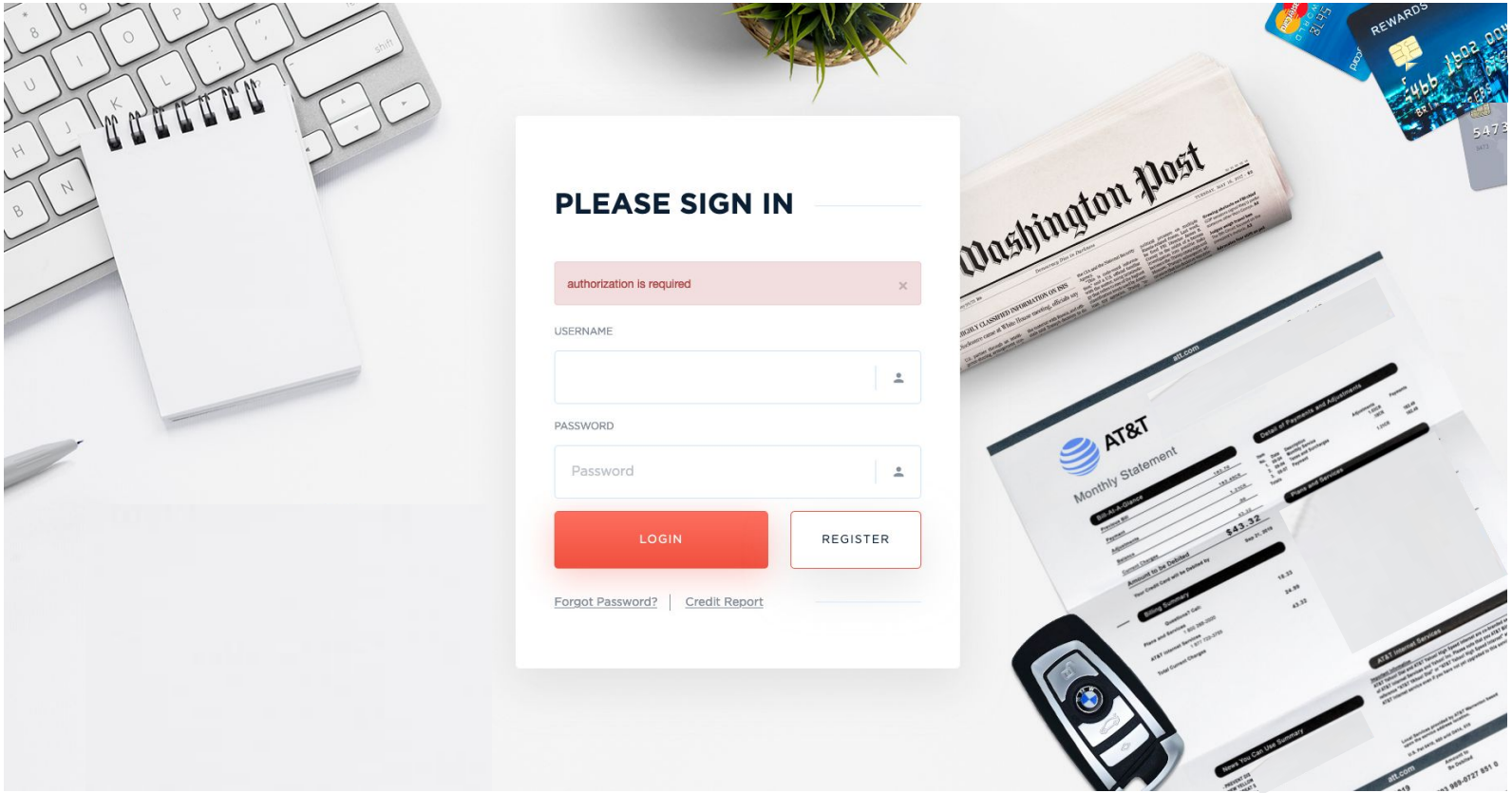
Swiped: Analyzing Ground-truth Data of a Marketplace for Stolen Debit and Credit Cards

Max Aliapoulios, Cameron Ballard, Rasika Bhalerao, Tobias Lauinger, Damon McCoy

NEW YORK UNIVERSITY


PLEASE SIGN IN
authorization is required
USERNAME
PASSWORD
Password
LOGIN
REGISTER
Forgot Password?
Credit Report
Washington Post
AT&T
Monthly Statement
REWARDS

Methodology

Methodology

Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts

Methodology

Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts
- Removed or hashed PII and other sensitive information

Methodology

Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts
- Removed or hashed PII and other sensitive information
- Operated in compliance with IRB

Methodology

Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts
- Removed or hashed PII and other sensitive information
- Operated in compliance with IRB

Data Validation

- Confirmed with security companies that had previously crawled data from the shop.

Methodology

Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts
- Removed or hashed PII and other sensitive information
- Operated in compliance with IRB

Data Validation

- Confirmed with security companies that had previously crawled data from the shop.
- We received confirmation that test purchases were in the database.

Methodology

Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts
- Removed or hashed PII and other sensitive information
- Operated in compliance with IRB

Data Validation

- Confirmed with security companies that had previously crawled data from the shop.
- We received confirmation that test purchases were in the database.
- 96.2% of 260k unique BTC wallet addresses were present on the blockchain

Methodology

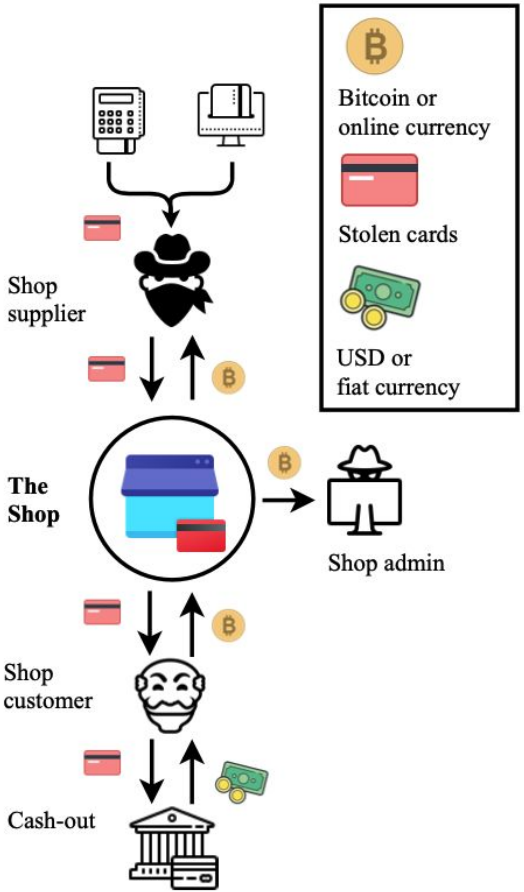
Leak Processing

- Ensured key stakeholders, like card networks and banks, had already been notified about the affected accounts
- Removed or hashed PII and other sensitive information
- Operated in compliance with IRB

