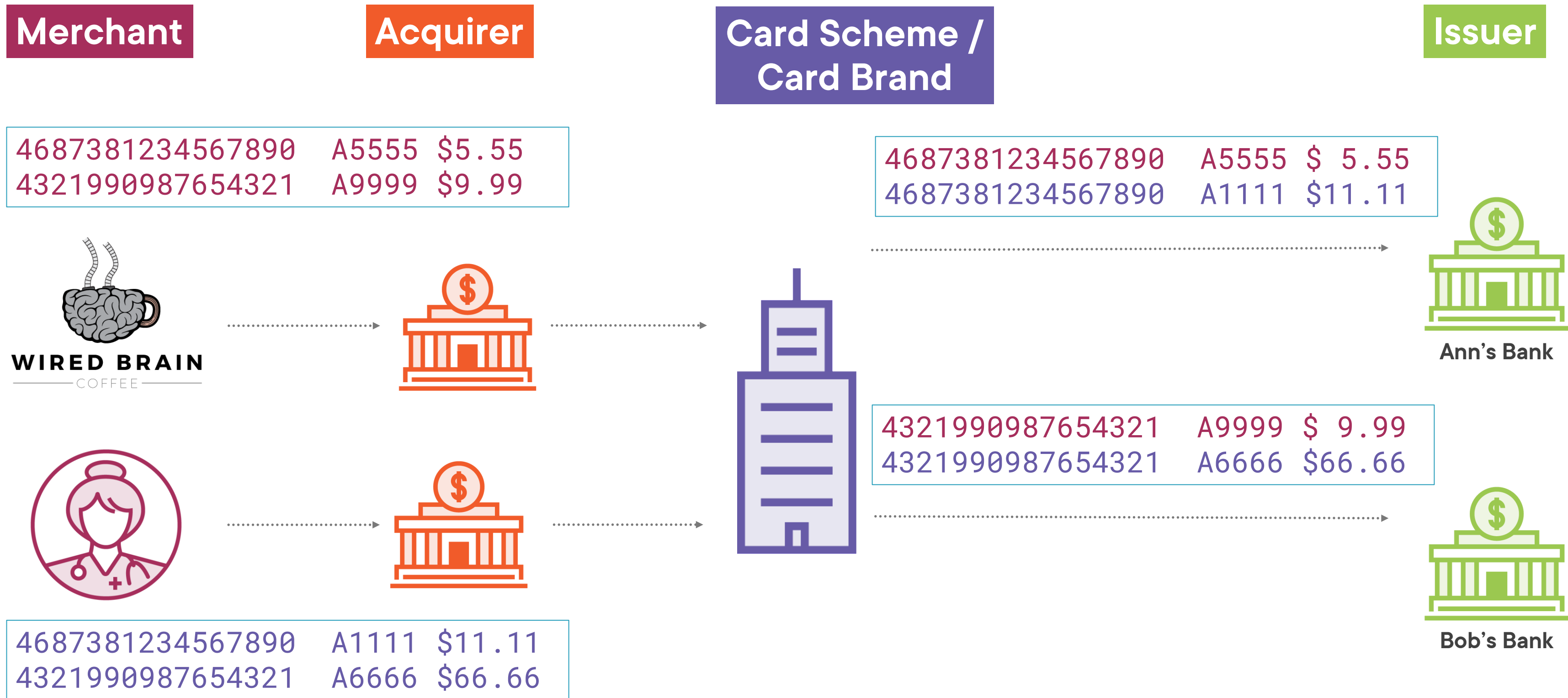
Settlement



**Undo:
Chargeback and
Refunds**



Clearing (4-party)



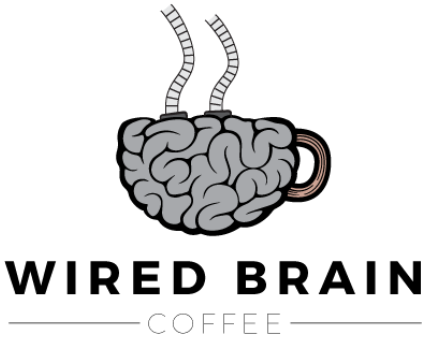
Settlement (4-party)

Merchant

Acquirer

Card Scheme /
Card Brand

Issuer



\$15.54



\$16.66



Ann's Bank

\$77.77



\$76.65



Bob's Bank

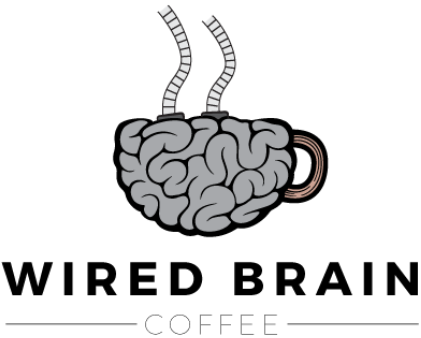


Clearing (3-party)

Merchant

Card Scheme /
Card Brand

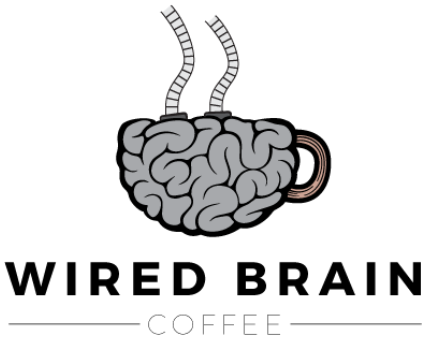
377738123456789	234Q	\$08.76
377799098765432	876Q	\$20.34



Settlement (3-party)

