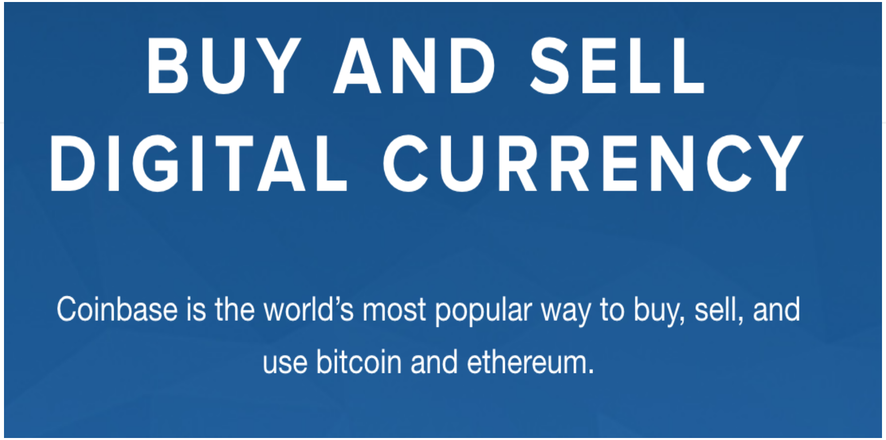
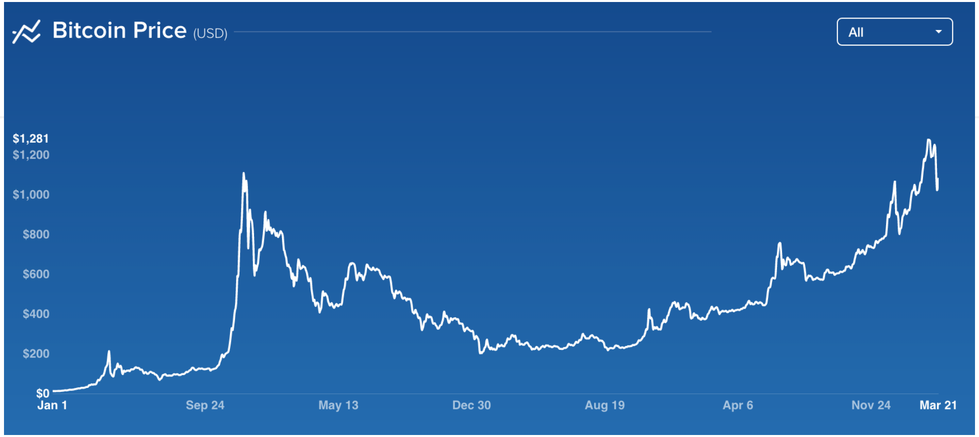
Preventing Fraud and Account Takeovers in Digital Currency

Soups Ranjan (soups@coinbase.com)
Dir. of Data Science & Risk engineering



BUY AND SELL DIGITAL CURRENCY

Coinbase is the world's most popular way to buy, sell, and use bitcoin and ethereum.



Our mission is to create an open financial system for the world

We've helped ~6M users in 33 countries exchange $6B in & out of digital currency

—cross-border remittances
—merchants can accept bitcoins with no chargeback risk
—alternative investment

Bitcoin is instant & non-reversible

↓

Hardest payment fraud & security problems in the world

↓

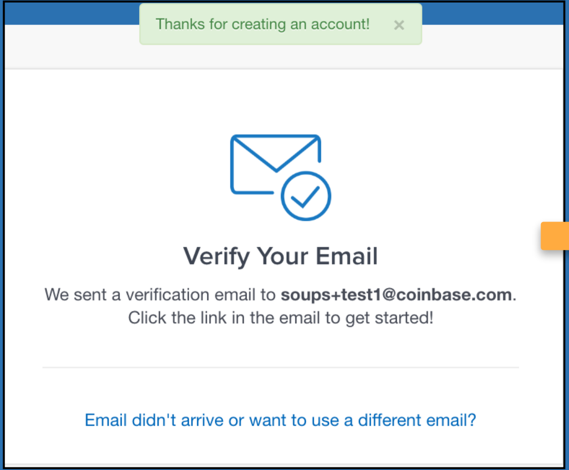
What does it take to solve it?