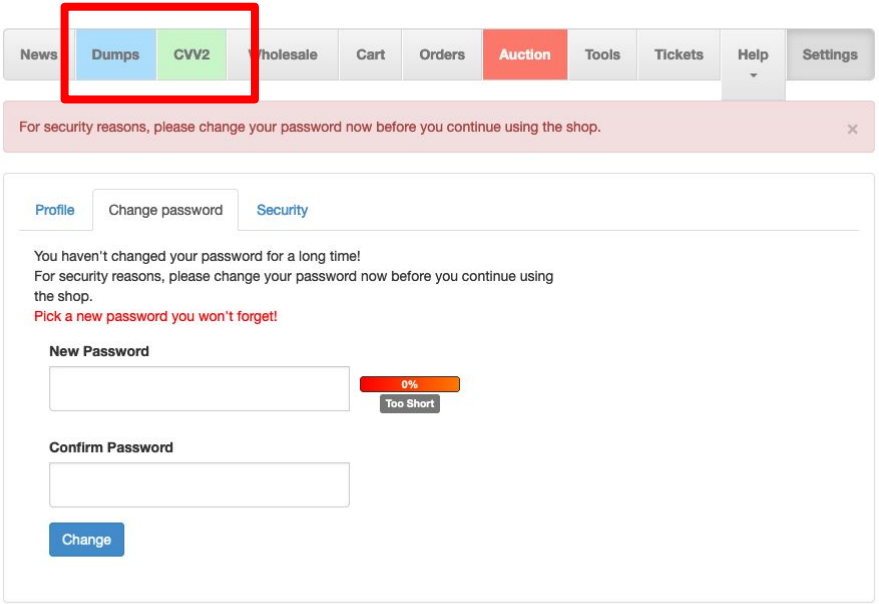
Data Validation

- Confirmed with security companies that had previously crawled data from the shop.
- We received confirmation that test purchases were in the database.
- 96.2% of 260k unique BTC wallet addresses were present on the blockchain
- Several cross consistency checks of the data

“The Shop”


Bitcoin or
online currency
Stolen cards
USD or
fiat currency
Shop
supplier
The
Shop
Shop admin
Shop
customer
Cash-out