Merchant

Card Scheme /
Card Brand



\$29.10



Irregularities

**Not all transactions
are authorized**

**Merchants may not
send clearing files,**

**Some merchants call
their clearing files
“settlement files”**

**Message formats differ
between acquirers,
schemes and
countries**

**In some countries
there is no clearing**



E-commerce / Customer Not Present (CNP) Transactions



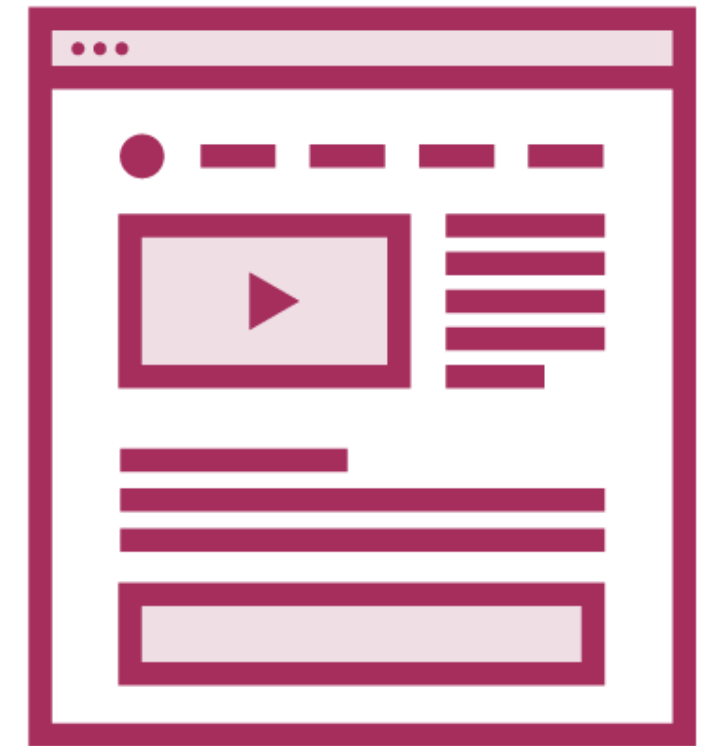
E-commerce



Ann Cardholder wants to
buy some beans...



... using her payment
card ...



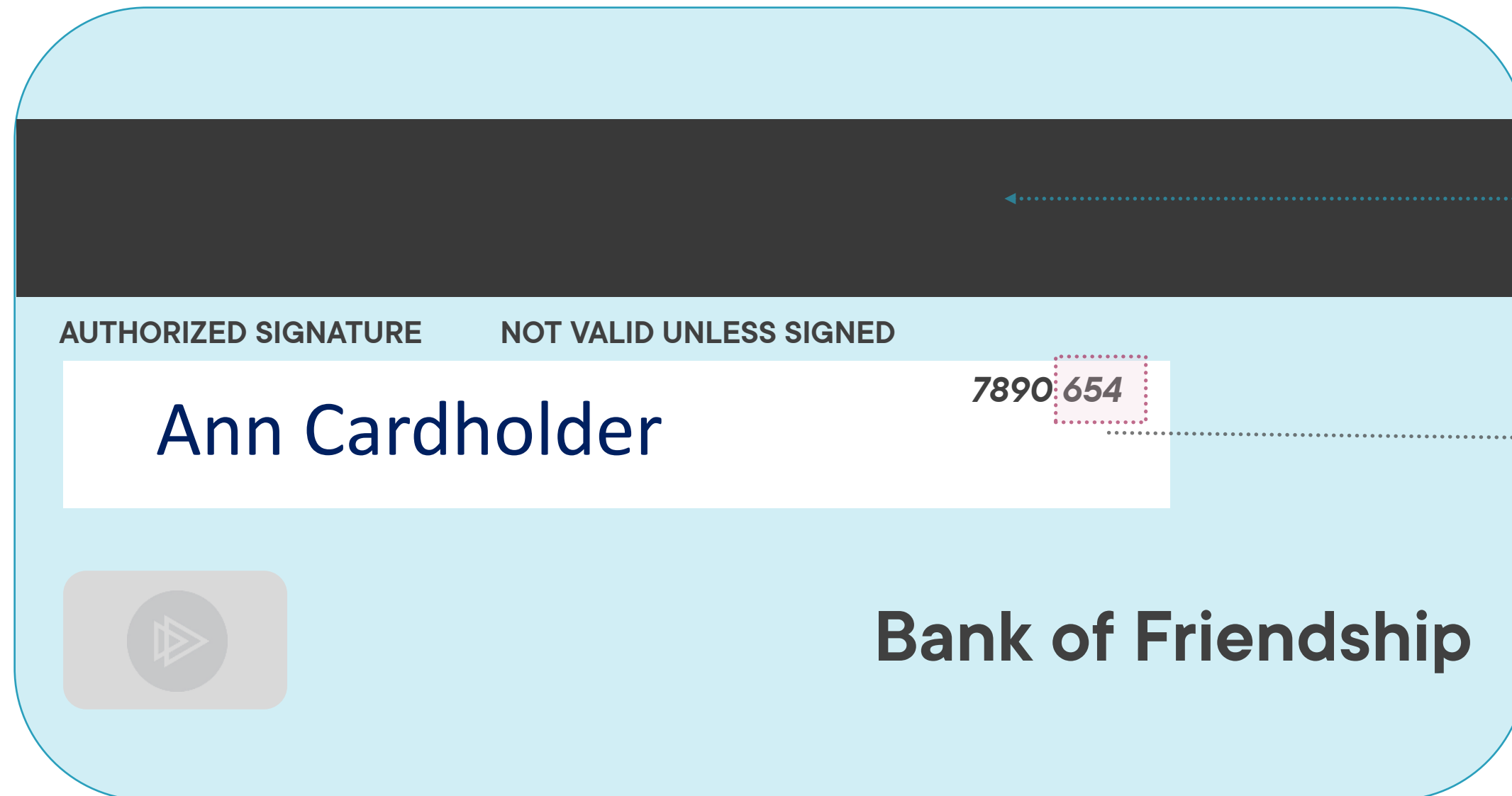
... from the **Wired Brain
Coffee** website