Agenda

- Payment fraud
- Account takeovers

Payment Fraud

Coinbase Sign-up Flow

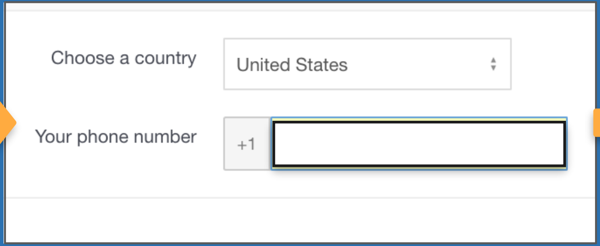


Thanks for creating an account! ×

Verify Your Email

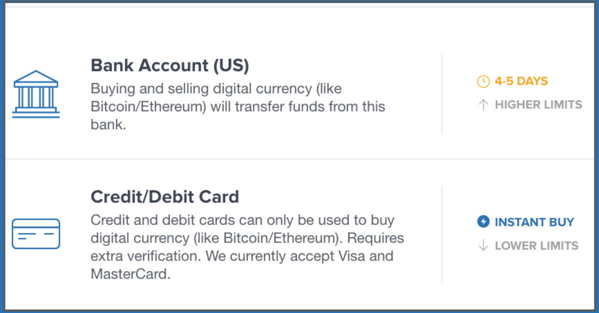
We sent a verification email to **soups+test1@coinbase.com**.
Click the link in the email to get started!

Email didn't arrive or want to use a different email?



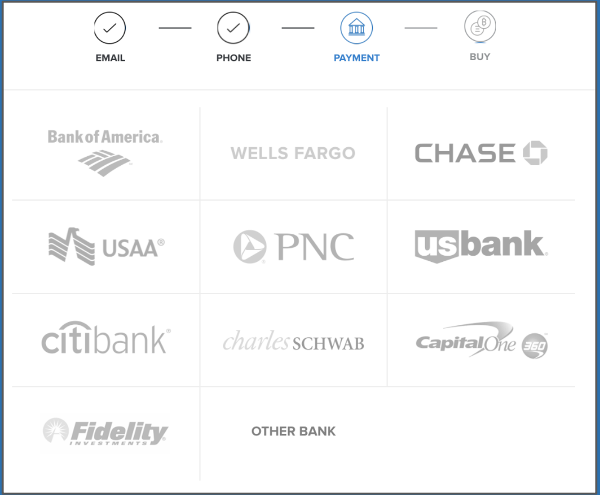
Choose a country: United States

Your phone number: +1



Bank Account (US)
Buying and selling digital currency (like Bitcoin/Ethereum) will transfer funds from this bank.
4-5 DAYS
HIGHER LIMITS

Credit/Debit Card
Credit and debit cards can only be used to buy digital currency (like Bitcoin/Ethereum). Requires extra verification. We currently accept Visa and MasterCard.
INSTANT BUY
LOWER LIMITS



EMAIL — PHONE — PAYMENT — BUY

Bank of America	WELLS FARGO	CHASE
USAA	PNC	usbank
citibank	charles SCHWAB	Capital One 360
Fidelity INVESTMENTS	OTHER BANK	

What does fraud at Coinbase look like?