Magnetic Stripe vs. CNP



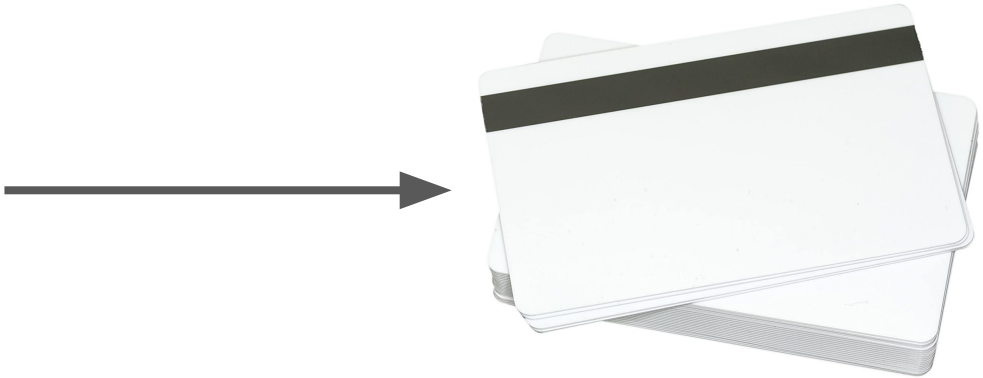
Shop Interface

Magnetic Stripe

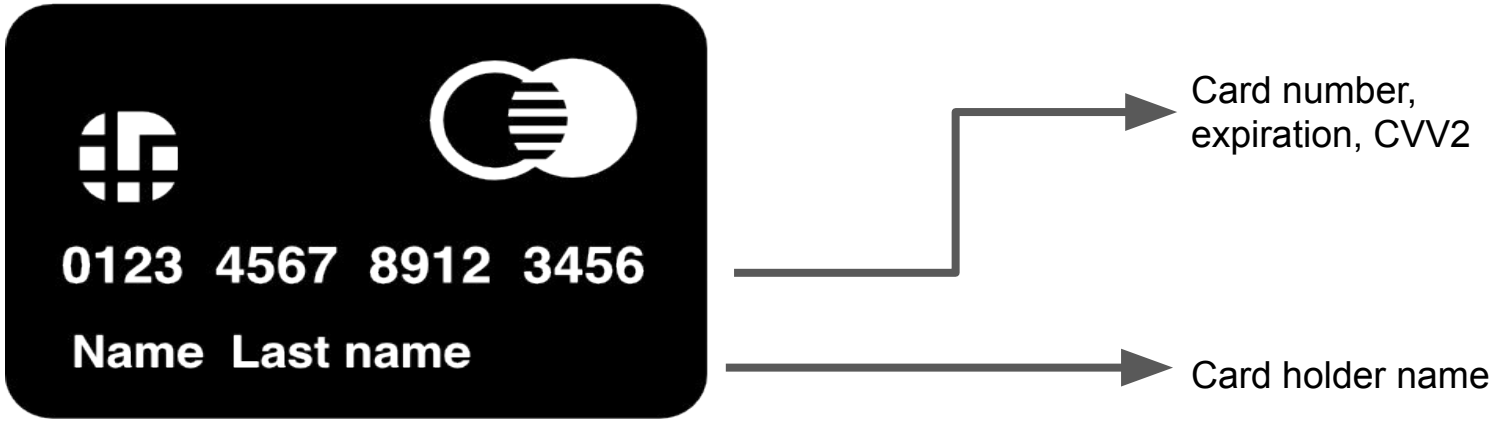
Magnetic stripe track data

- Card holder name
- Card number
- CVV1

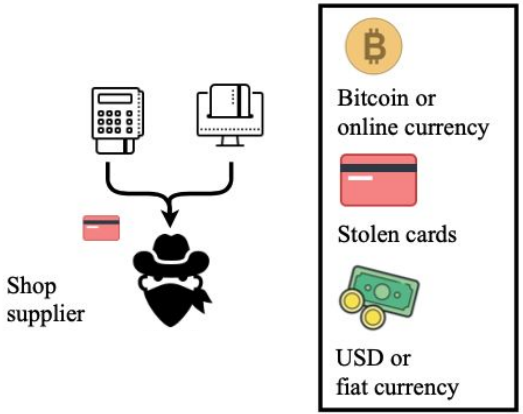
Magnetic Stripe



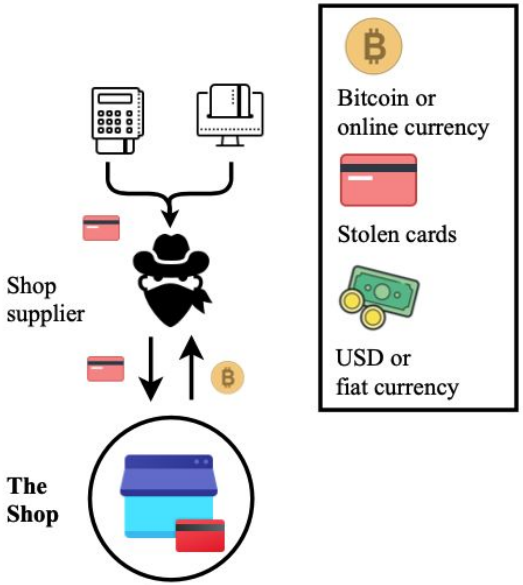
CNP


0123 4567 8912 3456
Name Last name
Card number,
expiration, CVV2
Card holder name

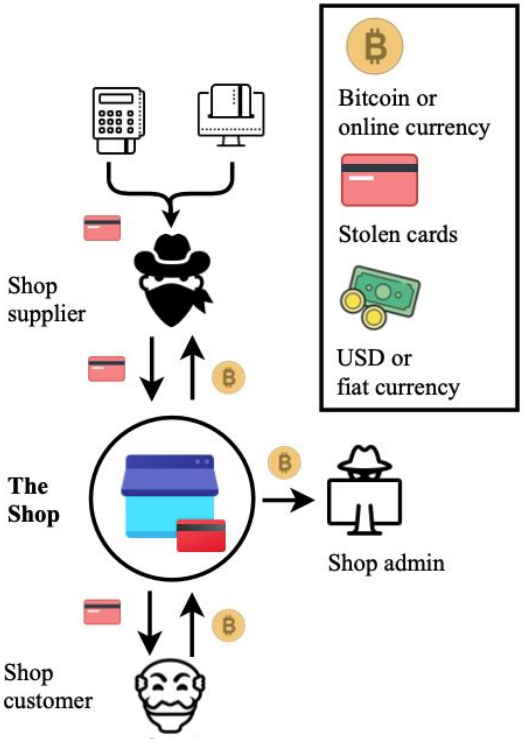
“The Shop”


Shop
supplier
Bitcoin or
online currency
Stolen cards
USD or
fiat currency

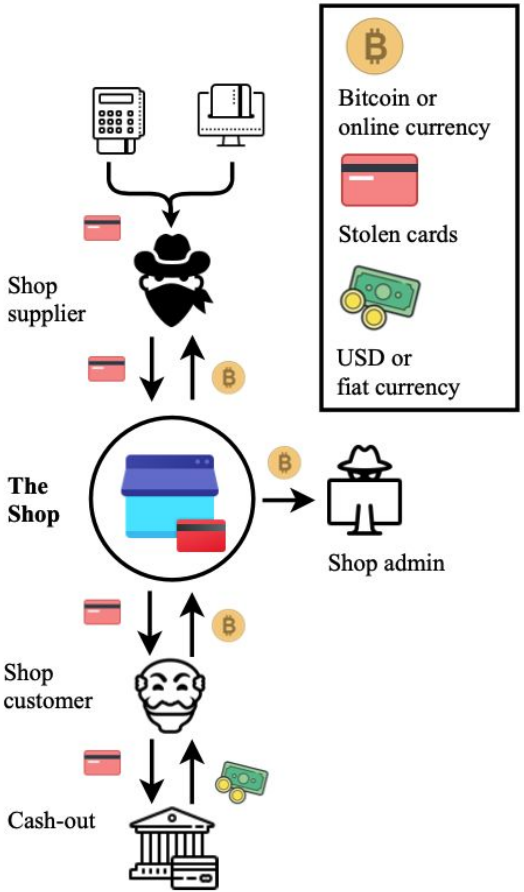
“The Shop”


Shop
supplier
The
Shop
Bitcoin or
online currency
Stolen cards
USD or
fiat currency

“The Shop”


Bitcoin or
online currency
Stolen cards
USD or
fiat currency
Shop
supplier
The
Shop
Shop admin
Shop
customer

“The Shop”


Bitcoin or
online currency
Stolen cards
USD or
fiat currency
Shop
supplier
The
Shop
Shop admin
Shop
customer
Cash-out

Back-end Data

Releases: Batches of stolen accounts grouped by a single seller who negotiated a commission

- 8,349 total releases

Back-end Data

Releases: Batches of stolen accounts grouped by a single seller who negotiated a commission

- 8,349 total releases

Inventory: Total available accounts

- 19.45M total accounts

Back-end Data

Releases: Batches of stolen accounts grouped by a single seller who negotiated a commission

