Online Payments: Attack and Defense

Or, how to not get pwned while processing card-not-present transactions

Overview

- Credit Card Anatomy
- What’s a Card-Not-Present transaction?
- Merchant and Issuer roles
- Threats / Attacks
- Balancing Risk

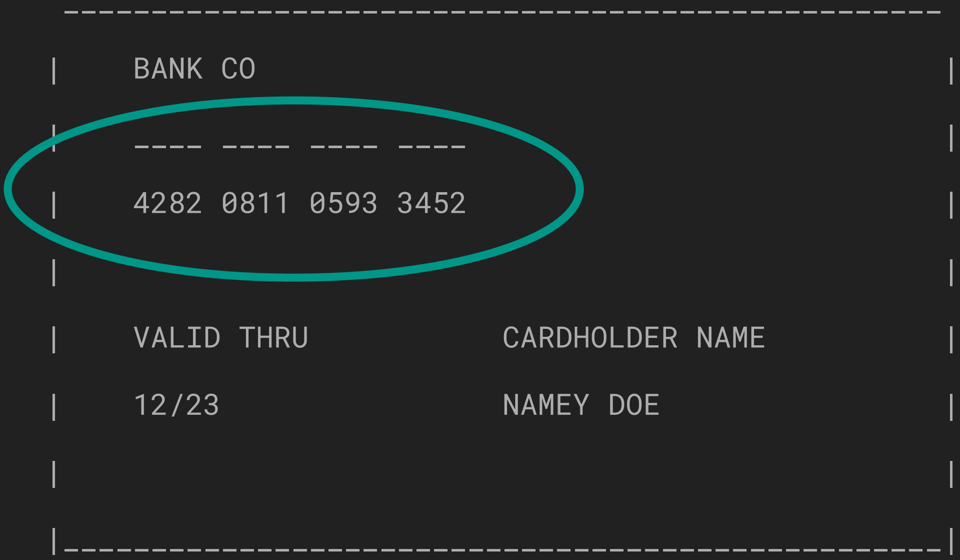
Credit Card Anatomy

Not pictured: EMV chip

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

Credit Card Anatomy

Primary Account Number
(PAN)

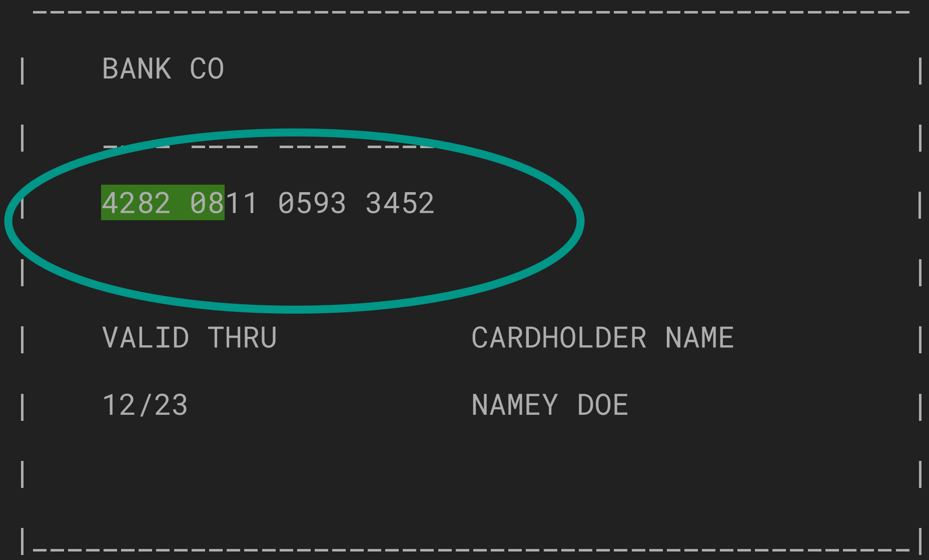


```
 --------------------------------------------------
|    BANK CO                                       |
|    ---- ---- ---- ----                           |
|    4282 0811 0593 3452                           |
|                                                  |
|    VALID THRU           CARDHOLDER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

Credit Card Anatomy

Primary Account Number (PAN):

- Bank ID Number (BIN)

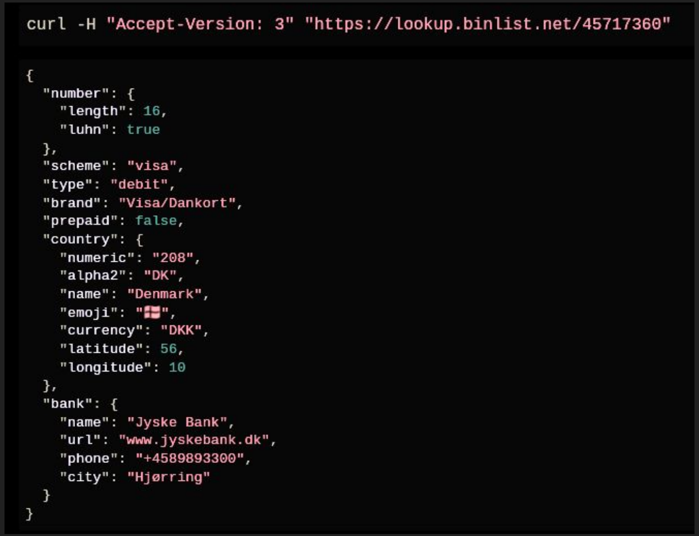