Scammer

1. Steals Alice's bank account info or credit card number

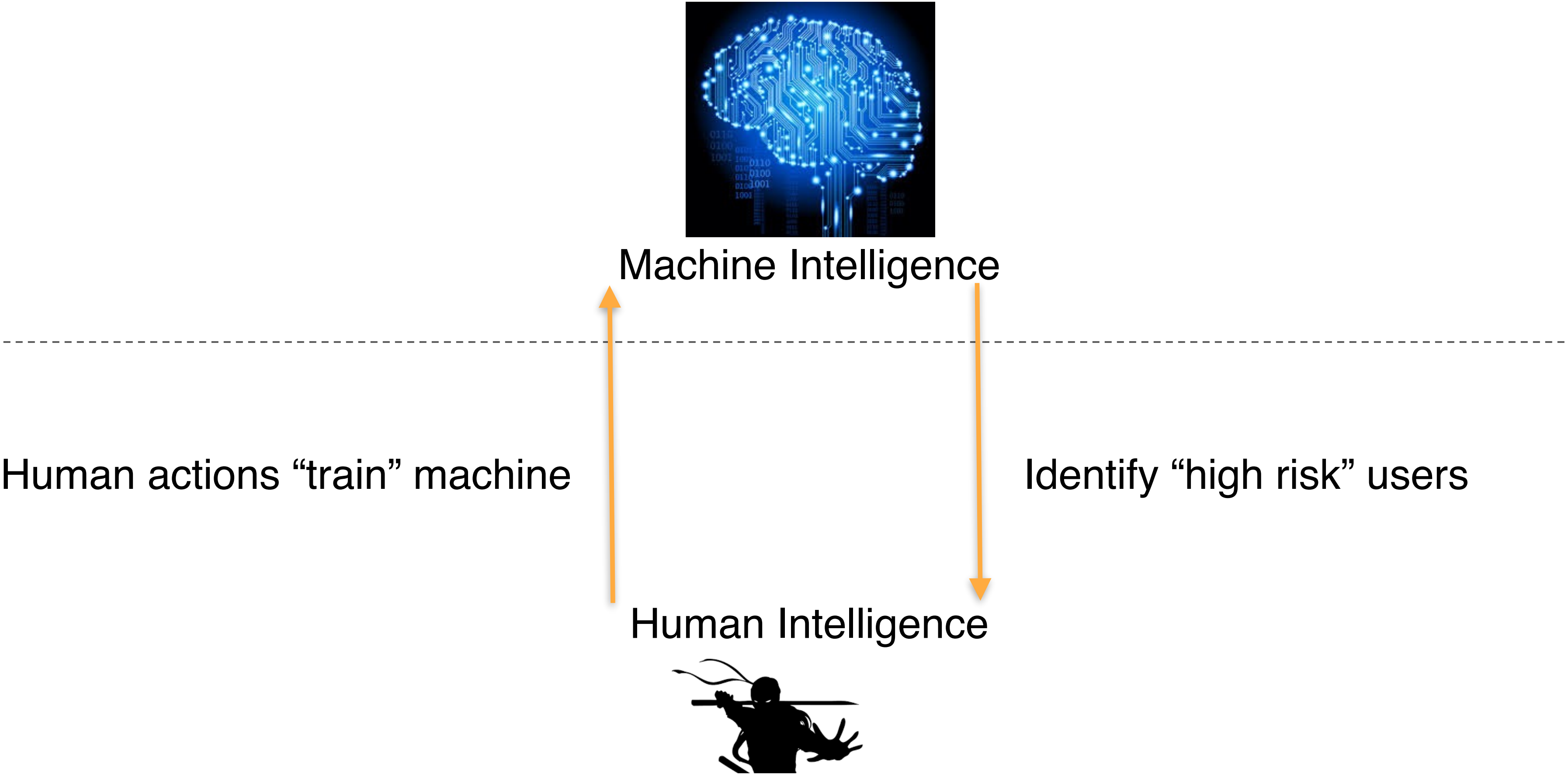
Alice disputes the purchase

Coinbase returns funds back to Alice

2. Steals Bob's identity

3. Steals Carl's mobile phone (call forwarding, SIM swap, etc)

Fraud Prevention: Human meets Machine Intelligence



Machine Intelligence

Human actions “train” machine

Identify “high risk” users

Human Intelligence

Supervised Machine Learning

Precog: Supervised Machine Learning

- Train a model with two labels:
  - Fraud vs. Non-fraud

- Collect signals from user as they are signing-up
  - Fingerprint: Device, Browser, Location
  - Email, Phone number, ID, SSN, Bank → name, address

- Use ML model to get risk-score for each user

Why does Machine Learning work to detect fraud?