The Data on a Payment Card



The Data on a Payment Card



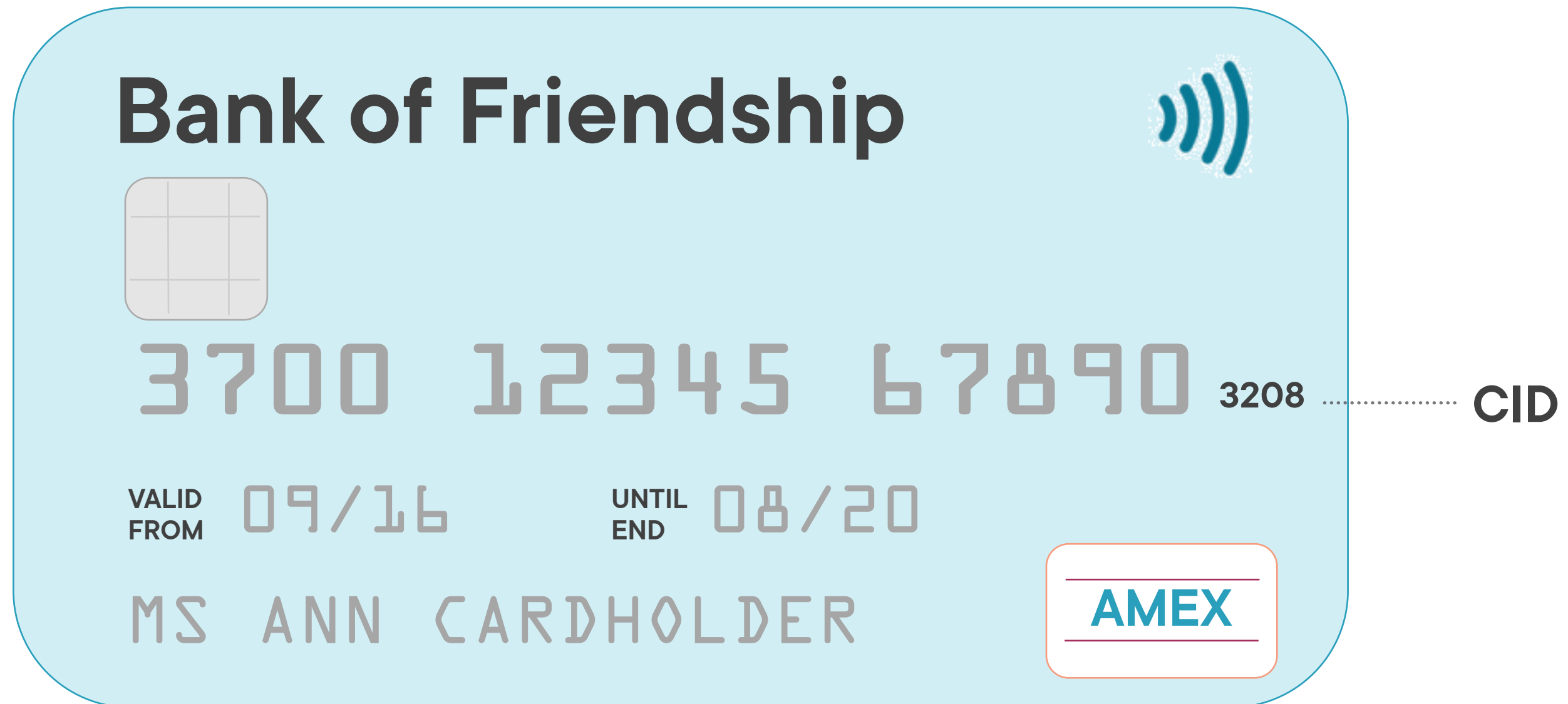
Remember the
CVV is in here

CVV2
CAV2
CVC2
CVN2

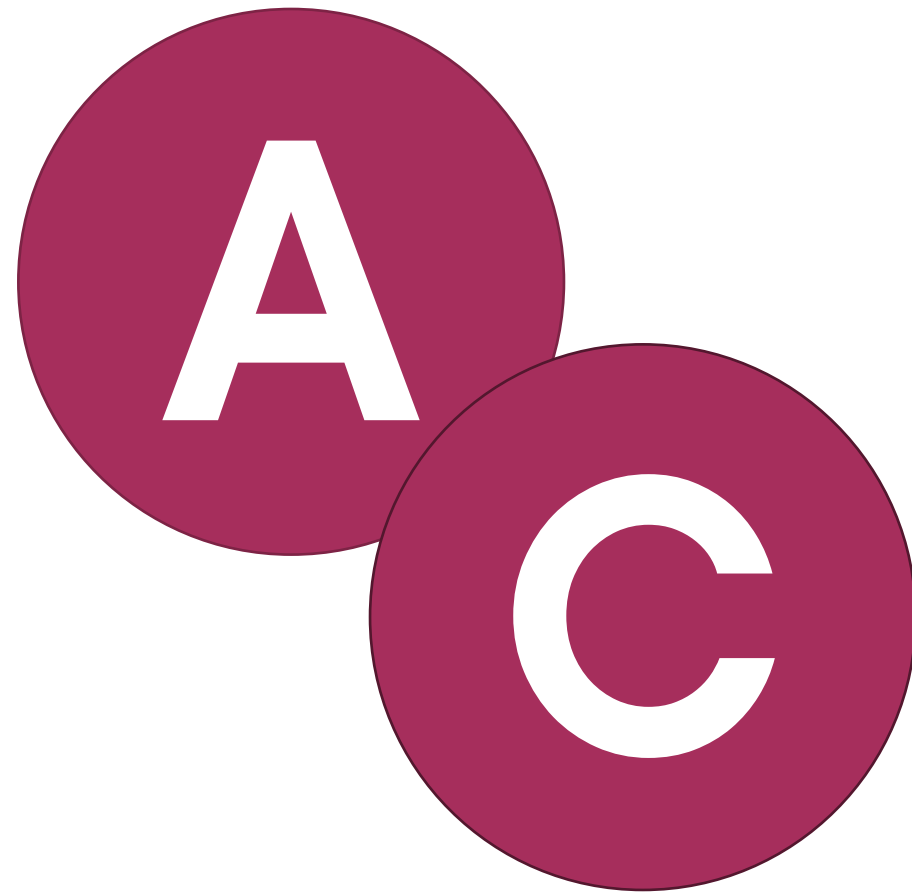
CVV2 != CVV



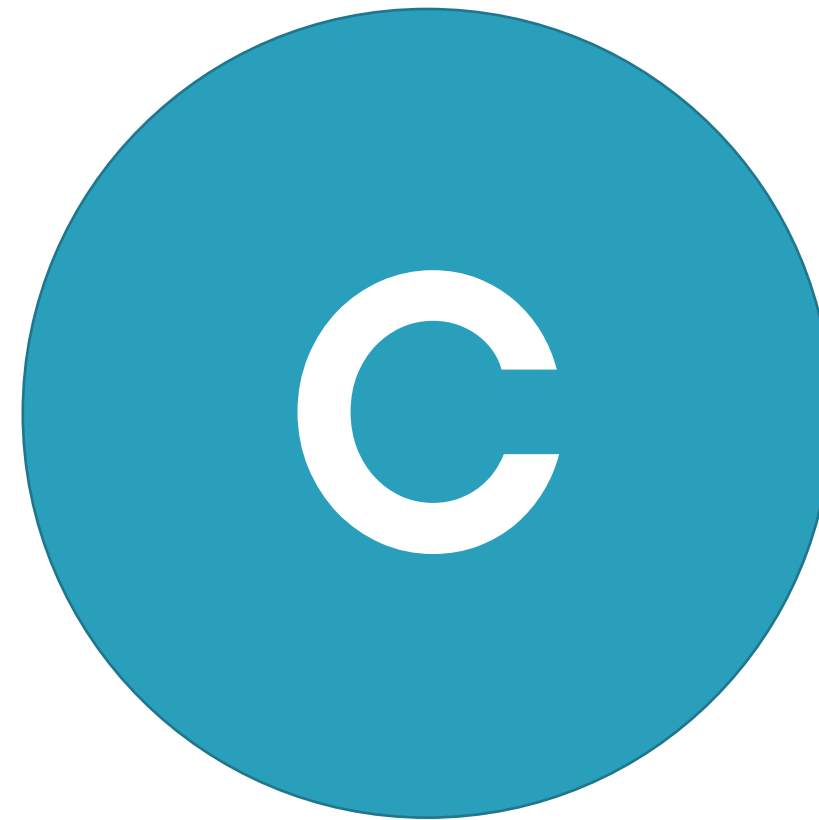
The Data on a Payment Card



Steps in the Transaction



**Authorization
and Capture**



Clearing



Settlement



**Undo:
Chargeback and
Refunds**



E-commerce Authorization

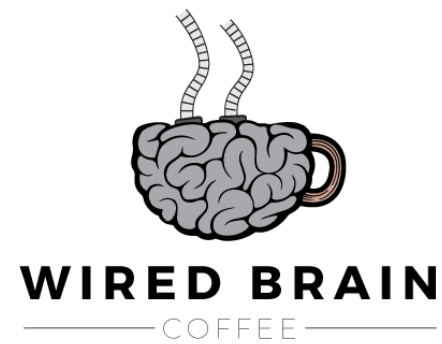
Merchant

Acquirer

**Card Scheme /
Card Brand**

Issuer

PAN, CVV2, Cardholder Name, Expiration Date + Merchant ID, Name, \$Amount