- 8,349 total releases

Inventory: Total available accounts

- 19.45M total accounts

Sold: Purchased accounts

- 7.83M total accounts sold

Revenue: Total gross sales before refund

- $103.9M in total revenue

Back-end Data

Releases: Batches of stolen accounts grouped by a single seller who negotiated a commission

- 8,349 total releases

Inventory: Total available accounts

- 19.45M total accounts
    - **19M (97%) were magnetic stripe accounts**

Sold: Purchased accounts

- 7.83M total accounts sold

Revenue: Total gross sales before refund

- $103.9M in total revenue

Back-end Data

Releases: Batches of stolen accounts grouped by a single seller who negotiated a commission

- 8,349 total releases

Inventory: Total available accounts

- 19.45M total accounts
    - **19M (97%) were magnetic stripe accounts**
    - **Relative demand for CNP was higher - shop sold 84% of all CNP inventory whereas only 40% of magnetic stripe**

Sold: Purchased accounts

- 7.83M total accounts sold

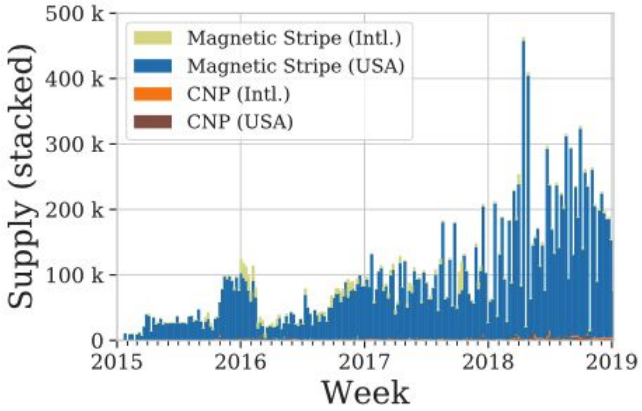
Revenue: Total gross sales before refund