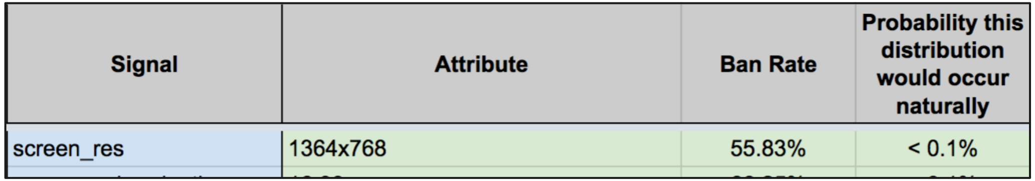
- Name & Address Mismatches across different sources

- Names may mismatch for regular users as well:
  - e.g. “Jonathan Kim” vs. “Jon Kim”
  - Use distance measures: Jaccard Similarity or Levenshtein

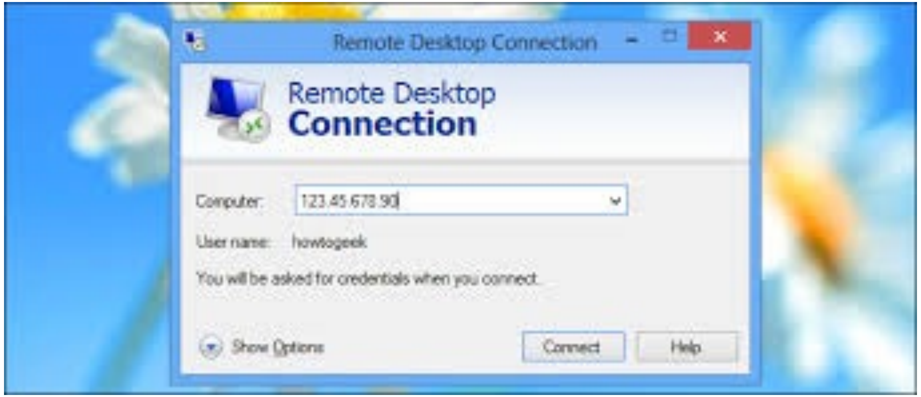
Why does Machine Learning work to detect fraud?

Broken Window Theory

Velocity based Signals



Signal	Attribute	Ban Rate	Probability this distribution would occur naturally
screen_res	1364x768	55.83%	< 0.1%



Computer: 123.45.678.90

User name: howtogeek

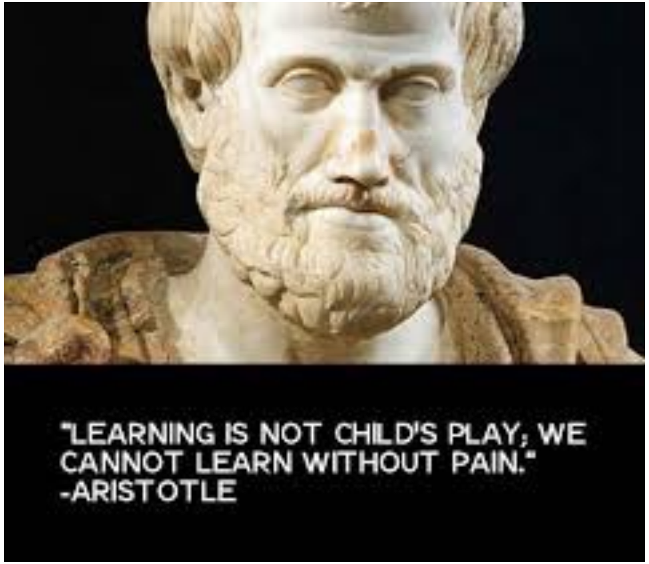
You will be asked for credentials when you connect.