Anne's Bank

Response | Reference



E-commerce Capture

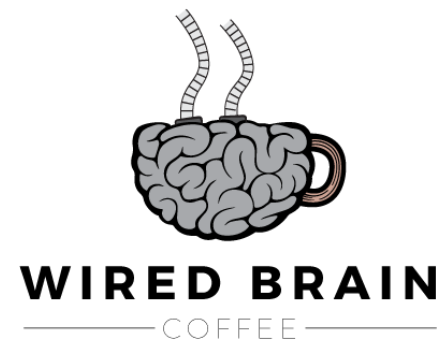
Merchant

Acquirer

**Card Scheme /
Card Brand**

Issuer

PAN, Reference



Anne's Bank



Payment Service Provider (PSP)

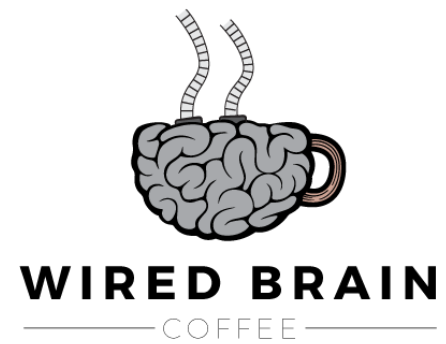
Merchant

PSP

Acquirer

Card Scheme /
Card Brand

Issuer



Anne's Bank

Sometimes also
called a Payment
Facilitator (PF)



Payment Service Provider (PSP)

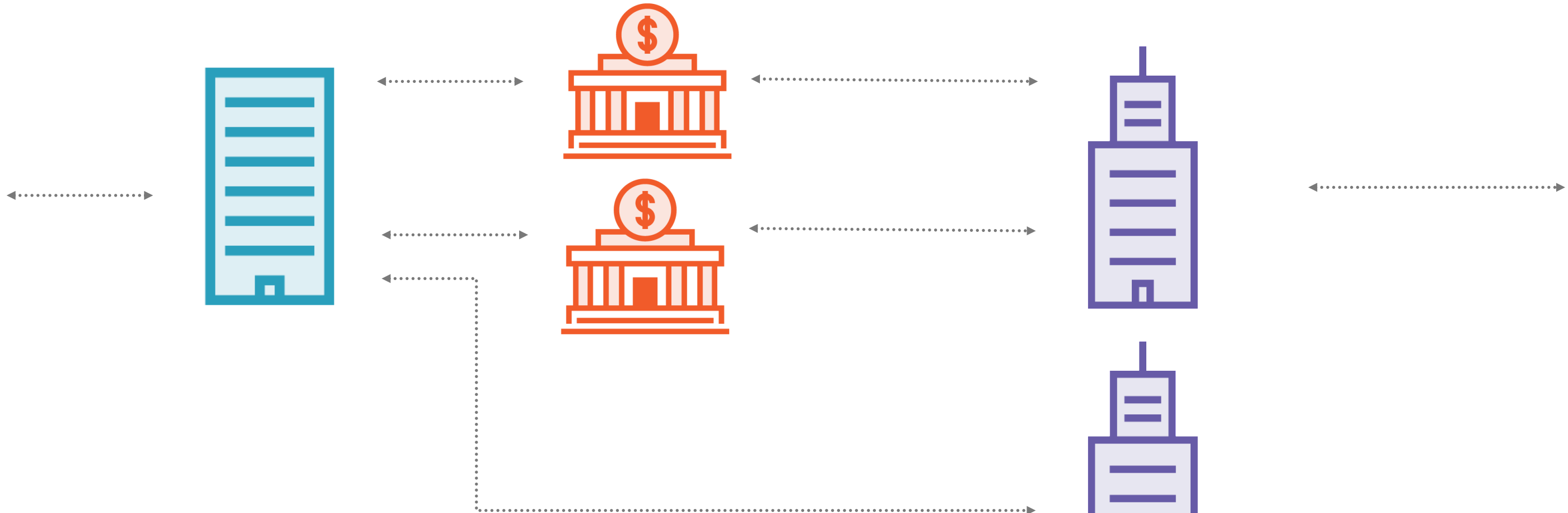
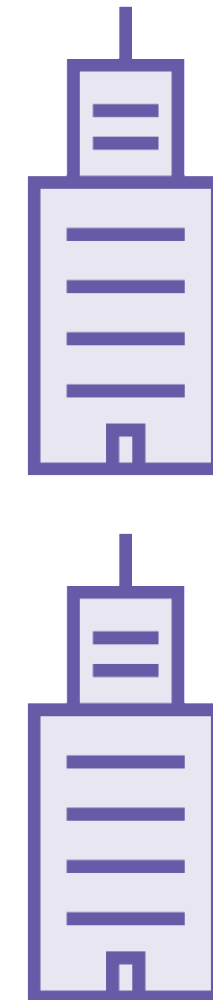
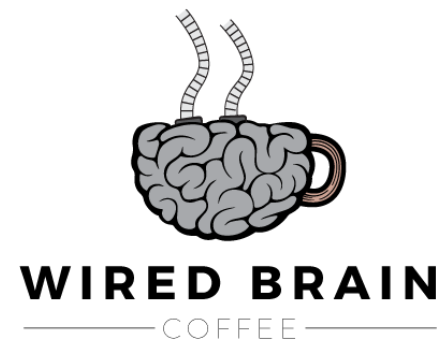
Merchant