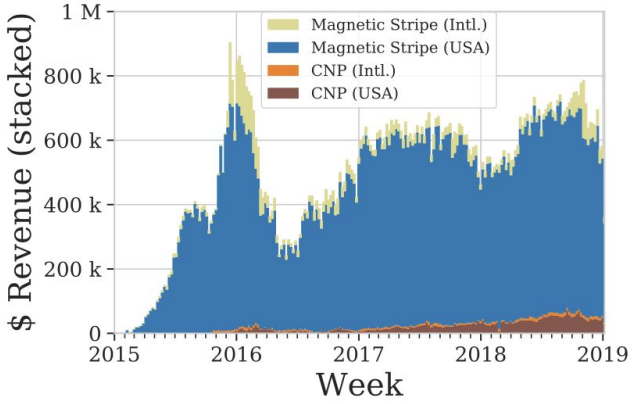
- $103.9M in total revenue

Supply & Demand

January 2015 - January 2019

Average 38k accounts per week

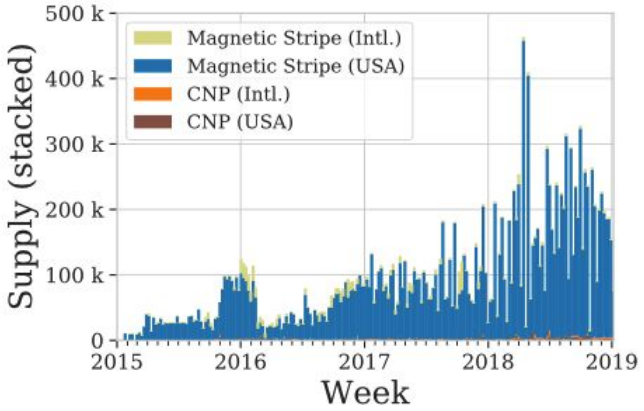


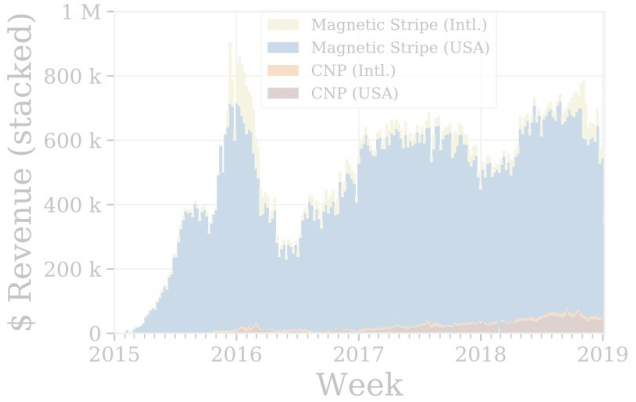


Supply & Demand

January 2015 - January 2019

Average 38k accounts per week

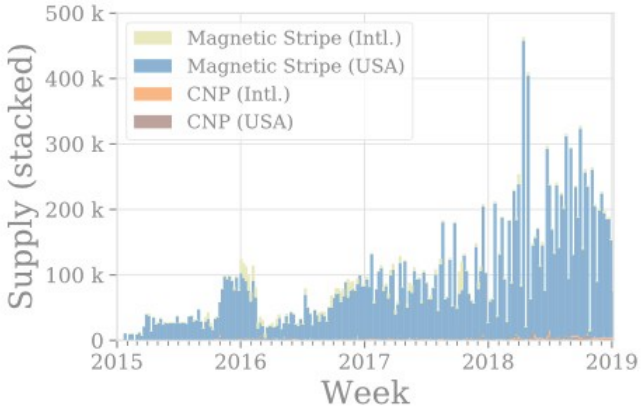


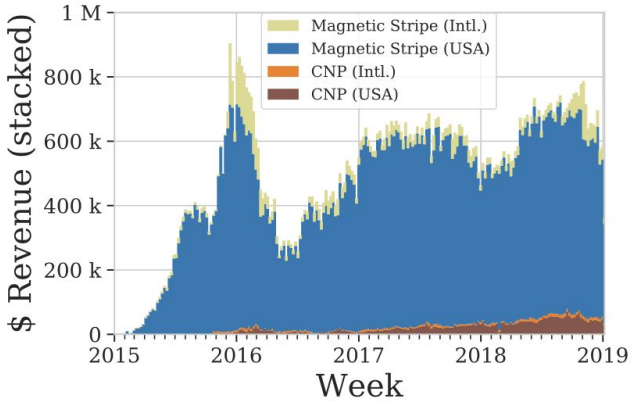


Supply & Demand

January 2015 - January 2019

Average 38k accounts per week



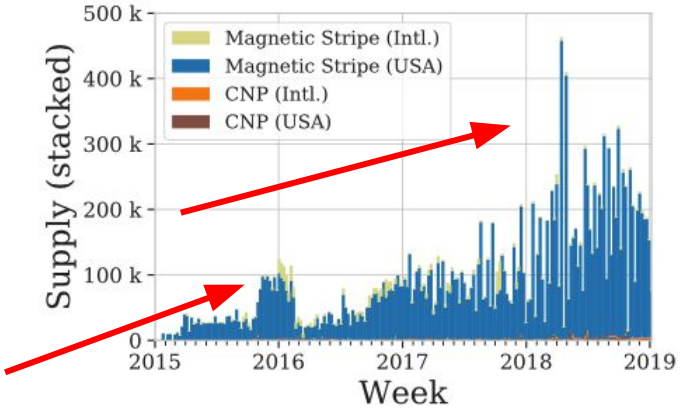


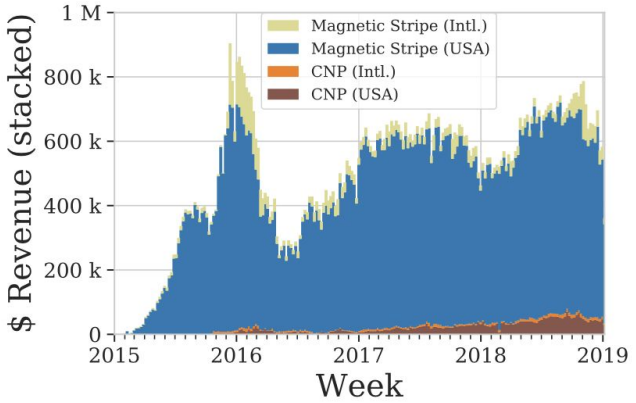
Supply & Demand

January 2015 - January 2019

Average 38k accounts per week

Spikes were mainly due to large releases





Supply & Demand

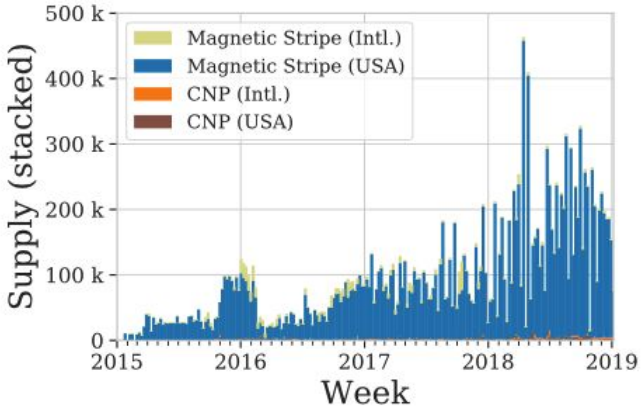
January 2015 - January 2019

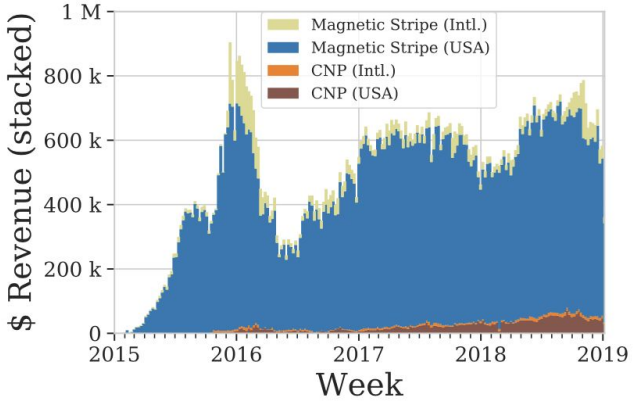
Average 38k accounts per week

Spikes were mainly due to large releases

CNP supply grate grew at 22.7% per week

Magnetic Stripe supply rate grew at 4.0% per week





Supply & Demand

January 2015 - January 2019

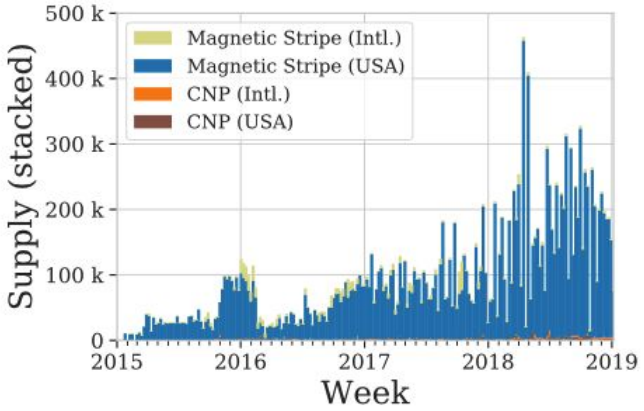
Average 38k accounts per week

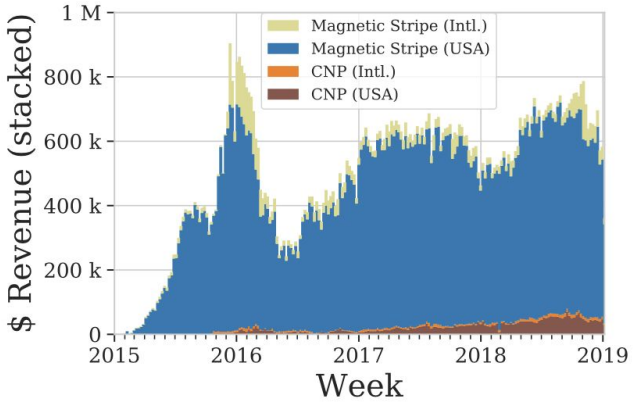
Spikes were mainly due to large releases

CNP supply grate grew at 22.7% per week

Magnetic Stripe supply rate grew at 4.0% per week

Shop had difficulty supplying more stolen CNP data which is counter to prior work