How do we use the risk score?

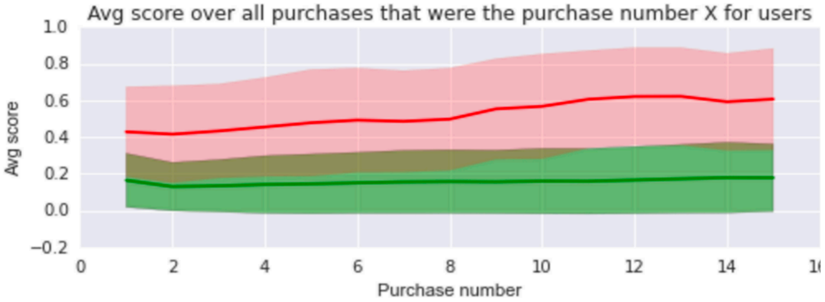
<u>Before</u>: Ban users with risk score > X

<u>Now</u>: Determine user's purchase limits

Paying to train our ML model

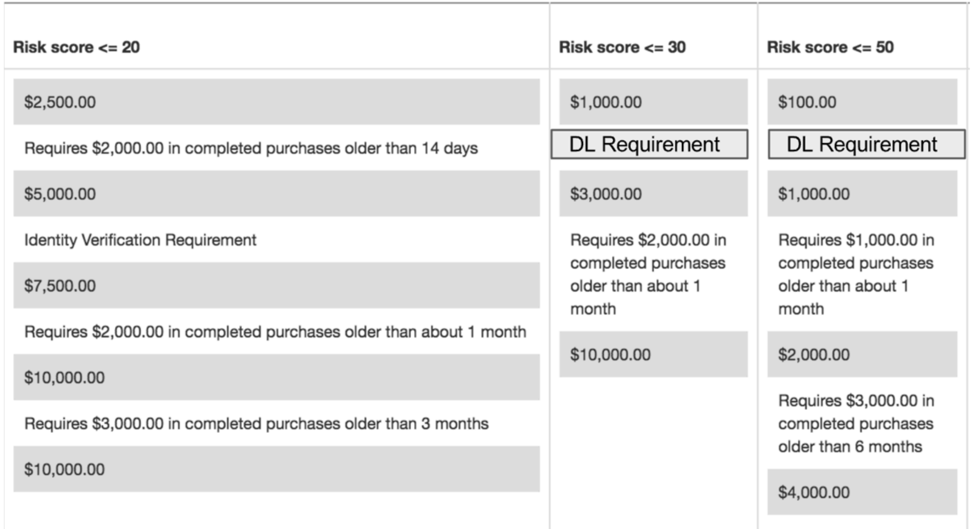

"LEARNING IS NOT CHILD'S PLAY; WE
CANNOT LEARN WITHOUT PAIN."
-ARISTOTLE

How does your purchase limit evolve?



