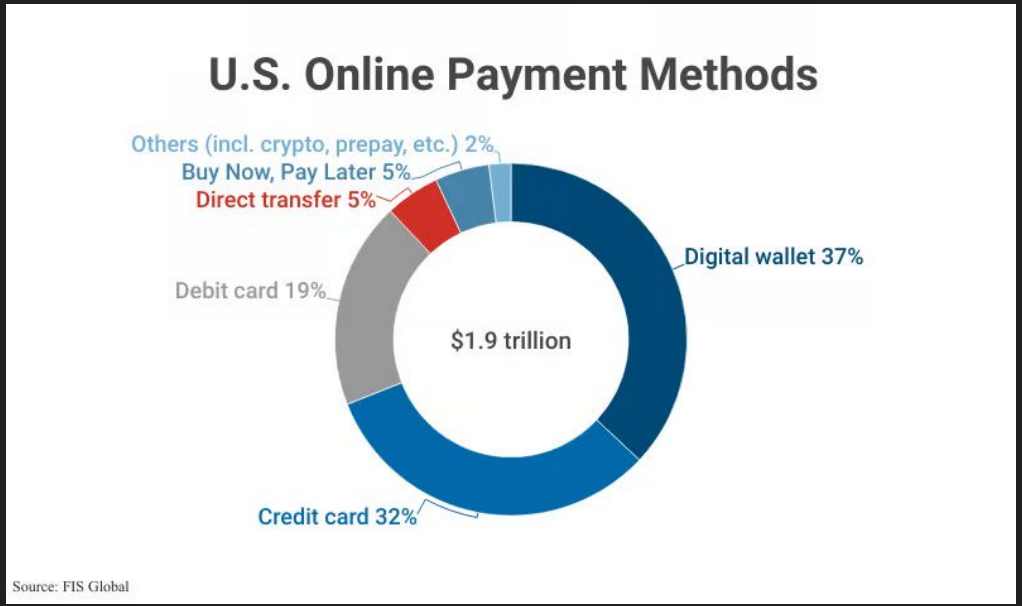
Online Payments: Attack and Defense

Or, how to stay safe while accepting credit cards as an online merchant

Overview

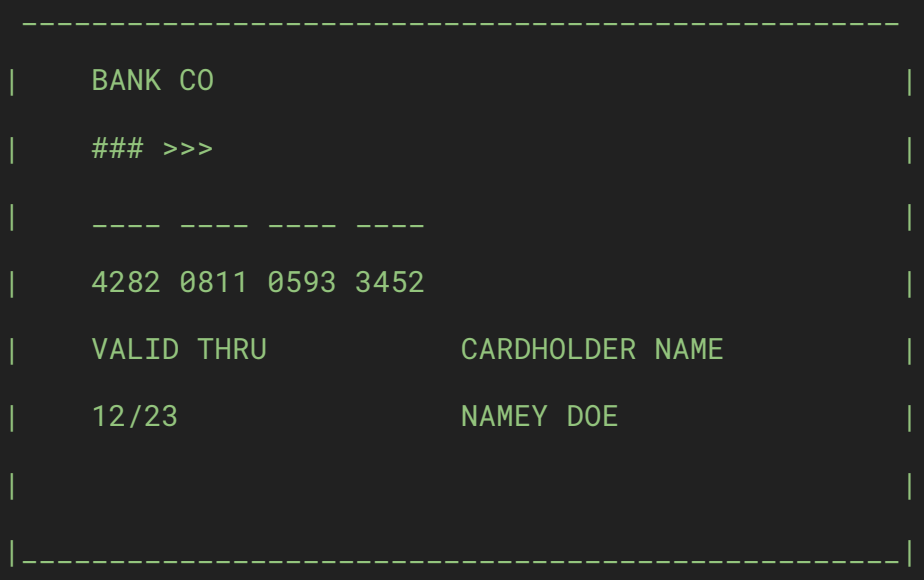
- Credit Cards
- Attacks/Threats
  - Motivation and Methods
  - Defense
- Balancing Risk

Why Credit (and Debit) Cards?



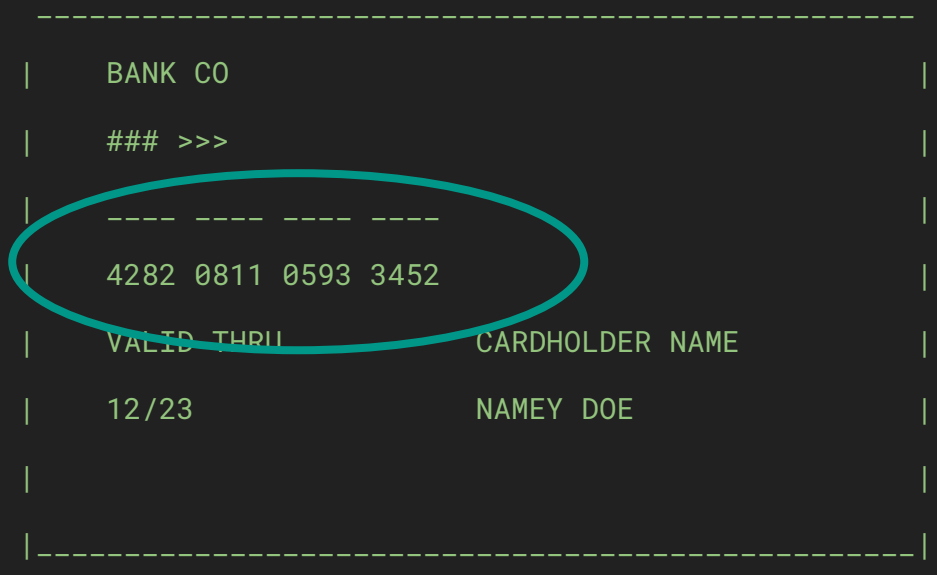
[1] https://capitaloneshopping.com/research/most-popular-online-payment-methods/

Credit Card Anatomy



Credit Card Anatomy

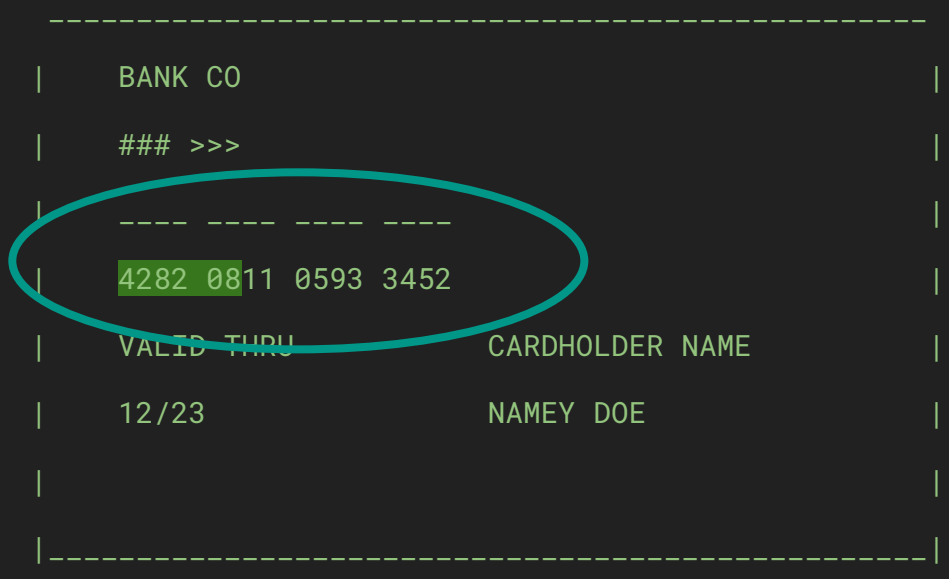
Primary Account Number (PAN)