```
 _________________________________________________
|    BANK CO                                      |
|    ---- ---- ---- ----                          |
|    4282 0811 0593 3452                          |
|                                                 |
|    VALID THRU           CARDHOLDER NAME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

Credit Card Anatomy

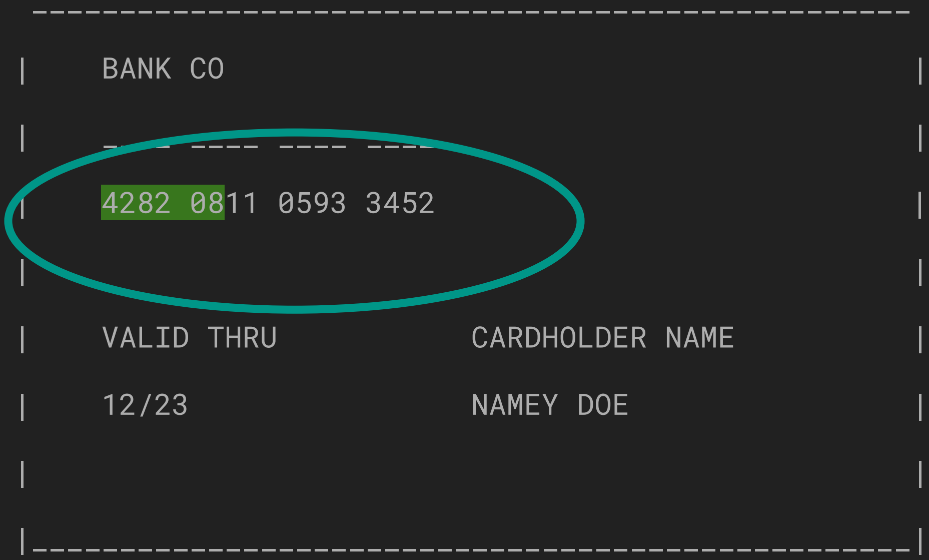
Primary Account Number (PAN):