PSP

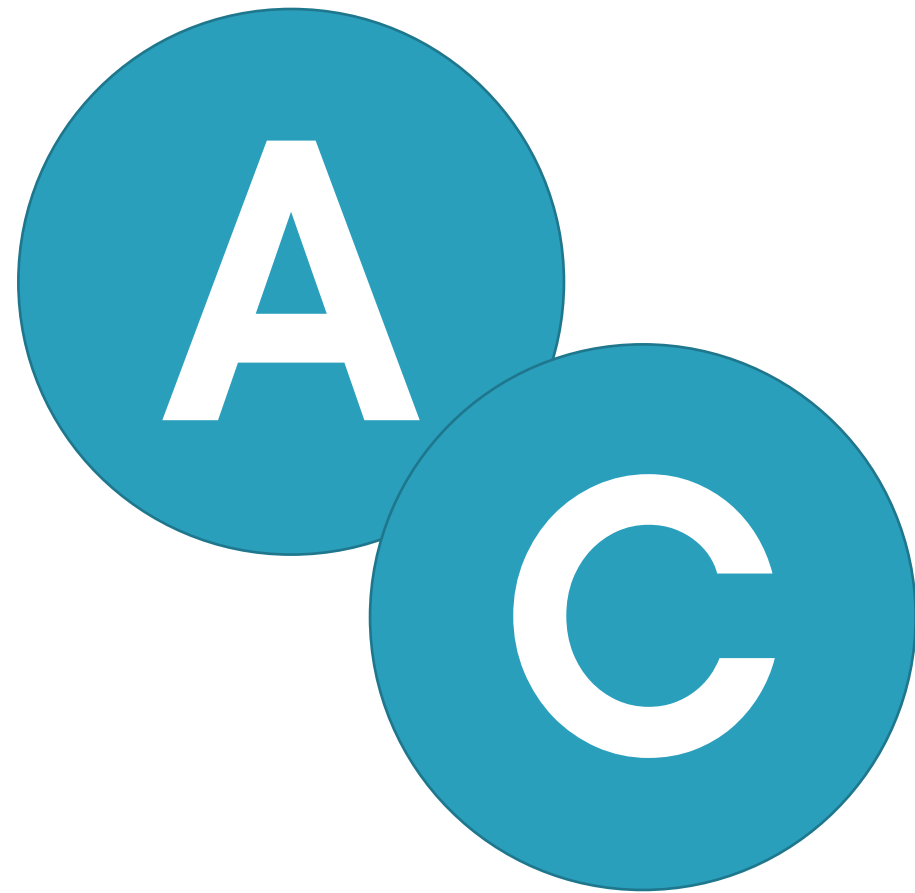
Acquirer

Card Scheme /
Card Brand

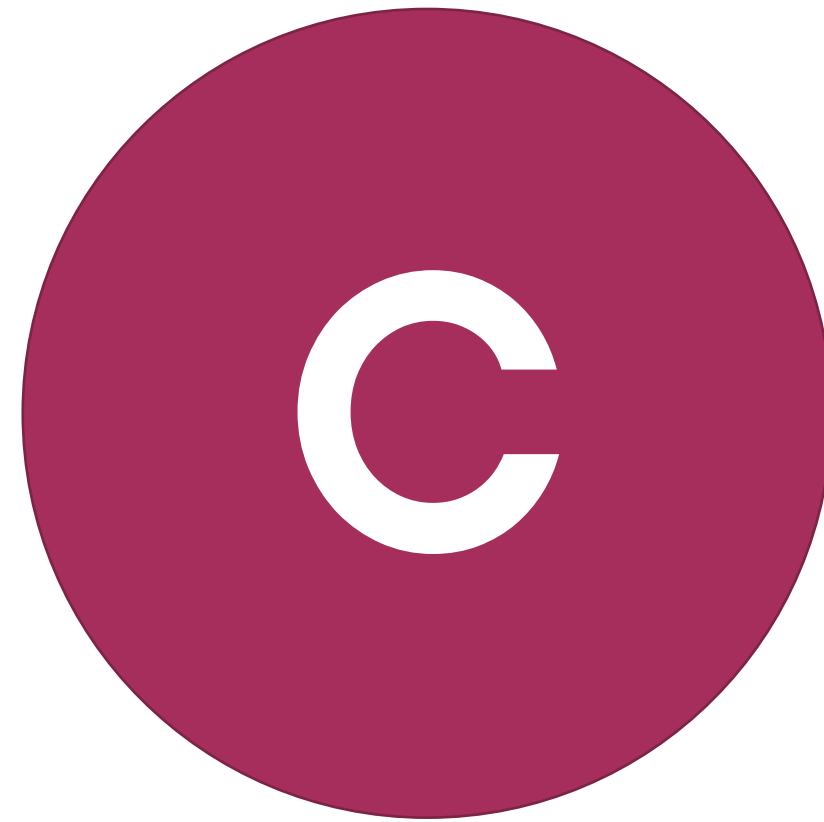
Issuer



Steps in the Transaction



**Authorization
and Capture**



Clearing



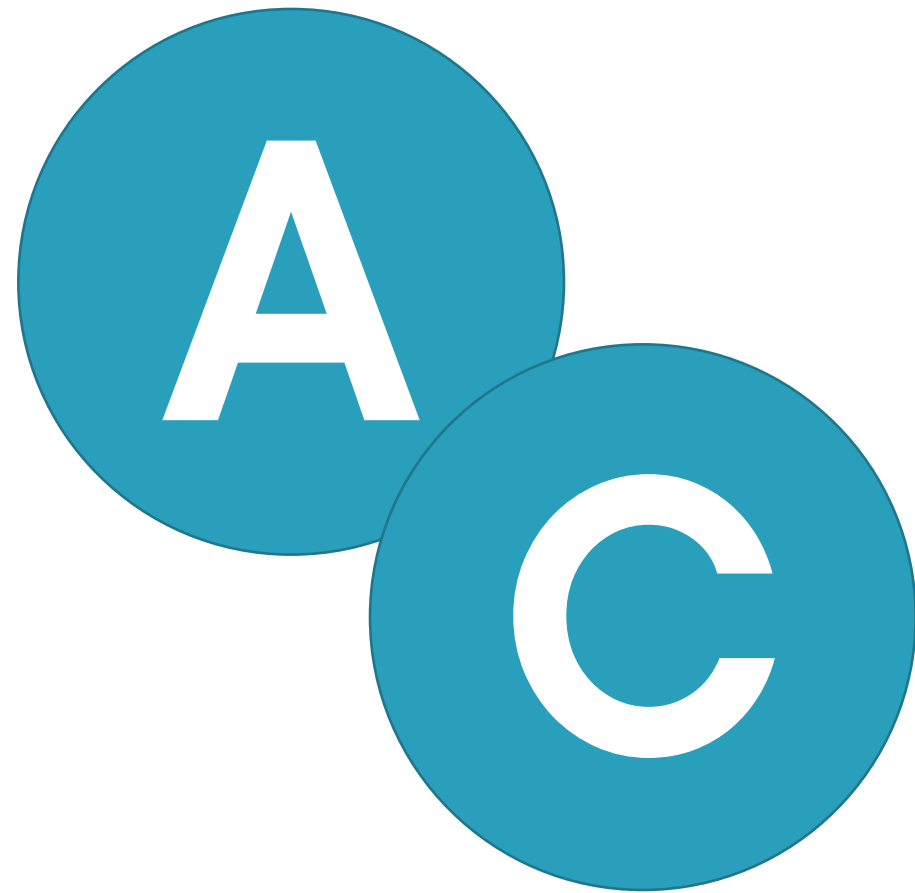
Settlement



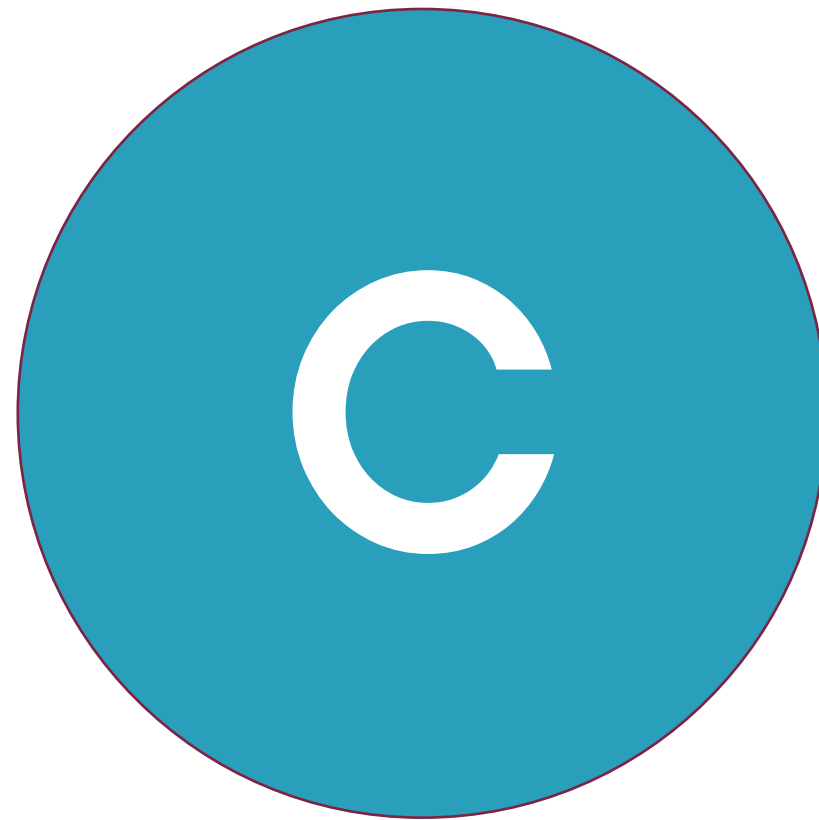
**Undo:
Chargeback and
Refunds**



Steps in the Transaction



**Authorization
and Capture**



Clearing



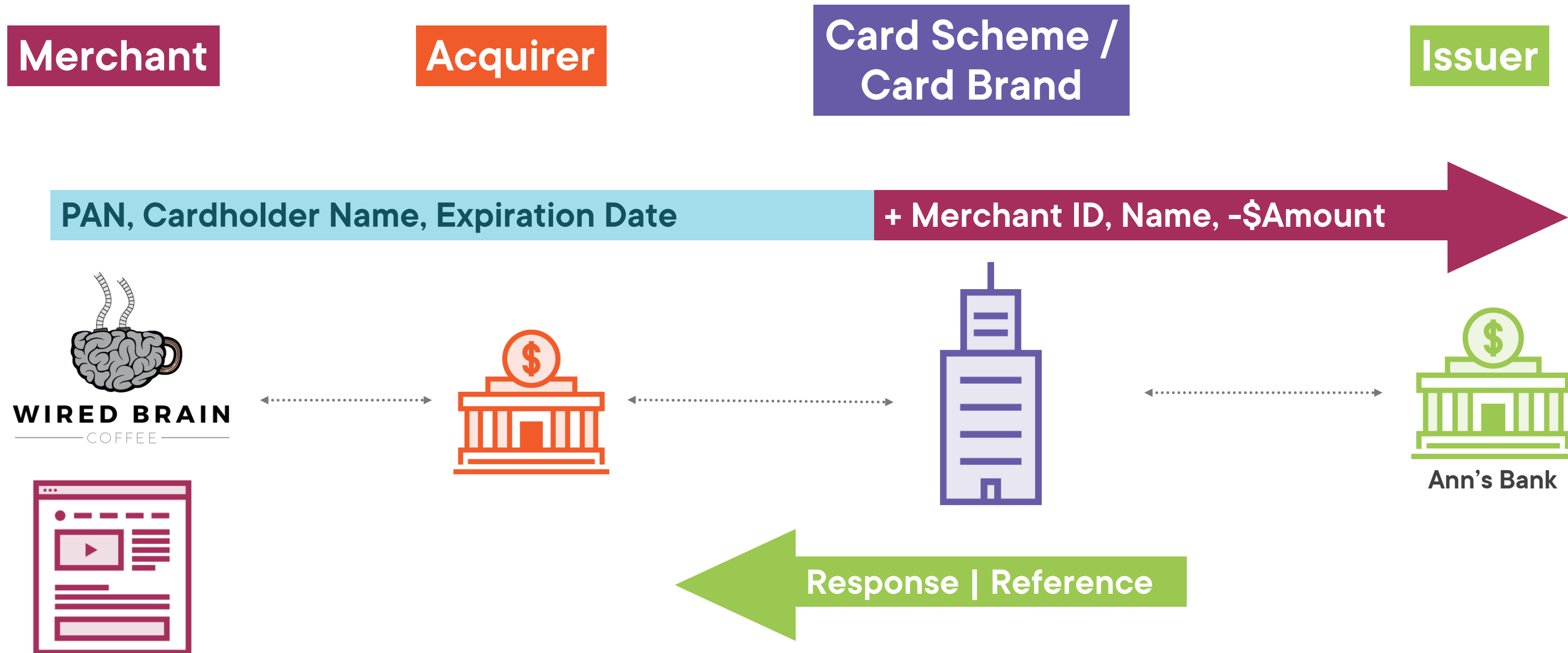
Settlement