Credit Card Anatomy

Primary Account Number (PAN):

- Bank ID Number (BIN)



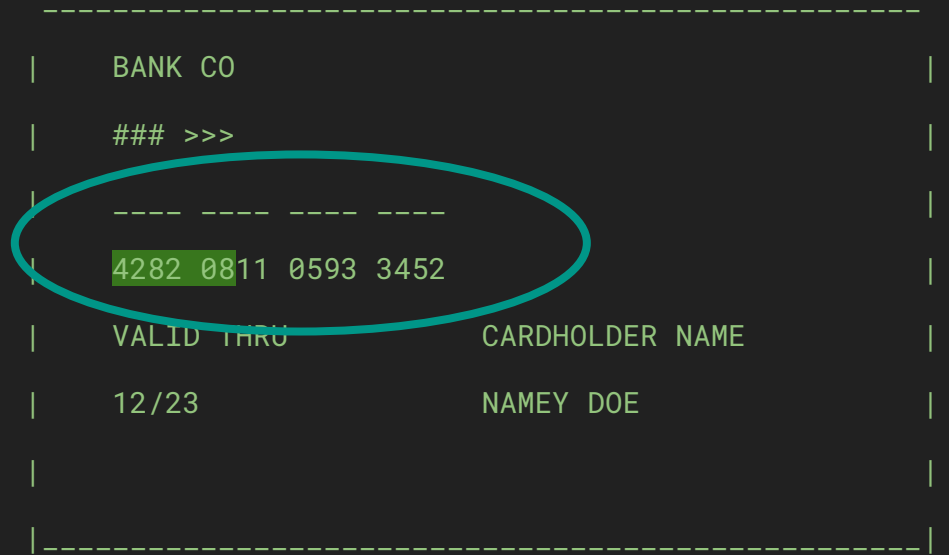
Credit Card Anatomy

Primary Account Number (PAN):

- Bank ID Number (BIN)

```
curl -H "Accept-Version: 3" "https://lookup.binlist.net/45717360"
```

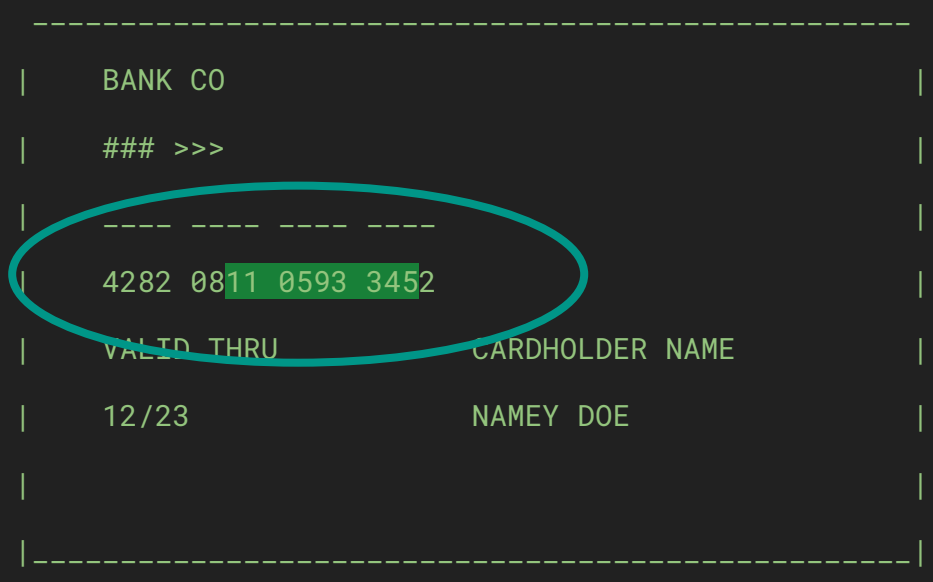

```
{
  "number": {
    "length": 16,
    "luhn": true
  },
  "scheme": "visa",
  "type": "debit",
  "brand": "Visa/Dankort",
  "prepaid": false,
  "country": {
    "numeric": "208",
    "alpha2": "DK",
    "name": "Denmark",
    "emoji": "🇩🇰",
    "currency": "DKK",
    "latitude": 56,
    "longitude": 10
  },
  "bank": {
    "name": "Jyske Bank",
    "url": "www.jyskebank.dk",
    "phone": "+4589893300",
    "city": "Hjørring"
  }
}
```

Credit Card Anatomy

Primary Account Number (PAN):

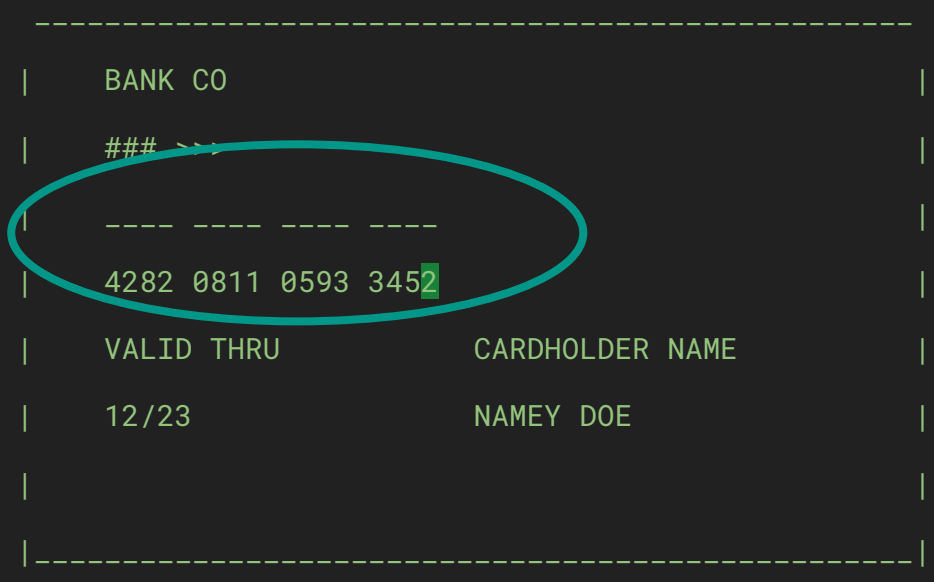
- Bank ID Number (BIN)
- Account Identifier



Credit Card Anatomy

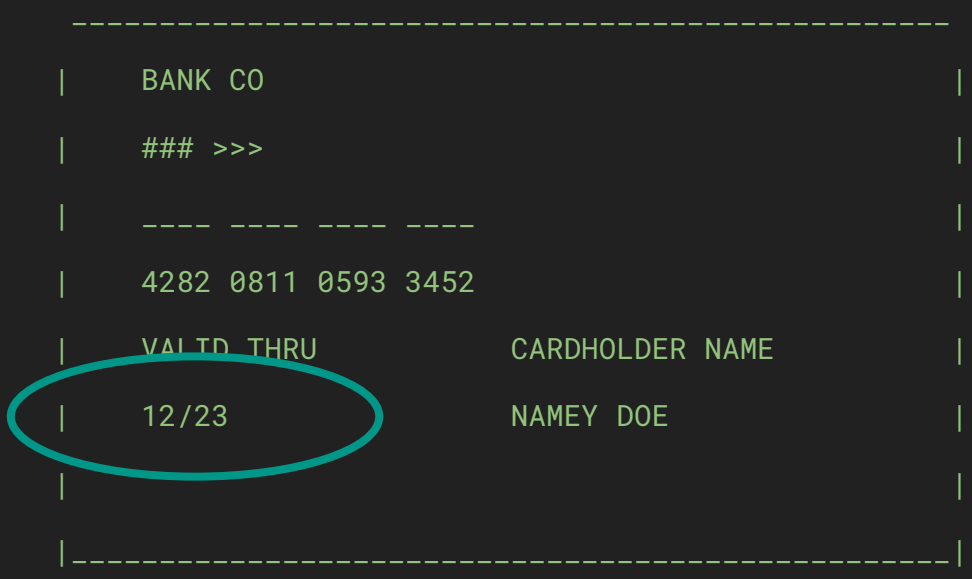
Primary Account Number (PAN):