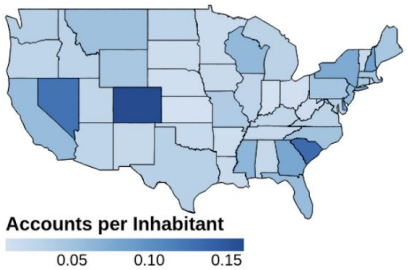


Regional Supply & Demand

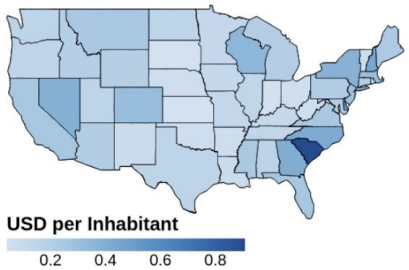
Normalized per capita

Magnetic Stripe

- SC by far the most popular state, $1 per inhabitant (60% more than the next highest state)



(a) Magnetic stripe (supply)



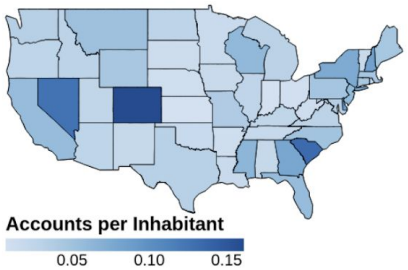
(b) Magnetic stripe (spending)

Regional Supply & Demand

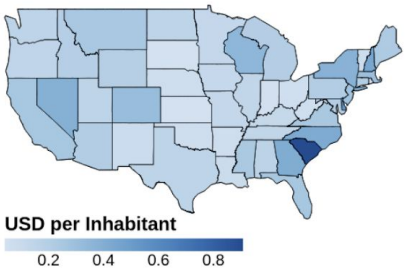
Normalized per capita

Magnetic Stripe

- SC by far the most popular state, $1 per inhabitant (60% more than the next highest state)
- CO and NV were popular for accounts added, but not purchased



(a) Magnetic stripe (supply)



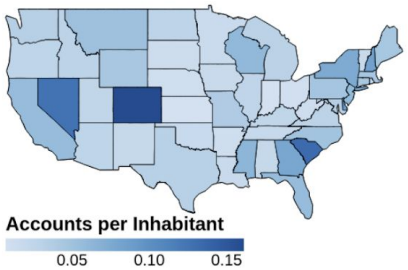
(b) Magnetic stripe (spending)

Regional Supply & Demand

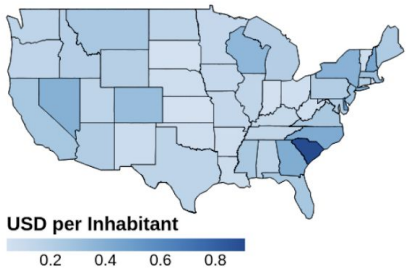
Normalized per capita

Magnetic Stripe

- SC by far the most popular state, $1 per inhabitant (60% more than the next highest state)
- CO and NV were popular for accounts added, but not purchased
- May be other factors than supply driving sale of these accounts



(a) Magnetic stripe (supply)



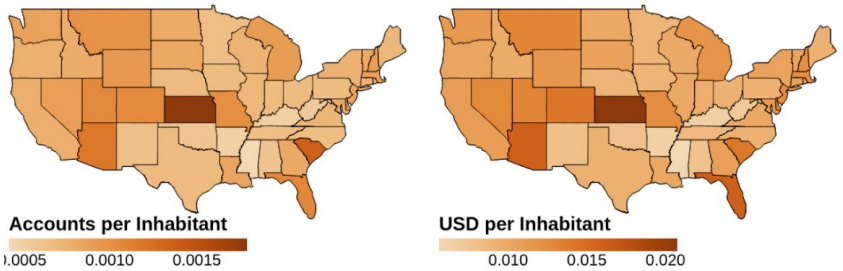
(b) Magnetic stripe (spending)

Regional Supply & Demand

Normalized per capita

CNP

- “Home” region of account had very little to do with purchases

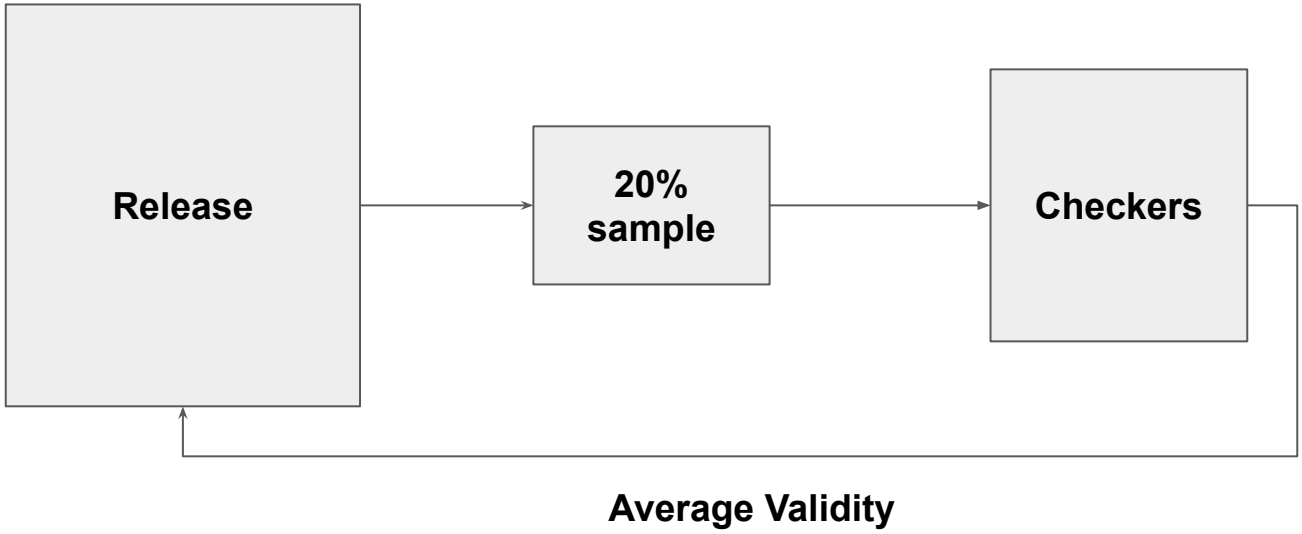


(c) CNP (supply)