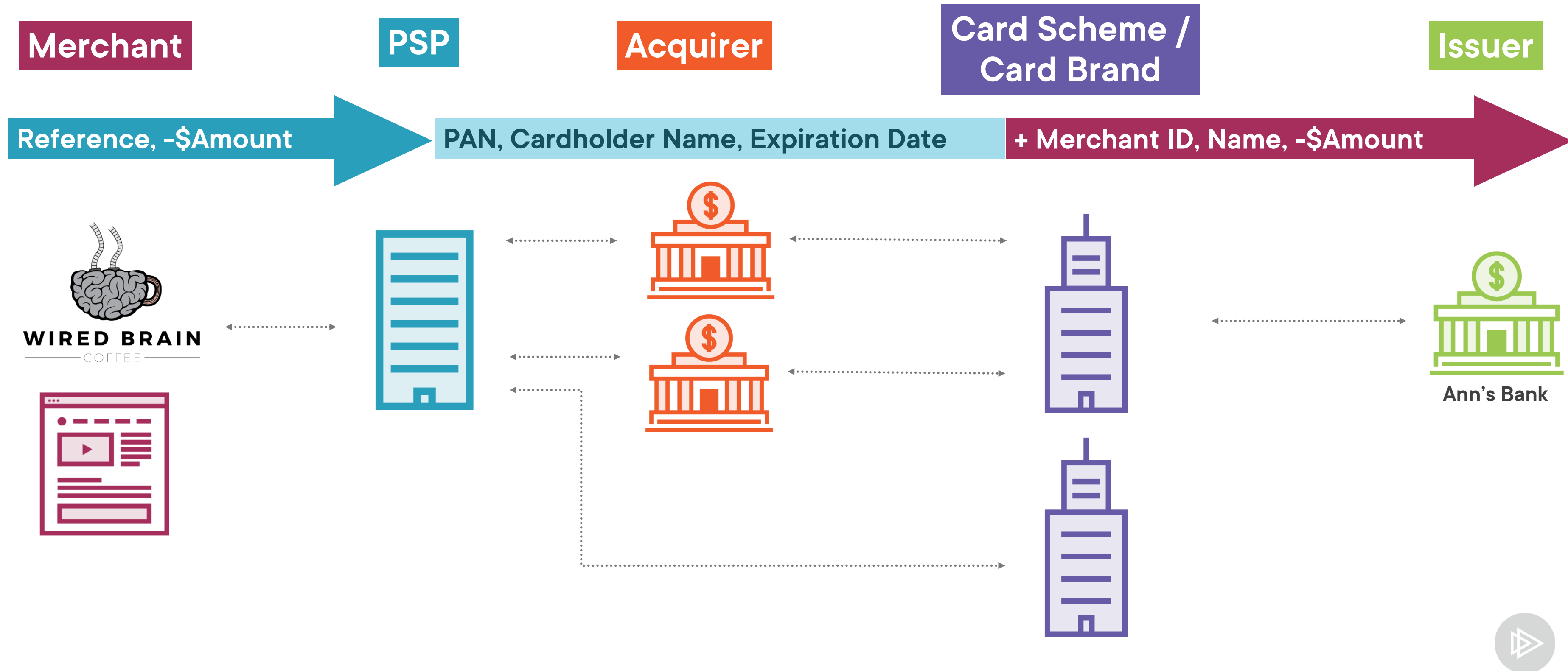
**Undo:
Chargeback and
Refunds**



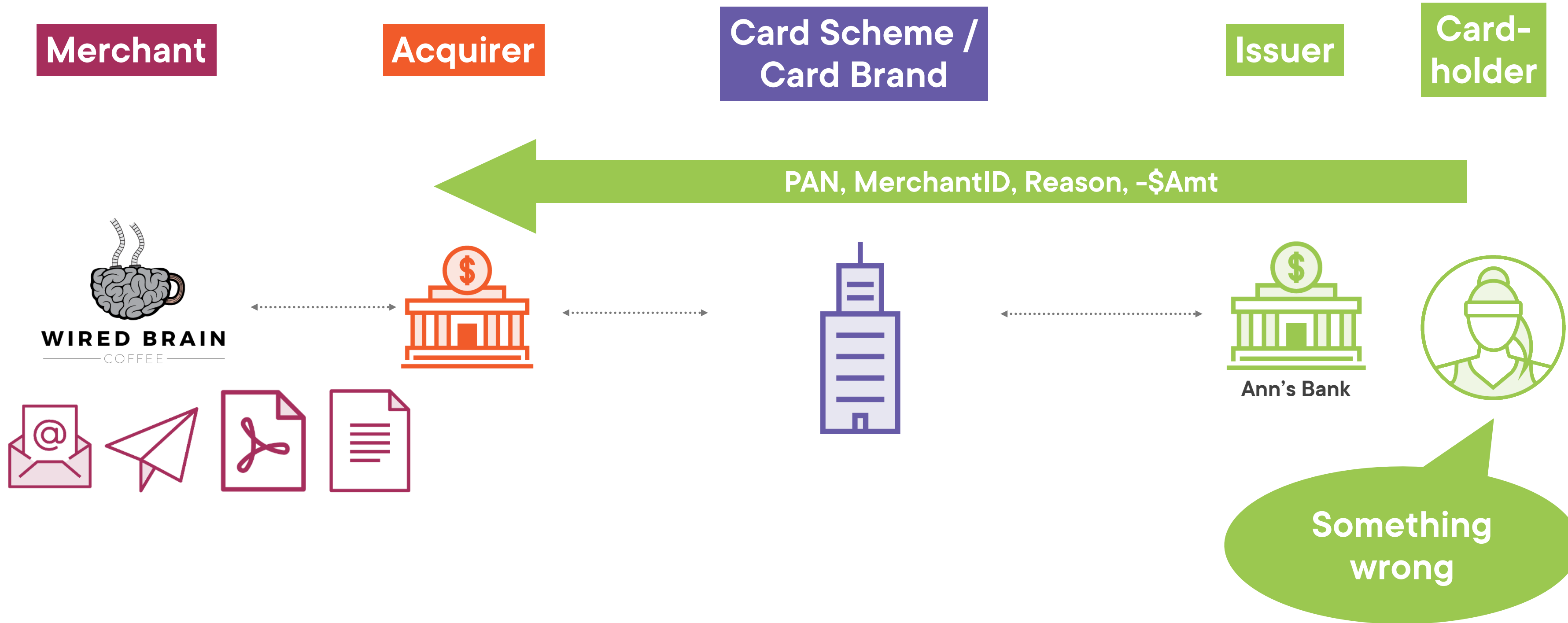
Refund: Merchant Initiates



Refund: Merchant Initiates



Chargeback: Cardholder Initiates



Not All Transactions Use Cards



Cash Authorization

Cardholder

ATM Bank

Card Scheme /
Card Brand

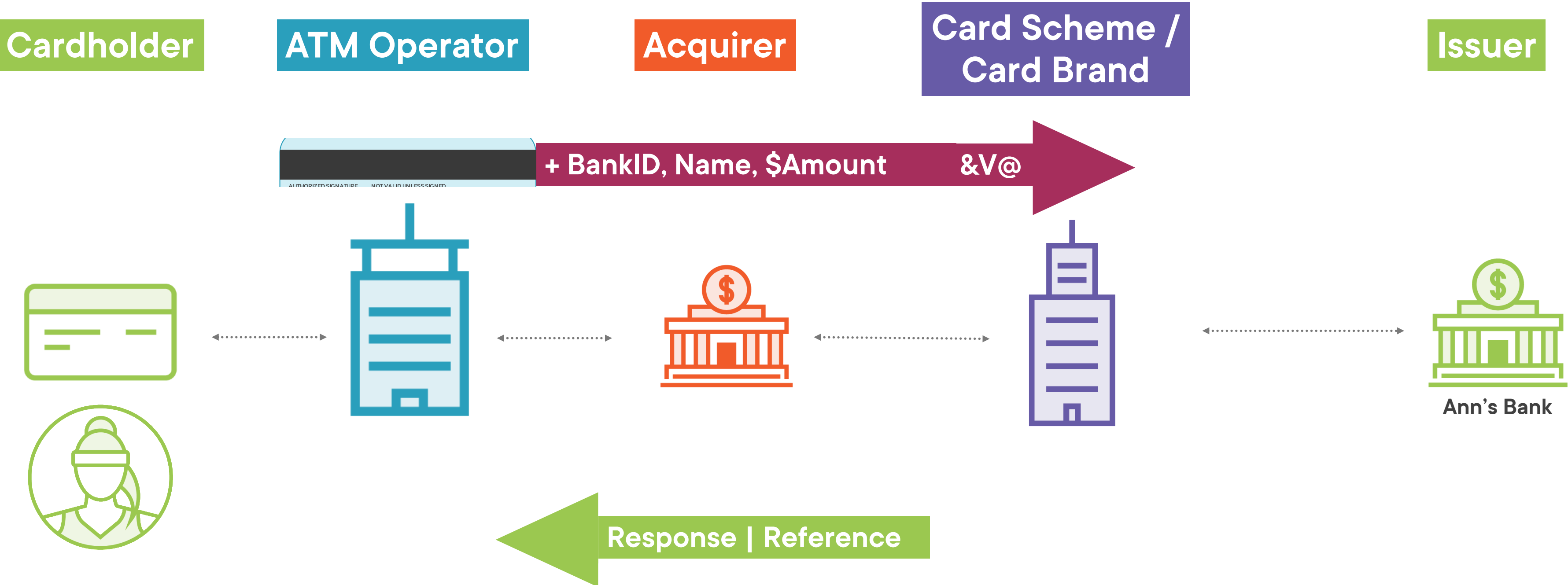
Issuer



Ann's Bank



Cash Authorization – ATM Operators



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



Participants: Summary