- Bank ID Number (BIN)
- Account Identifier
- Check Digit



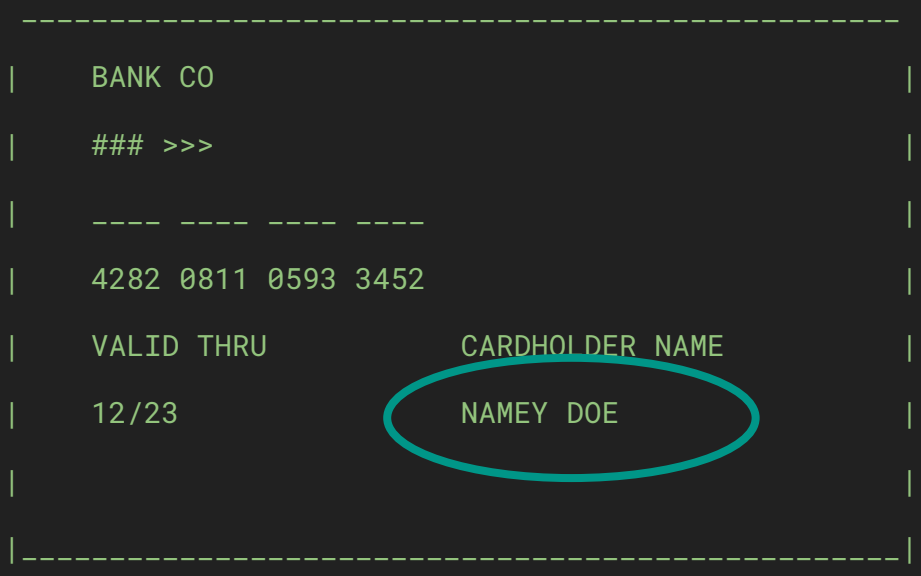
Credit Card Anatomy

- Expiration date



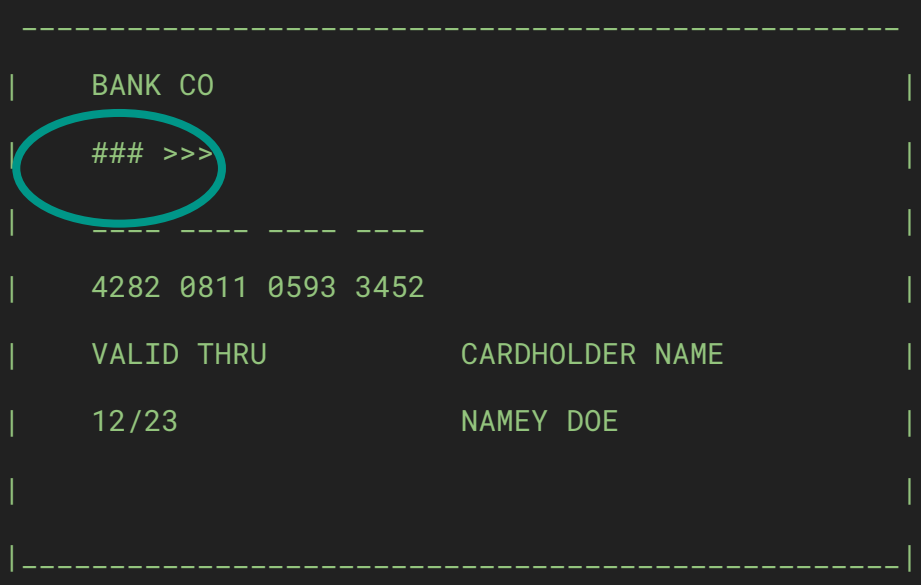
Credit Card Anatomy

- Cardholder name



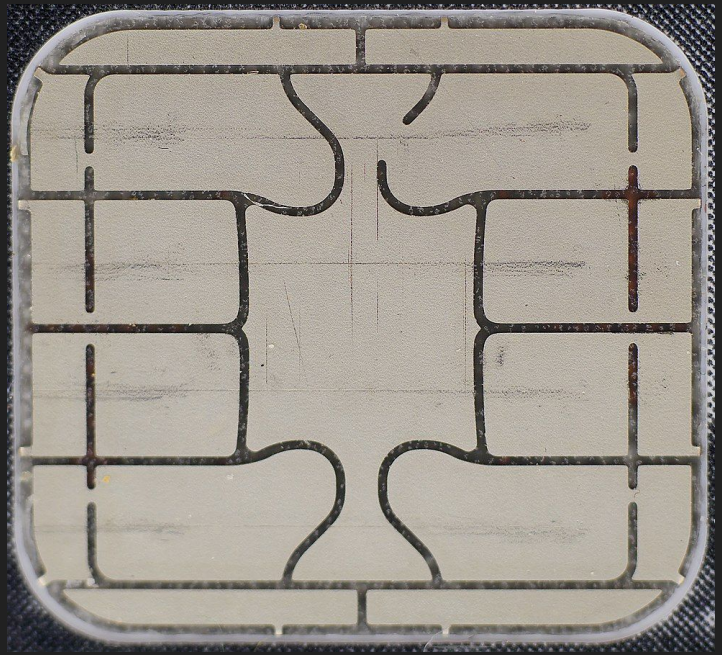
Credit Card Anatomy

- EMV Chip



Credit Card Anatomy

- EMV Chip



```
 ------------------------------------------------
|    BANK CO                                     |
|    ### >>>                                     |
|    ---- ---- ---- ----                         |
|    4282 0811 0593 3452                         |
|    VALID THRU           CARDHOLDER NAME        |
|    12/23                NAMEY DOE              |
|                                                |
|________________________________________________|
```

Credit Card Anatomy

- EMV Chip + NFC


```
 ------------------------------------------------
|    BANK CO                                     |
|    ### >>>                                     |
|    ---- ---- ---- ----                         |
|    4282 0811 0593 3452                         |
|    VALID THRU          CARDHOLDER NAME         |
|    12/23               NAMEY DOE               |
|                                                |
|________________________________________________|
```

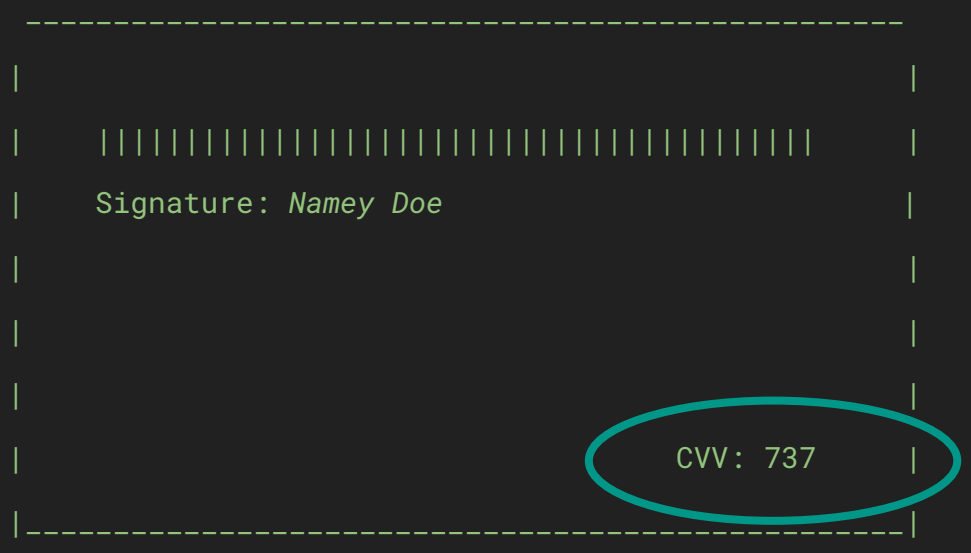
[1] https://www.rewire.com/blog/2019/11/06/transparent-credit-card/

Credit Card Anatomy

Back of Card

Credit Card Anatomy

Back of Card



Card-Not-Present

Cardholder not physically present at the time of transaction.