- 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"
  }
}
```

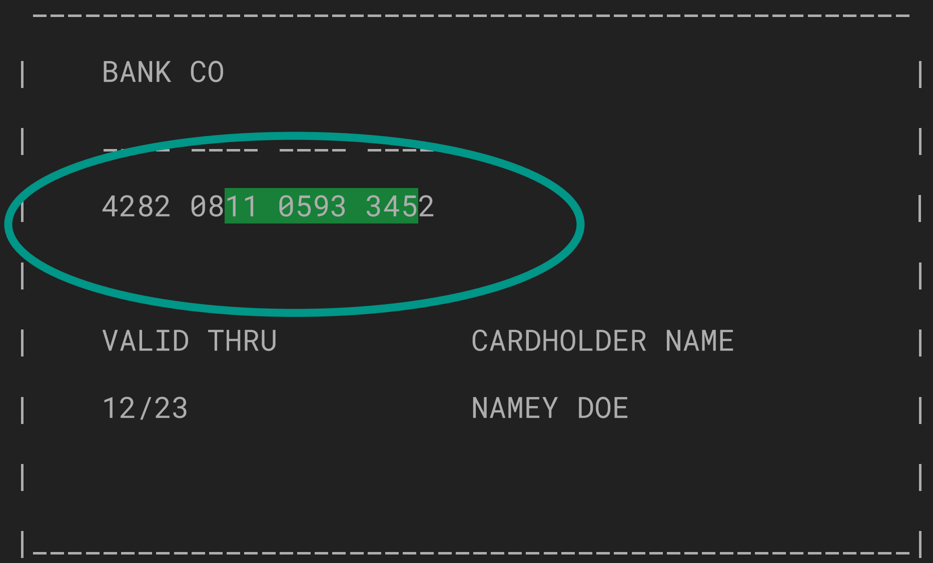


```
 ---------------------------------------------------
|    BANK CO                                        |
|    ____ ____ ____ ____                            |
|    4282 0811 0593 3452                            |
|                                                   |
|    VALID THRU             CARDHOLDER NAME         |
|    12/23                  NAMEY DOE               |
|                                                   |
|___________________________________________________|
```

Credit Card Anatomy

Primary Account Number (PAN):

- Bank ID Number (BIN)
- Account Identifier

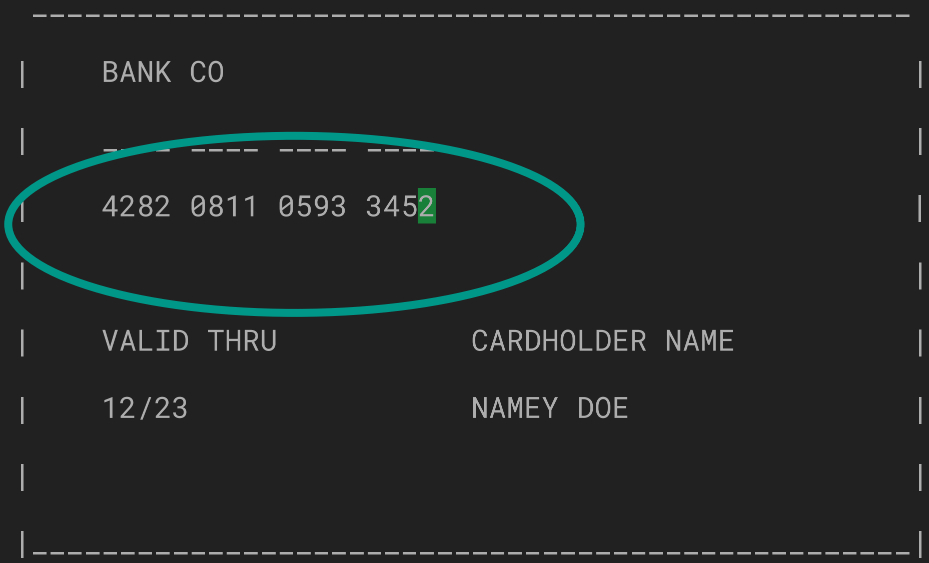


```
 --------------------------------------------------
|    BANK CO                                       |
|    ---- ---- ---- ----                           |
|    4282 0811 0593 3452                           |
|                                                  |
|    VALID THRU            CARDHOLDER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

Credit Card Anatomy

Primary Account Number (PAN):

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



```
 ----------------------------------------
|   BANK CO                              |
|   ____ ____ ____ ____                  |
|   4282 0811 0593 3452                  |
|                                        |
|   VALID THRU      CARDHOLDER NAME      |
|   12/23           NAMEY DOE            |
|                                        |
|________________________________________|
```

Credit Card Anatomy

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

Credit Card Anatomy

Back of Card

```
 --------------------------------------------------
|                                                  |
|    |||||||||||||||||||||||||||||||||||||||||     |
|    Signature: Namey Doe                          |
|                                                  |
|                                                  |
|                                                  |
|                                     CVV: 737     |
|__________________________________________________|
```

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 number (PAN) + expiration date

The rest is (usually) optional -

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.