Issuing banks (ISSUERS) and CARD SCHEMES (3-party) provide cards to CARDHOLDERS

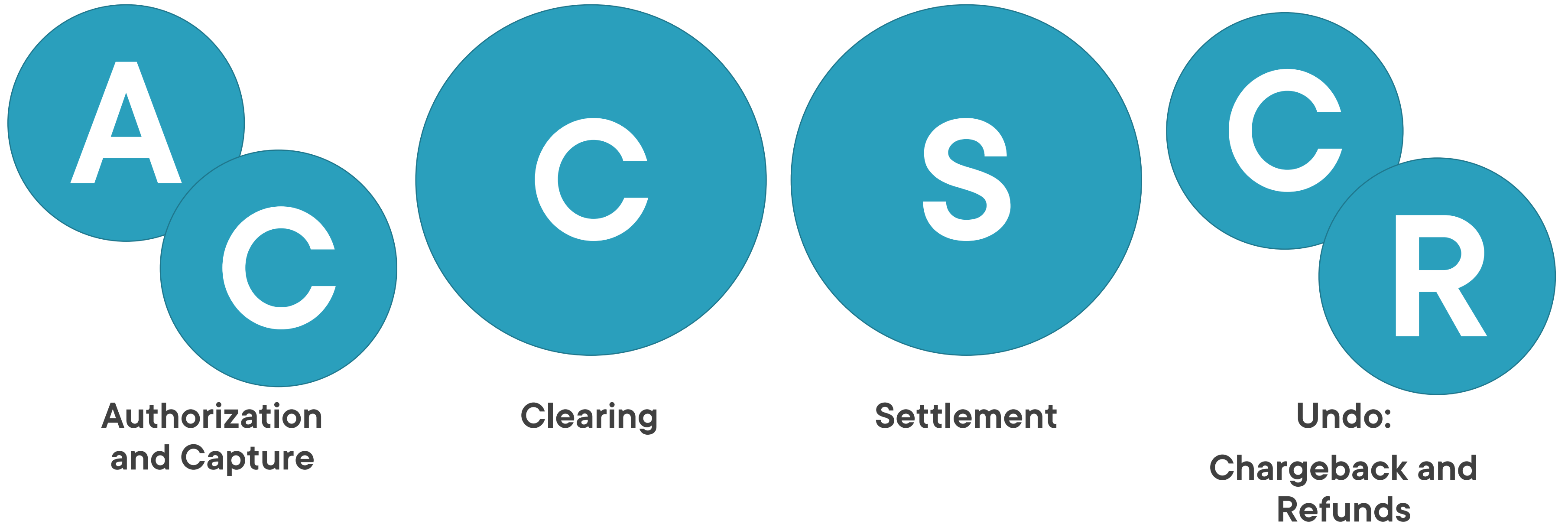
Acquiring banks (ACQUIRERS) and card schemes (3 party) acquire transactions from MERCHANTS

Card schemes (4 party) connect acquirers to issuers

PAYMENT SERVICE PROVIDERS (PSP) and PAYMENT FACILTATORS (PF) contract with merchants to send the transactions to acquirers



Steps in the Transaction



The Key Steps: Summary



In **AUTHORIZATION**, the merchant checks with the issuing bank that they will be paid

In **CAPTURE**, a merchant confirms the transaction has taken place

In **CLEARING**, merchants and acquirers summarize their daily transactions, issuers debit the cardholder account

In **SETTLEMENT**, issuers transfer money to acquirers and the acquirer pays the merchant

A merchant can **REFUND** a transaction

A cardholder can **CHARGEBACK** a transaction (via their issuer)



Remember:
The world is a **very** big place