- Mail order
- Telephone
- Fax

Card-Not-Present

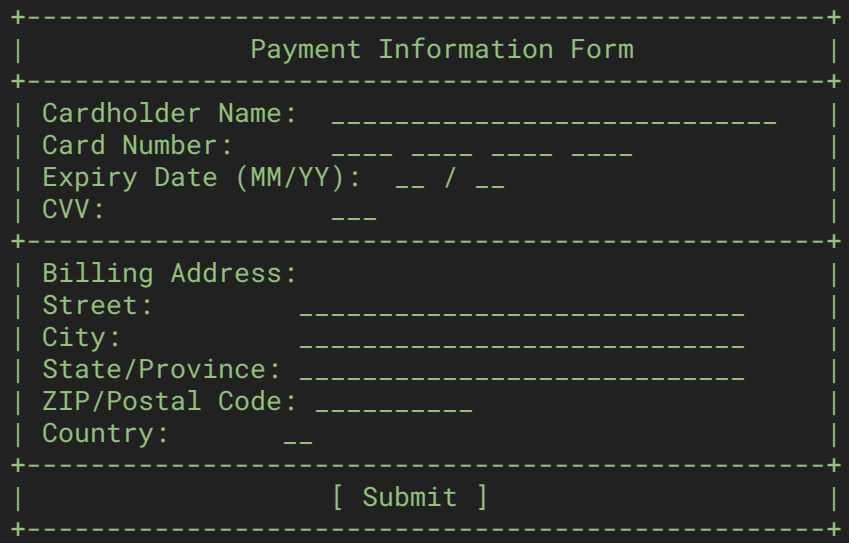
Cardholder not physically present at the time of transaction.

- Mail order
- Telephone
- Fax
- The *internet*

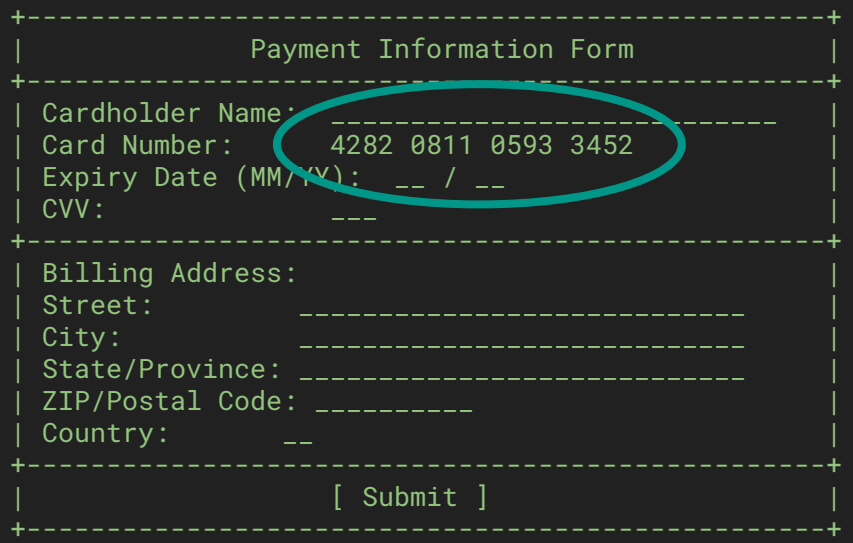
Card-Not-Present

- No EMV, no magstripe
- What’s required?

Card-Not-Present



Card-Not-Present



Card-Not-Present

Validation available from the issuer

- CVV2 / CVS
- Address (full or partial) / AVS
- Cardholder Name / ANI
- 3-D Secure (surprise sometimes required)

We’ll come back to these in detail.

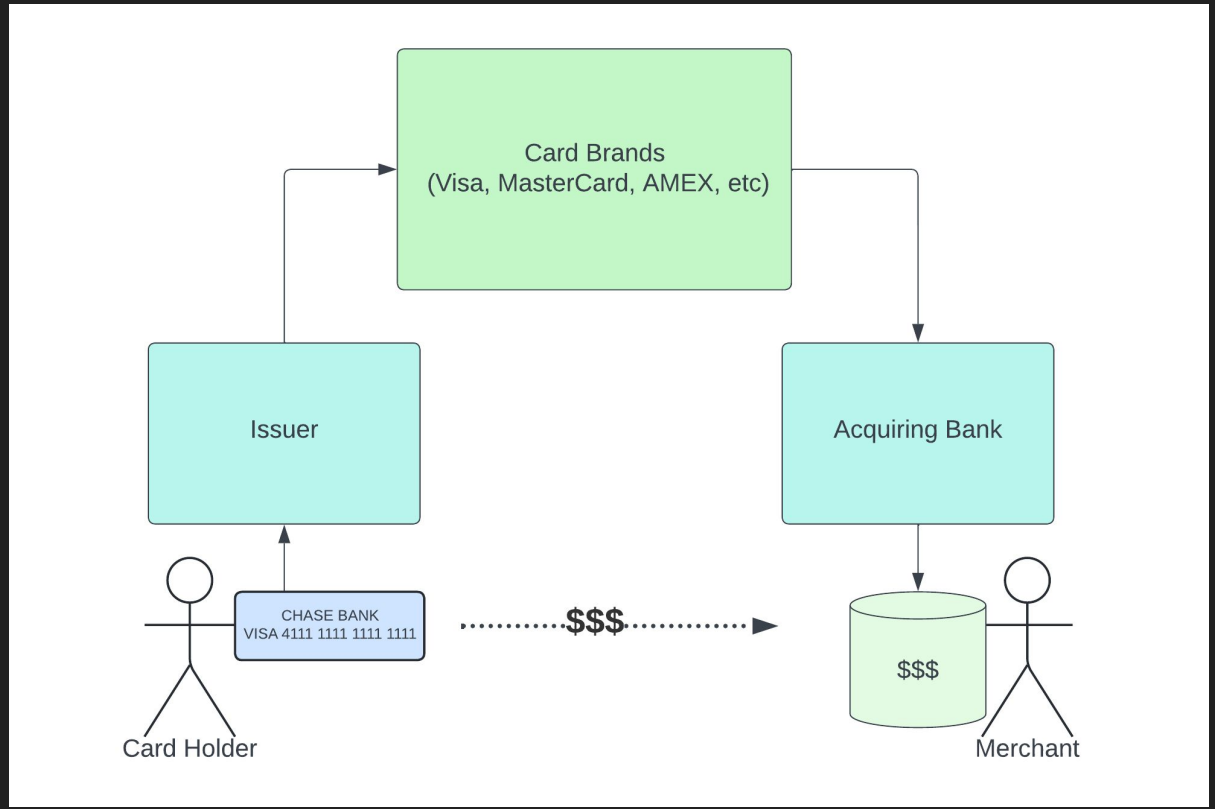
What’s a Merchant

“… any *entity* that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services.” (PCI-DSS)