(d) CNP (spending)

Pricing Strategies

Pricing Strategies - Average Validity



Pricing Strategies - Features

Initial asking price

- Magnetic stripe R^2 of 0.74
    - **54% was explained by average validity**

Pricing Strategies - Features

Initial asking price

- Magnetic stripe R^2 of 0.74
  - **54% was explained by average validity**
  - **Debit vs. Credit (11.4%), type (prepaid, corporate, etc., 10.4%), issuing bank (10.4%) and location (7.1%)**

Pricing Strategies - Features

Initial asking price

- Magnetic stripe R^2 of 0.74
  - **54% was explained by average validity**
  - **Debit vs. Credit (11.4%), type (prepaid, corporate, etc., 10.4%), issuing bank (10.4%) and location (7.1%)**
- CNP: R^2 was only 0.33
  - **No significant pricing features**

Pricing Strategies - Features

Initial asking price

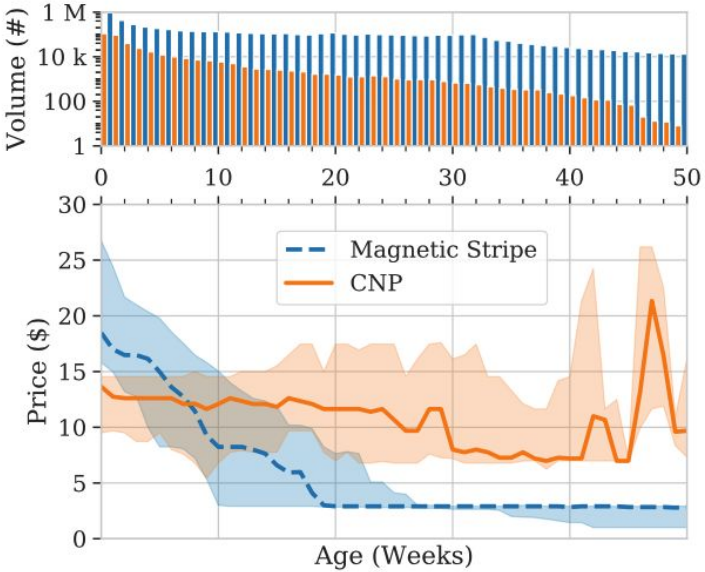
- Magnetic stripe R^2 of 0.74
  - **54% was explained by average validity**
  - **Debit vs. Credit (11.4%), type (prepaid, corporate, etc., 10.4%), issuing bank (10.4%) and location (7.1%)**
- CNP: R^2 was only 0.33
  - **No significant pricing features**

Sale price

- Time on the shop made an impact

Pricing Strategies

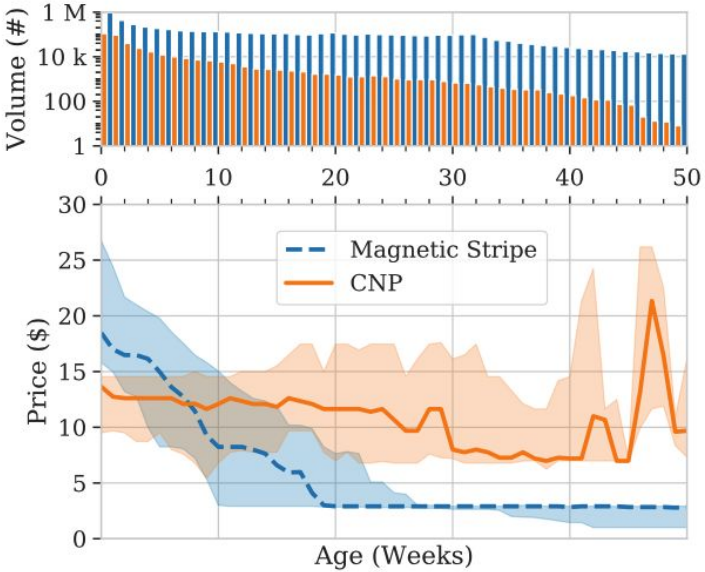
CNP purchase prices were more stable



Pricing Strategies

CNP purchase prices were more stable

CNP stay valid longer because there is no common point of purchase

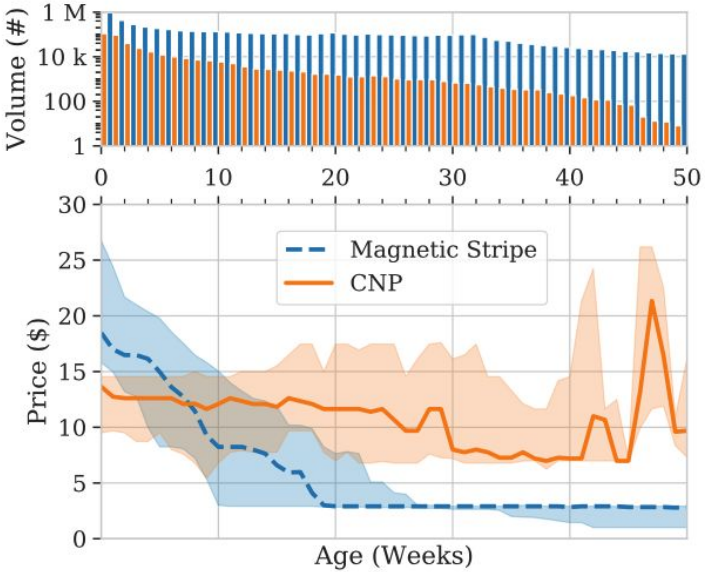


Pricing Strategies

CNP purchase prices were more stable

CNP stay valid longer because there is no common point of purchase

According to support tickets, magnetic stripe validity decreases over time due to banks detecting the breach source



Magnetic Stripe Account Attractiveness

Segmented across three variables: issuer, network and type

Magnetic Stripe Account Attractiveness

Segmented across three variables: issuer, network and type

Accounts are considered more attractive if:

1) Customers purchased a higher percentage of available accounts

Magnetic Stripe Account Attractiveness

Segmented across three variables: issuer, network and type

Accounts are considered more attractive if:

1) Customers purchased a higher percentage of available accounts
2) Customers purchased accounts for a higher price

Magnetic Stripe Account Attractiveness

Segmented across three variables: issuer, network and type

Accounts are considered more attractive if:

1) Customers purchased a higher percentage of available accounts
2) Customers purchased accounts for a higher price

- Segmented issuers into Top 10, medium and small in terms of total spend

Magnetic Stripe Account Attractiveness

Top 10 Issuers:

- 43% of spending
- Spending was in the millions for each

Medium Issuers:

- 104 total issuers accounted for 25% of the total spending
- Saw a larger fraction of listed accounts sold (53.4%) than top issuers (32.1%)
    - Except for USAA (83.2%)

Small Issuers:

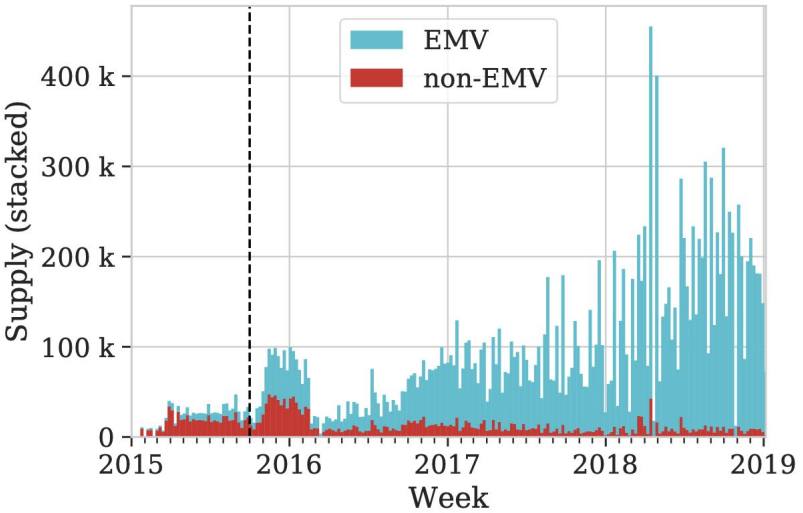
- 6,815 small issuers accounted for 22% of the spending
- Saw a larger percentage (55.2%) of their accounts sold compared to medium and small issuers
    - Again except for USAA (83.2%)

U.S. EMV Chip Deployment

U.S. EMV Chip Deployment

Liability shift for card-present transactions involving counterfeit cards to discourage merchants from processing magstripe transactions

- Took place on Oct 1 2015 in the U.S.

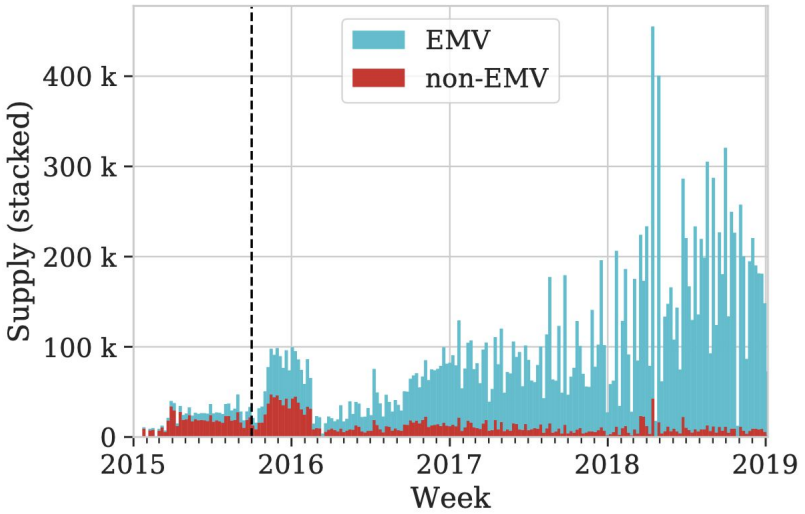


U.S. EMV Chip Deployment

Liability shift for card-present transactions involving counterfeit cards to discourage merchants from processing magstripe transactions

- Took place on Oct 1 2015 in the U.S.

Most of the magnetic stripe data added after the liability shift was equipped with a chip



Marketplaces Finance

Year	Revenue	Commissions	Refunds	Margins
2015*	13.4M	7.7M (57%)	3.6M (27%)	2.1M (16%)
2016	24M	10.8M (45%)	7.6M (32%)	5.6M (23%)
2017	32.2M	13.6M (42%)	11.8M (37%)	6.8M (21%)
2018	33.5M	13.6M (41%)	10.8M (32%)	9.1M (27%)
2019*	770K	313K (41%)	241K (31%)	217K (28%)
Total	103.9M	46M (44%)	34.1M (33%)	23.8M (23%)

Table 4: Yearly finances of the shop, in USD. *Partial data for 2015 and 2019. The shop earned $23.8M before costs such as advertising, employees and infrastructure.

Implications

Implications

Appears the liability shift alone was not enough to disincentivize merchants from swiping EMV-enabled cards

Implications

Appears the liability shift alone was not enough to disincentivize merchants from swiping EMV-enabled cards

2018 study by the U.S. Federal Reserve estimated a 20.9% ($770M) decline in card-present fraud

Implications

Appears the liability shift alone was not enough to disincentivize merchants from swiping EMV-enabled cards

2018 study by the U.S. Federal Reserve estimated a 20.9% ($770M) decline in card-present fraud

Carders appear to have an idea of which banks, card types, etc. are more likely to succeed for fraud

Implications

Appears the liability shift alone was not enough to disincentivize merchants from swiping EMV-enabled cards

2018 study by the U.S. Federal Reserve estimated a 20.9% ($770M) decline in card-present fraud

Carders appear to have an idea of which banks, card types, etc. are more likely to succeed for fraud

Open question whether future trends in the carding underground can be inferred from partial data, such as scrapes

Thank You