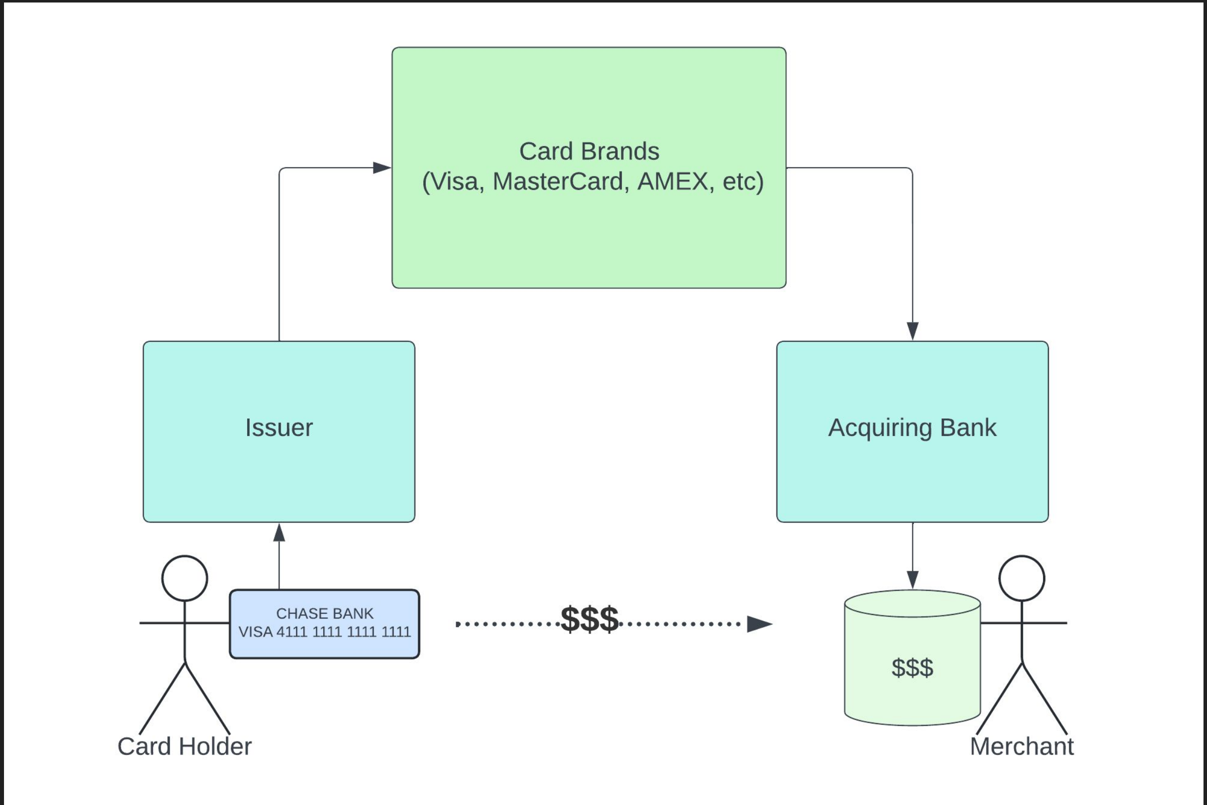
What’s a Merchant

“… 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).

Merchant and Issuer



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 - will try to intercept card details sent transiently, without being noticed.
- Looking for card data at rest (if lucky!)
  - Logs, database
  - Plaintext, encrypted, hashed
- PCI-DSS