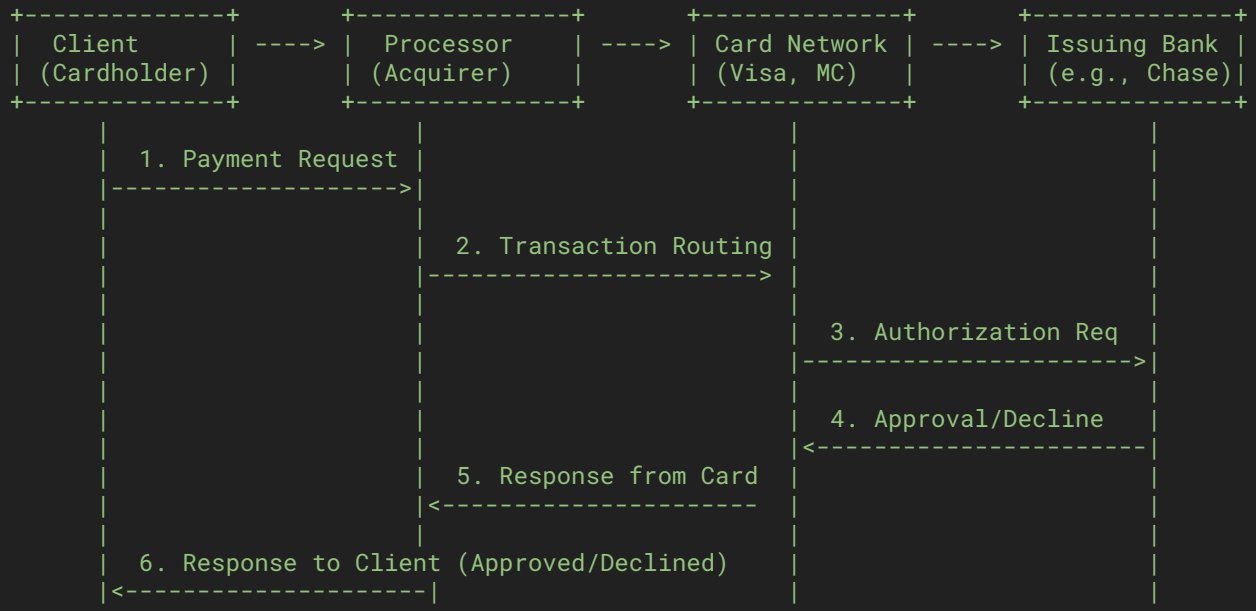
or…

You have customers that are paying you for goods or services (with credit cards).

Card Holder -> Merchant



Card Network



Threats

Threats

1. Data Thieves
    a. Compromise your system to steal card details
2. Card Testers
    a. Use your system to verify/attest card details
3. Fraudsters
    a. Use your system to extract value through goods, services or monetary value with stolen card details.

Not covered: ATO, friendly fraud, phishing

Threat #1: Data Thieves

Data Thieves

- Skimming - intercept card details without being noticed.
- Find card data at rest
  - Logs, database
  - Plaintext, encrypted, hashed

Data Thieves

Value

- Sell the card data to other criminals
- Or, use the card data for fraud themselves

Data Thieves

2018 British Airways hack

- 380,000 cardholder details compromised including address and CVV[1]

[1] https://www.reuters.com/article/us-iag-cybercrime-british-airways/ba-apologizes-after-380000-customers-hit-in-cyber-attack-idUSKCN1LM2P6

Data Thieves

2018 British Airways hack

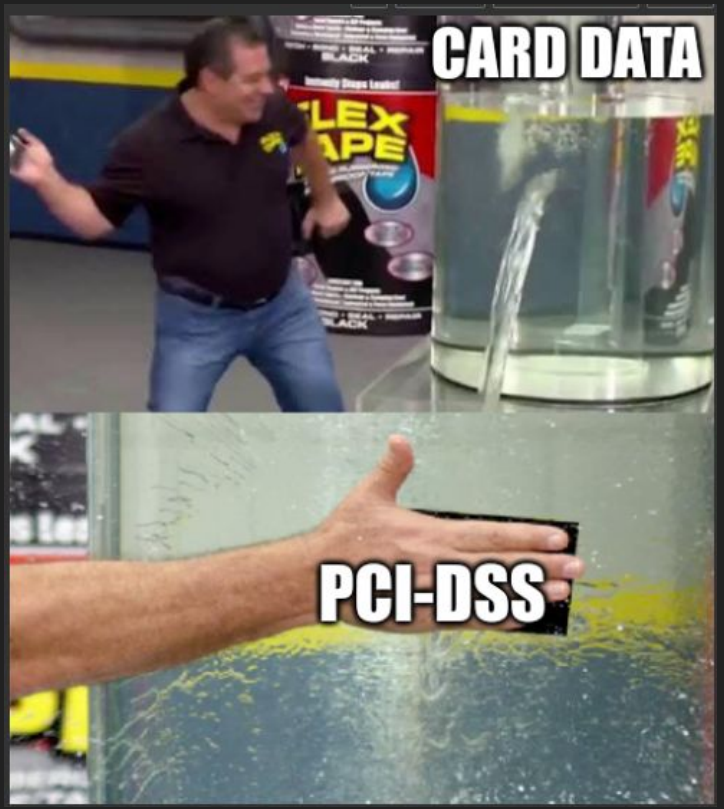
- Skimming - intercepted card details on the front-end with malicious javascript[1]
- Data at rest - found 95 days worth of card details in unencrypted logs[1]

[1] https://web.archive.org/web/20240206185013/https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf

Data Thieves

Detection and Mitigation

- Payment Card Industry Data Security Standard (PCI-DSS)