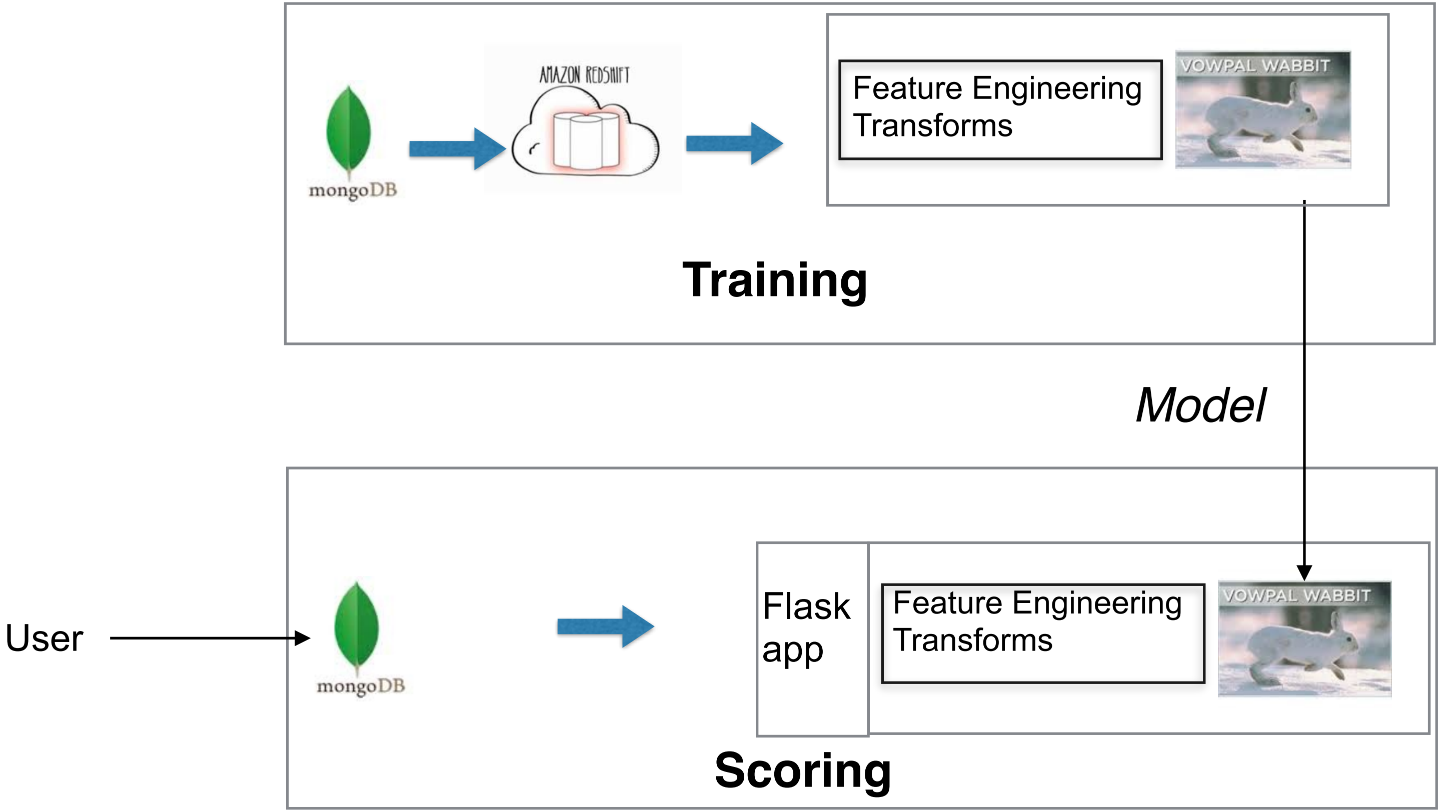
Risk Score

- Purchase volume
- Time (Aging of funds w/ no reversals)
- Verifications



Risk score <= 20	Risk score <= 30	Risk score <= 50
$2,500.00	$1,000.00	$100.00
Requires $2,000.00 in completed purchases older than 14 days	DL Requirement	DL Requirement
$5,000.00	$3,000.00	$1,000.00
Identity Verification Requirement	Requires $2,000.00 in completed purchases older than about 1 month	Requires $1,000.00 in completed purchases older than about 1 month
$7,500.00	$10,000.00	$2,000.00
Requires $2,000.00 in completed purchases older than about 1 month		Requires $3,000.00 in completed purchases older than 6 months
$10,000.00		$4,000.00
Requires $3,000.00 in completed purchases older than 3 months		
$10,000.00		

Precog: ML training and scoring



Logistic Regression - Feature Selection

Generalizable models work better with unseen data

- use regularization to remove less important features
- cross validation to pick hyper-parameter