Data Thieves

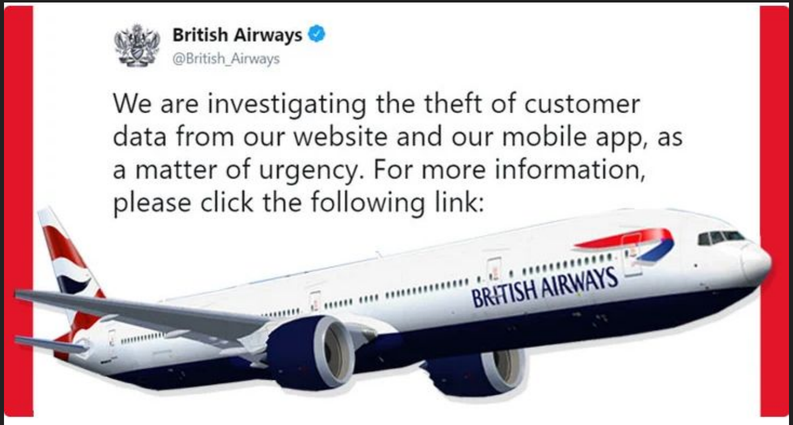
Value

- Sell the card data
- Or, use the card data for fraud

Data Thieves

2018 British Airways hack

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



British Airways
@British_Airways

We are investigating the theft of customer data from our website and our mobile app, as a matter of urgency. For more information, please click the following link:

[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

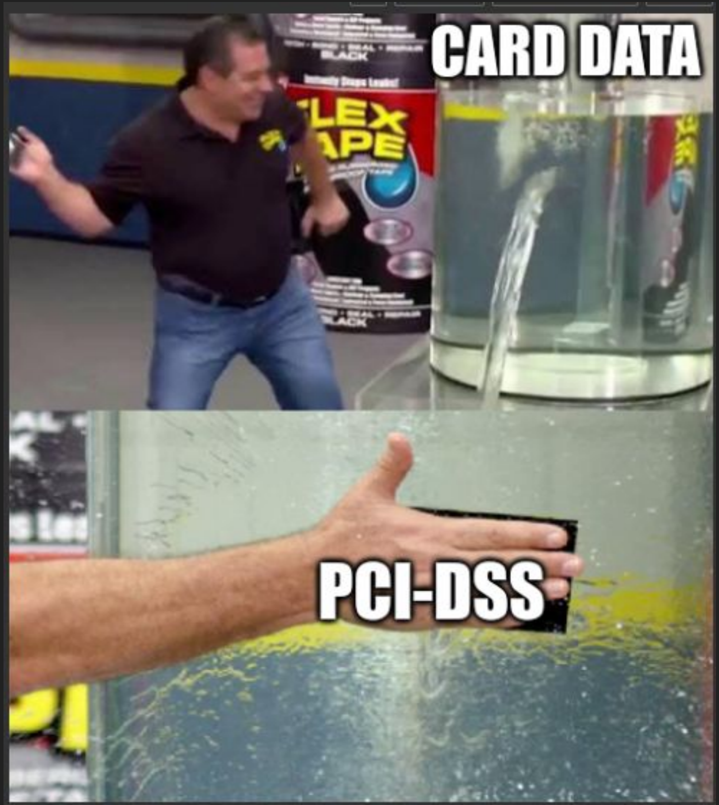
- Skimming - intercepted card details on the front-end with malicious javascript[1]
- Data at rest - found 95 days worth of card details in unencrypted logs[1]

[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

Storing and Transmitting Card Data

- Simply Do Not

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

Threat #2: Card Testers

Card Testers

- Use you as a way to test out unattested card data
  - Either purchased cheaply or taken from freely available sources
- Use you to guess card numbers from partial data
  - Partial data from other breaches, or BIN stuffing