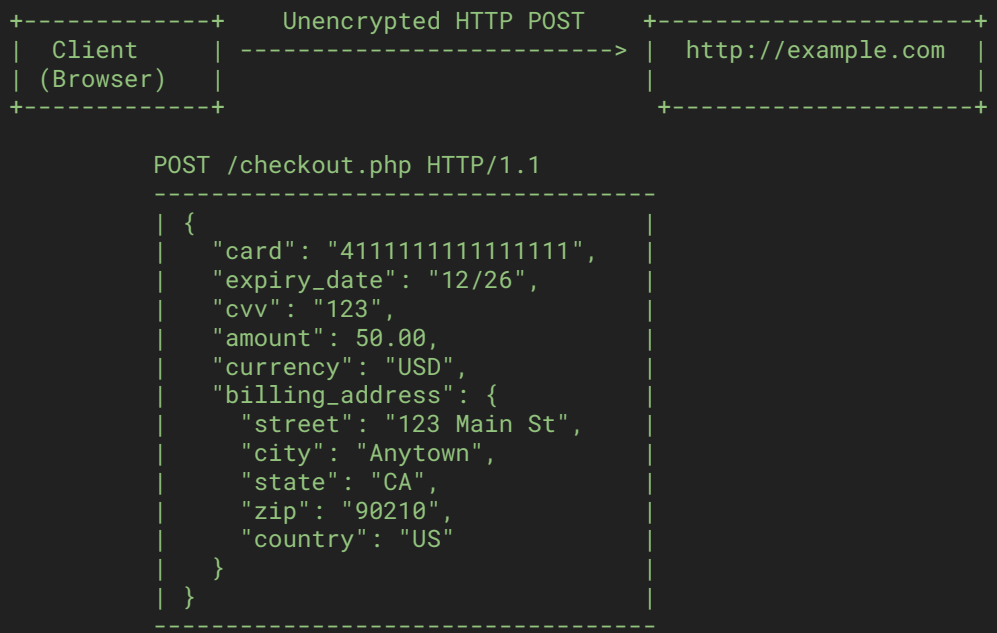


Data Thieves

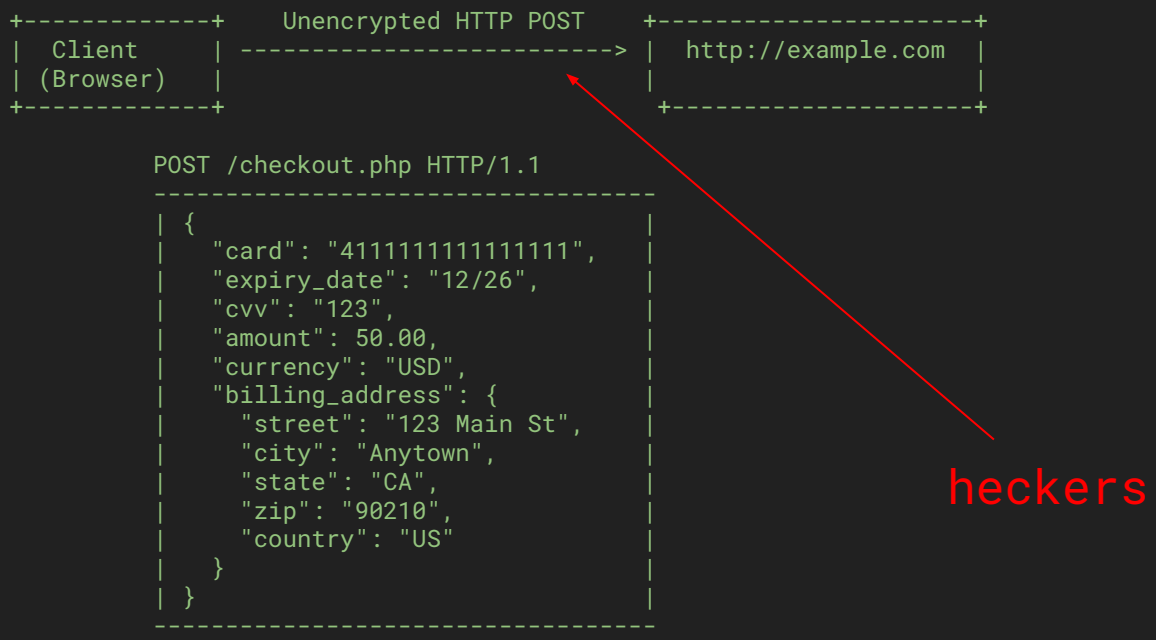
PCI-DSS

- Protect Cardholder Data at rest and in transit
- Maintain a Secure Network
- Implement Strong Access Controls and Monitoring
- Also fines