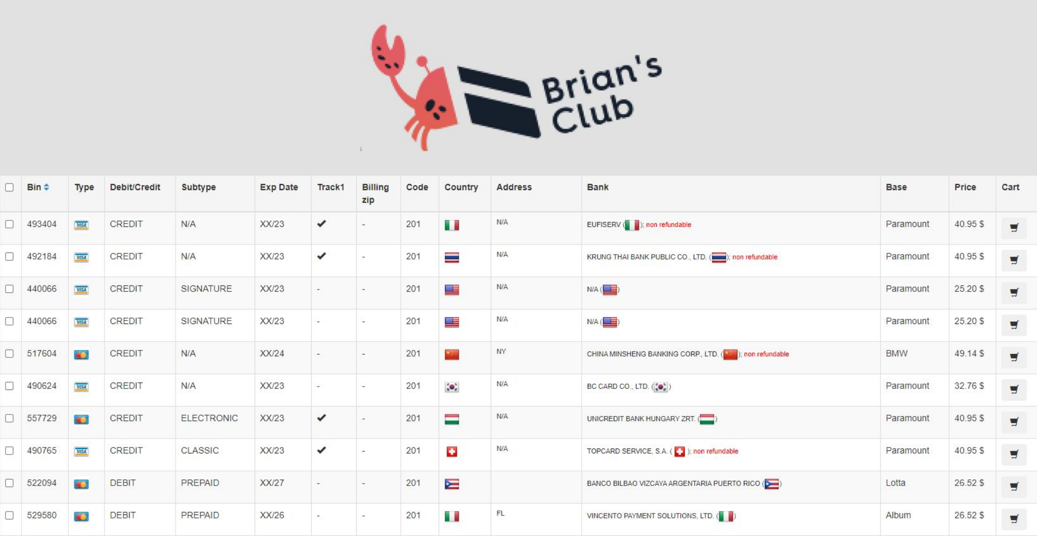
Card Testers

Value

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

Card Testers

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



Brian's Club

□	Bin ⇕	Type	Debit/Credit	Subtype	Exp Date	Track1	Billing zip	Code	Country	Address	Bank	Base	Price	Cart
□	493404	VISA	CREDIT	N/A	XX/23	✓	-	201		N/A	EUFISERV (); non refundable	Paramount	40.95 $	🛒
□	492184	VISA	CREDIT	N/A	XX/23	✓	-	201		N/A	KRUNG THAI BANK PUBLIC CO., LTD. (); non refundable	Paramount	40.95 $	🛒
□	440066	VISA	CREDIT	SIGNATURE	XX/23	-	-	201		N/A	N/A ()	Paramount	25.20 $	🛒
□	440066	VISA	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	VISA	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	VISA	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

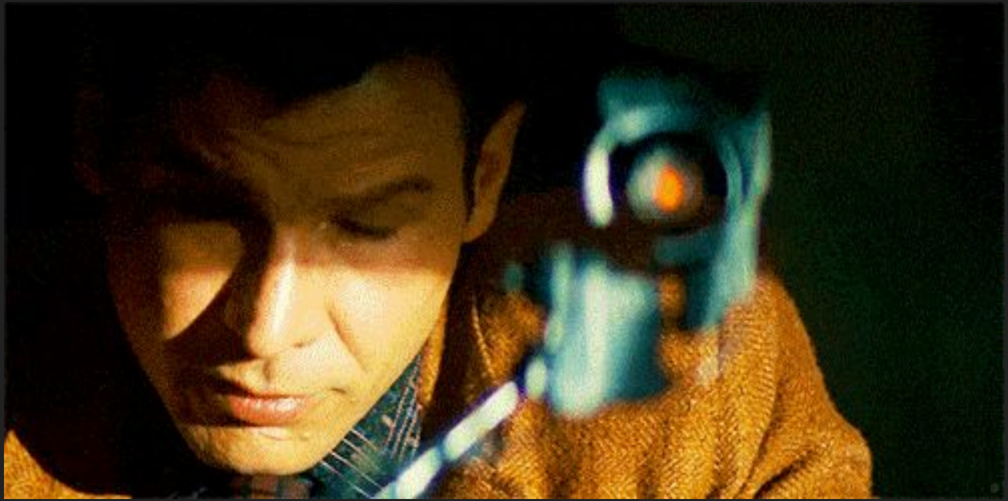
Detection

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

Card Testers

Mitigation

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



Card Testers

Mitigation

- CVV, AVS and 3DS
- All signal provided by issuer

Card Testers

Mitigation cont’d

- 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

Mitigation

- 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

Mitigation cont’d

- 3DS (3D Secure)
- Not entirely up to merchant
- Used much more widely outside of the US

```
+----------------------------------------+
|            [Bank Logo]                 |
|                                        |
|          3D Secure Verification        |
|                                        |
| For your security, please complete     |
| the following verification:            |
|                                        |
| Enter the OTP sent to your mobile:     |
| +-------------------------------+      |
| |                               |      |
| +-------------------------------+      |
|                                        |
|            [ Submit ]                  |
|                                        |
|                                        |
+----------------------------------------+
```