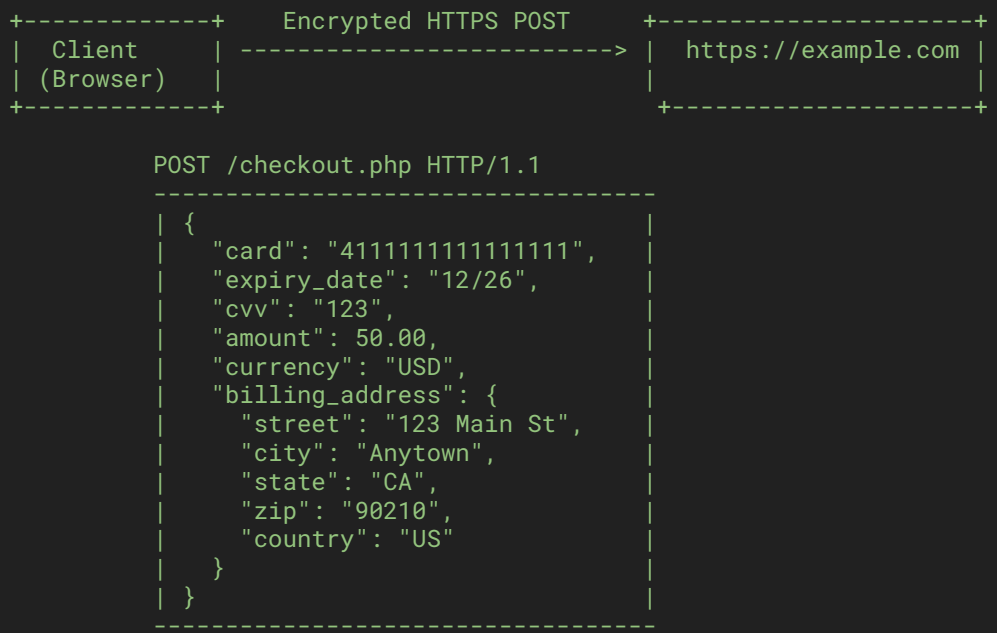
Data Thieves



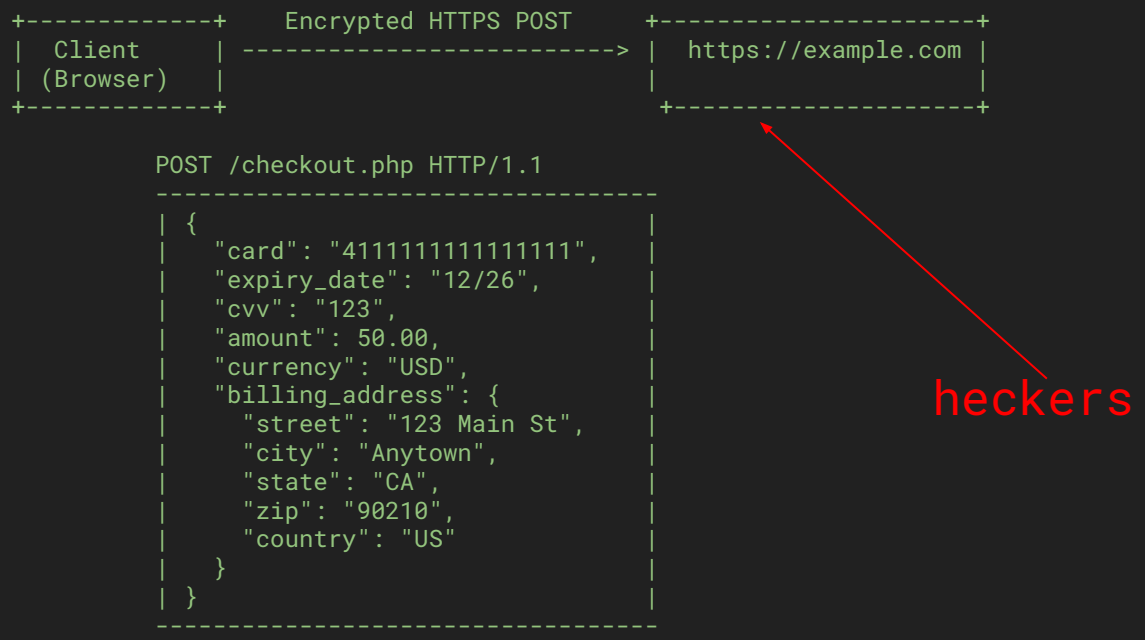
Data Thieves



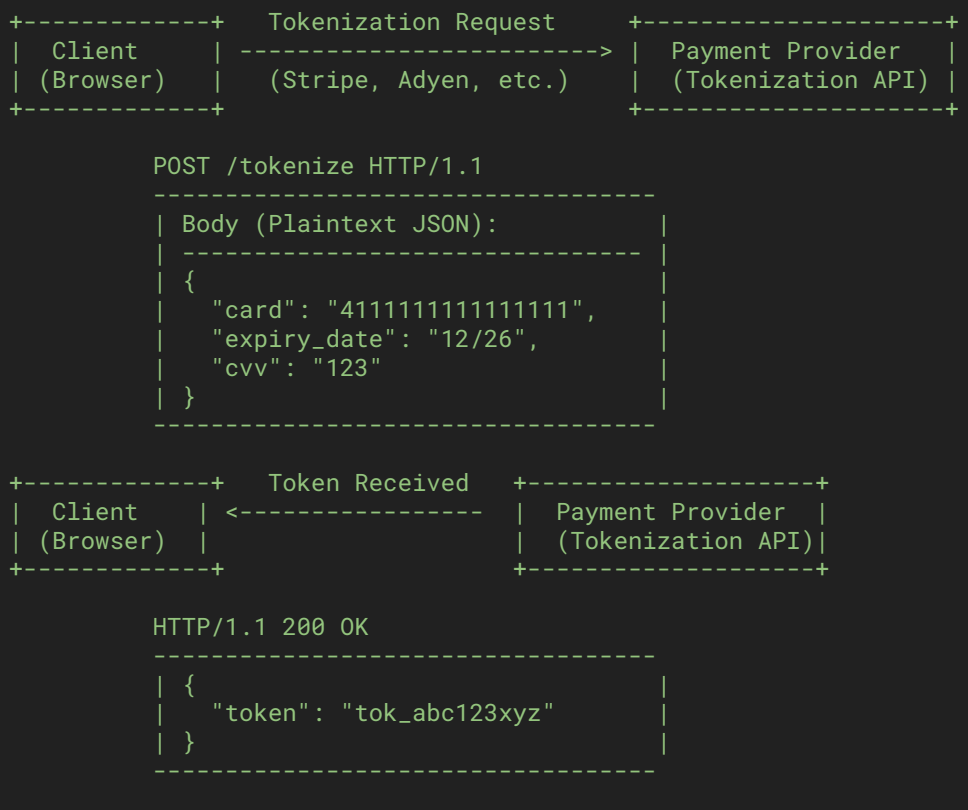
Data Thieves



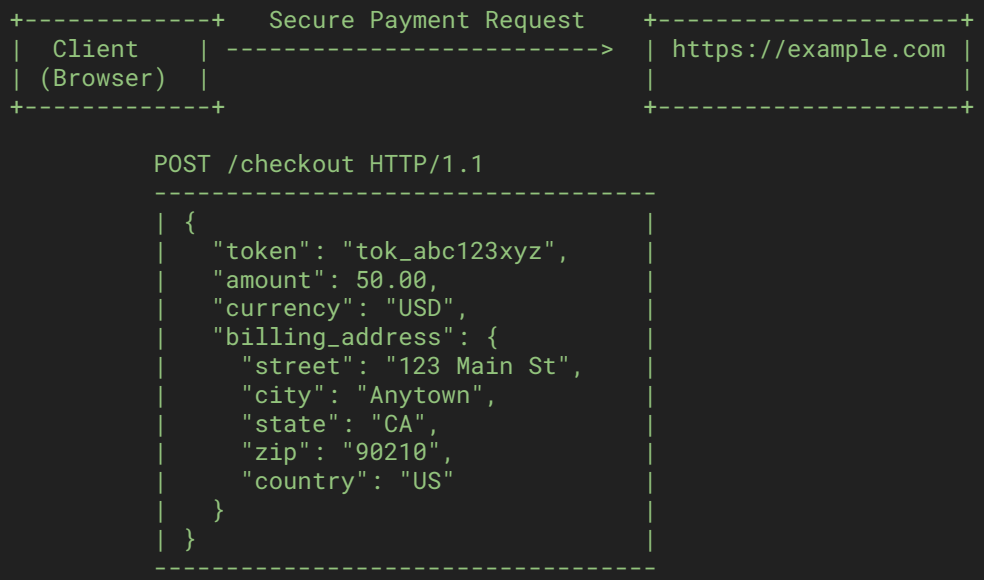
Data Thieves



Data Thieves



Data Thieves



Data Thieves

Mind the front-end

- Keeping data away from the backend isn’t enough
- PCI DSS v4.0 has lots of guidance on front-end

(iframe, subresource integrity, monitor changes)

Data Thieves

Storing Card Data

- Simply Do Not

Threat #2: Card Testers

Card Testers

- Use you as a way to test out unverified card data
  - Purchased cheaply on illegal marketplaces
- Use you to guess card numbers from partial data
  - Partial data from other breaches, or BIN stuffing

Card Testers

Value

- Sell the now cleaned, verified card data
- Or, use the card data themselves for fraud

Card Testers

- Stolen card details are bought and sold regularly at online marketplaces.
- Data quality is major factor in price.

Bin	Type	Debit/Credit	Subtype	Exp Date	Track1	Billing zip	Code	Country	Address	Bank	Base	Price	Cart
493404		CREDIT	N/A	XX/23	✔	-	201		N/A	EUFISERV ( ); non refundable	Paramount	40.95 $	
492184		CREDIT	N/A	XX/23	✔	-	201		N/A	KRUNG THAI BANK PUBLIC CO., LTD. ( ); non refundable	Paramount	40.95 $	
440066		CREDIT	SIGNATURE	XX/23	-	-	201		N/A	N/A ( )	Paramount	25.20 $	
440066		CREDIT	SIGNATURE	XX/23	-	-	201		N/A	N/A ( )	Paramount	25.20 $	
517604		CREDIT	N/A	XX/24	-	-	201		NY	CHINA MINSHENG BANKING CORP., LTD. ( ); non refundable	BMW	49.14 $	
490624		CREDIT	N/A	XX/23	-	-	201		N/A	BC CARD CO., LTD. ( )	Paramount	32.76 $	
557729		CREDIT	ELECTRONIC	XX/23	✔	-	201		N/A	UNICREDIT BANK HUNGARY ZRT. ( )	Paramount	40.95 $	
490765		CREDIT	CLASSIC	XX/23	✔	-	201		N/A	TOPCARD SERVICE, S.A. ( ); non refundable	Paramount	40.95 $	
522094		DEBIT	PREPAID	XX/27	-	-	201			BANCO BILBAO VIZCAYA ARGENTARIA PUERTO RICO ( )	Lotta	26.52 $	
529580		DEBIT	PREPAID	XX/26	-	-	201		FL	VINCENTO PAYMENT SOLUTIONS, LTD. ( )	Album	26.52 $	

https://webz.io/dwp/the-top-5-deep-and-dark-web-credit-card-sites/

Card Testers

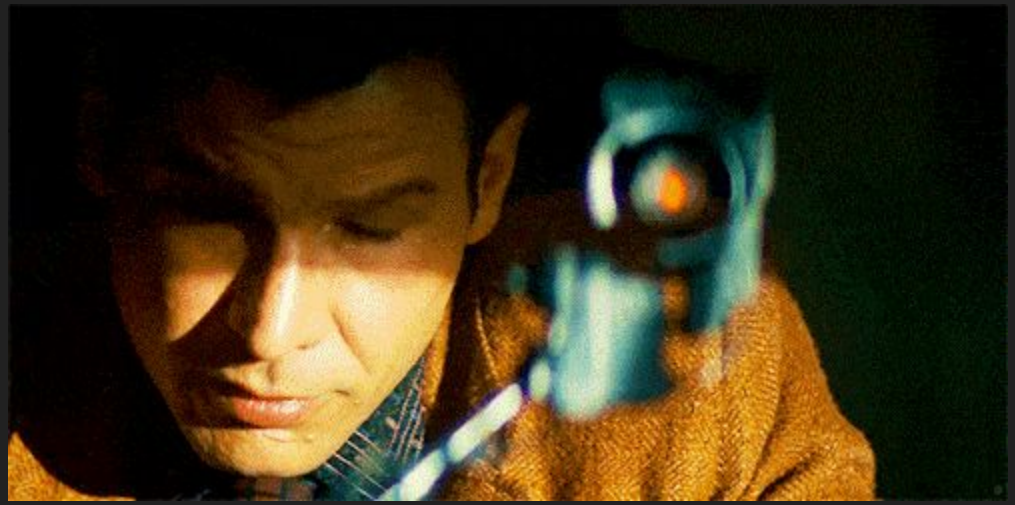
Detection

- Auth rates / conversion
- Anomalous traffic sources and patterns
- Low value transactions
- Chargebacks (late and expensive)

Card Testers

Mitigation

- Low-hanging fruit: bot protection + rate limiting
- Reduce volume by driving up cost for attackers



Card Testers

Mitigation

- Bot protection and rate limiting
- Use data provided by issuer
  - CVV
  - AVS
  - ANI (rare)
- 3DS

Card Testers

- CVV
  - Don’t ever store this

Code	Description
M	Match
N	No Match
P	Not Processed
S	Merchant has indicated that CVV2 is not present on card
U	Issuer is not certified and/or has not provided encryption key
I	Invalid or no response

Card Testers

- AVS (address)

Code	Description
Y	Full Match
A	Partial Match (street address only)
Z	Partial Match (postal/zip only)
N	Non-Match
U	Unable to Verify
R	Indeterminate Outcome (Retry)

Card Testers

3DS (3D Secure)

- Not entirely up to merchant
  - You can request exemption
  - You can request mandatory
- Used much more widely outside of the US

Card Testers

- Don’t be a cheap oracle!
  - e.g “The CVV is incorrect”
- Other step-ups, trade-offs

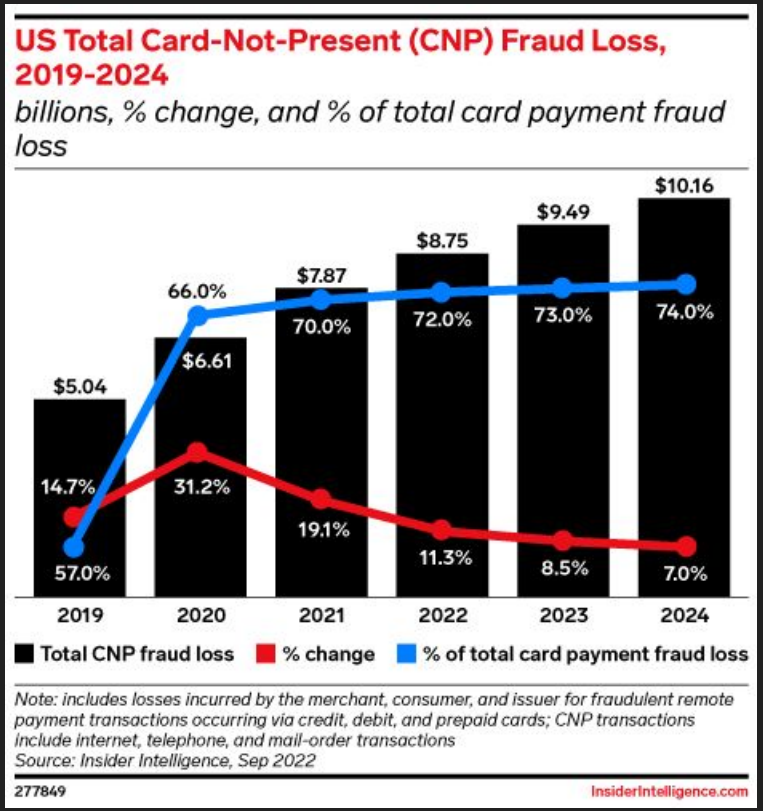
Threat #3: Fraudsters

Fraudsters

- Use stolen card details to purchase goods or services.
- Or, more directly extract money through self-payment.

Fraudsters

- Billions of dollars lost annually to Card-Not-Present fraud in the US alone



Fraudsters

Detection

- Anomalous patterns, maybe
- Auth rates and conversion hits, maybe
- Chargebacks :’(

Fraudsters

Mitigation

- CVV, AVS, 3DS
- Address matching
- In-house rules, tools from vendors

Balancing Risk

The merchant has to balance deterring bad actors, with the risk of turning away good customers.

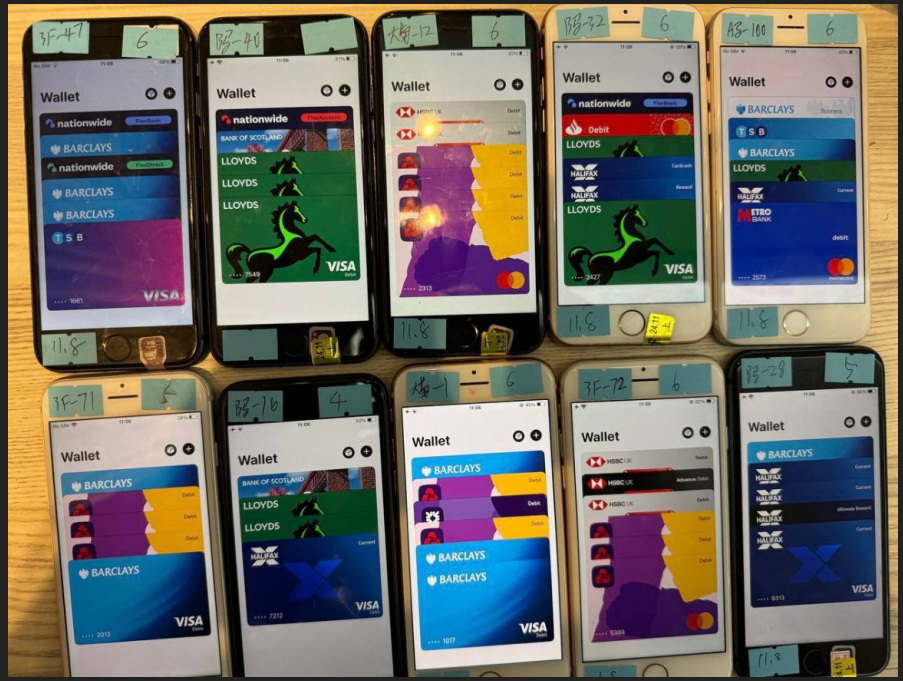
The ideal system would block 100% of bad traffic and convert 100% of good customers. This does not exist.

Balancing Risk

- No silver bullets
- Pull in different signals
- Make good decisions

Bonus: Smishing and Next-Gen carding

- Trick victims into enrolling cards into attackers wallets



https://krebsonsecurity.com/2025/02/how-phished-data-turns-into-apple-google-wallets/

The End

- More secure methods available, but imperfect, and adoption is slow.
- Risk is almost entirely on the merchant.
- Be smart about protecting cardholder data, and avoid storing it whenever possible. Understand PCI beyond the checkboxes.
- Understand the value you provide attackers.
- Don’t be an easy or cheap target.

Q&A / Discussion

Vincent Sloan

on the internet & *world wide web*

vincentsloan.com

hello@vincentsloan.com

Software | Payments | Security | Jiujitsu *not a designer