Card Testers

Mitigation cont’d

- Don’t be a cheap oracle!
- Other step-ups, trade-offs

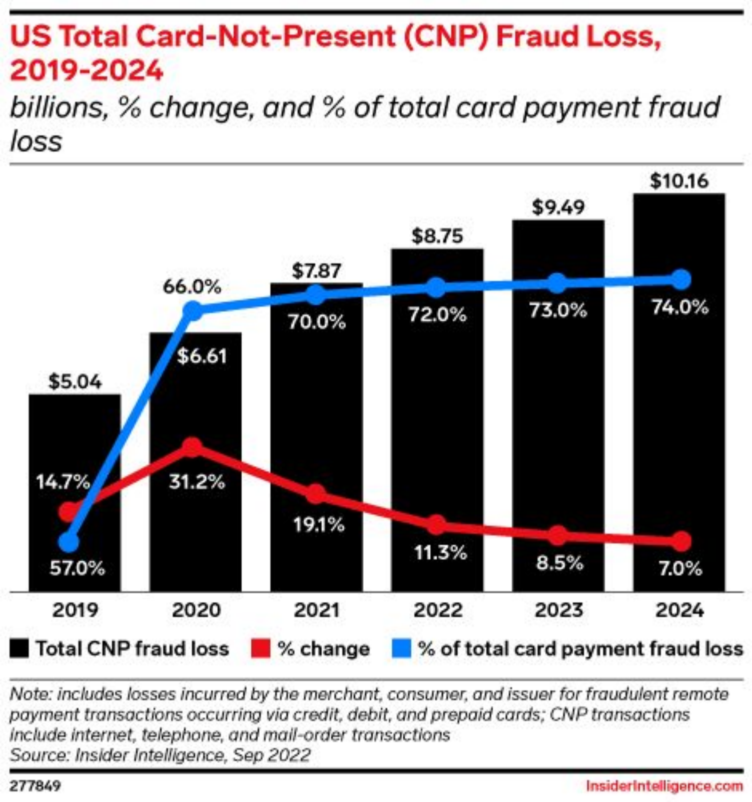
Threat #3: Fraudsters

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



US Total Card-Not-Present (CNP) Fraud Loss, 2019-2024

billions, % change, and % of total card payment fraud loss

Note: includes losses incurred by the merchant, consumer, and issuer for fraudulent remote payment transactions occurring via credit, debit, and prepaid cards; CNP transactions include internet, telephone, and mail-order transactions
Source: Insider Intelligence, Sep 2022

277849 InsiderIntelligence.com

Fraudsters

Detection

- Anomalous patterns, maybe
- Auth rates and conversion hits, maybe
- Chargebacks :’(
- You need a risk engine

Fraudsters

Mitigation

- CVV, AVS, 3DS
- Address matching
- KYC, SCA
- Risk Engine

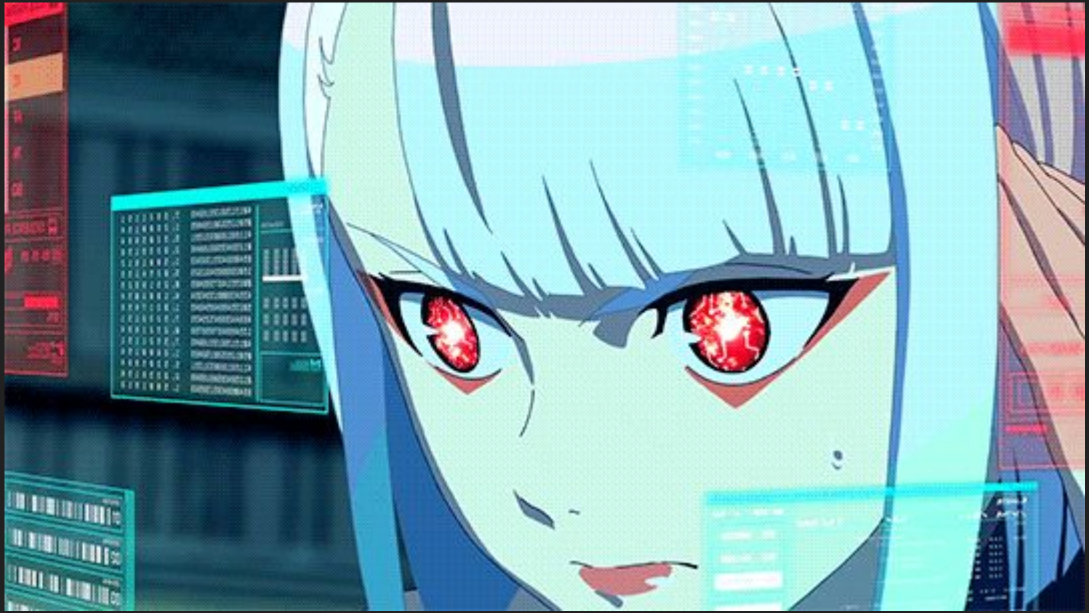
Balancing Risk

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.

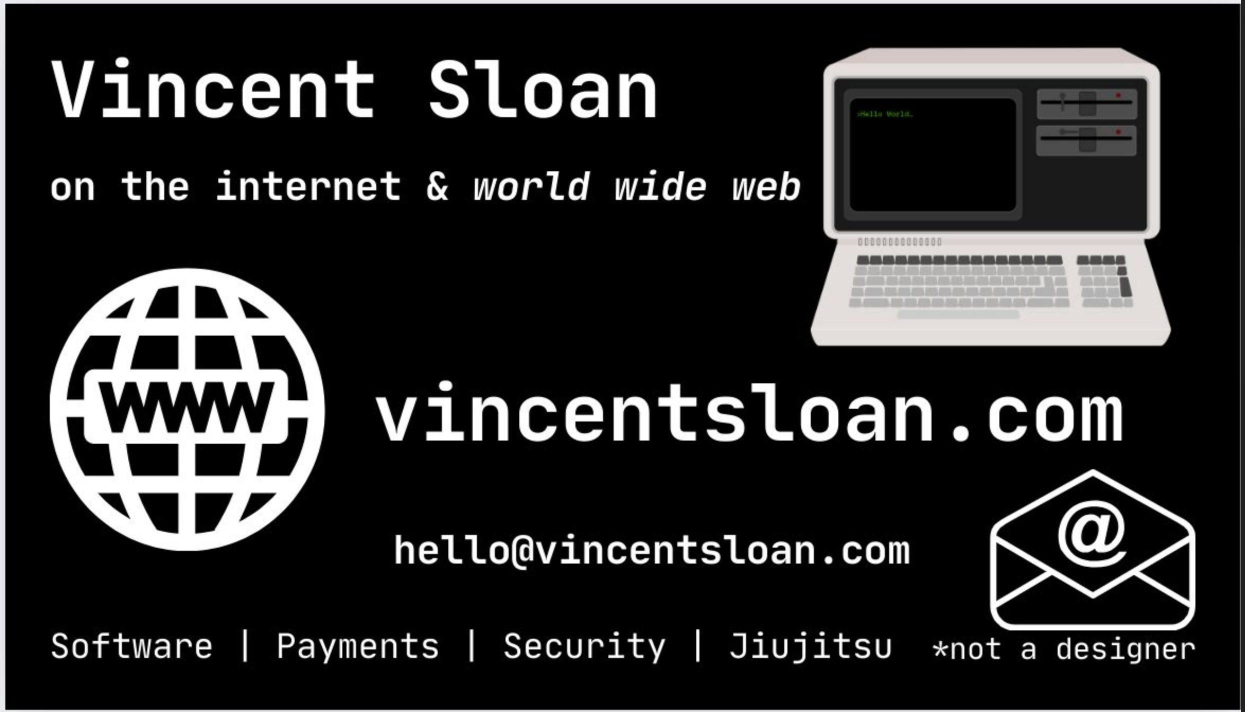
Balancing Risk

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



The End

- 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.
- Balancing risk is multi-faceted.



Vincent Sloan

on the internet & *world wide web*

vincentsloan.com

hello@vincentsloan.com

Software | Payments | Security | Jiujitsu *not a designer