If two signals are 100% correlated with each other

- L1-regularization will pick one signal at random and other will be 0
- L2-regularization will pick both and give them equal coefficients

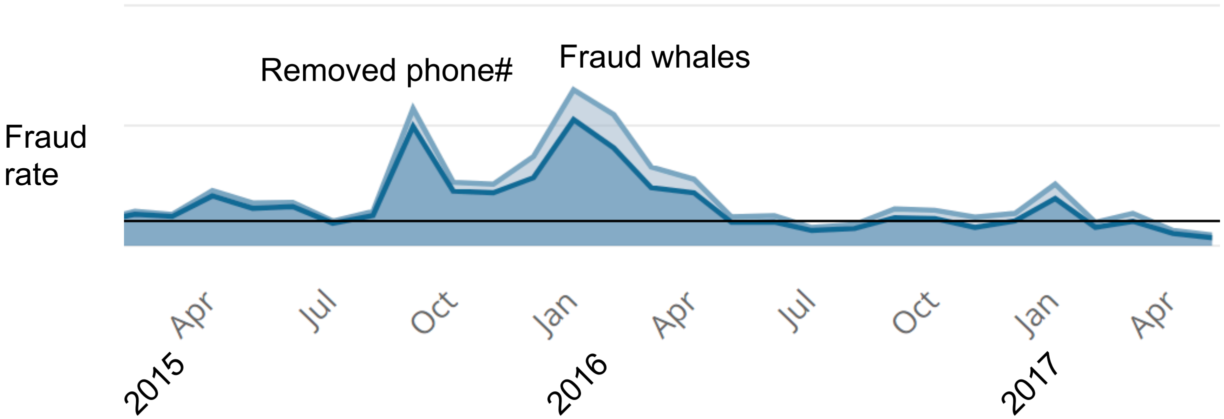
Metrics

Machine Learning:

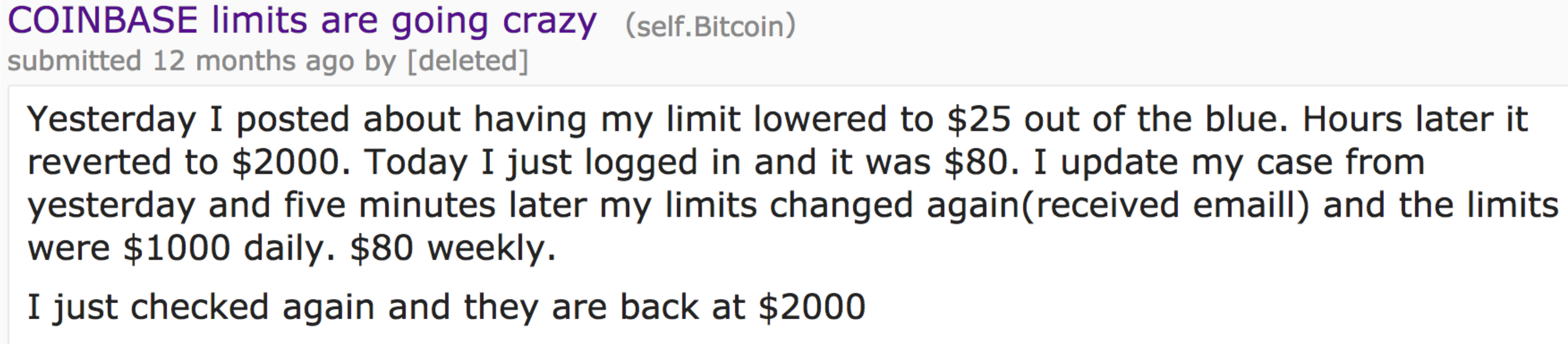
- **Log loss:** how close is P(fraud) to 1 (0) for fraud (good)

Business:

- **Fraud rate:** Loss ($) / Purchase volume ($)



When an ML model goes wrong



COINBASE limits are going crazy (self.Bitcoin)

submitted 12 months ago by [deleted]

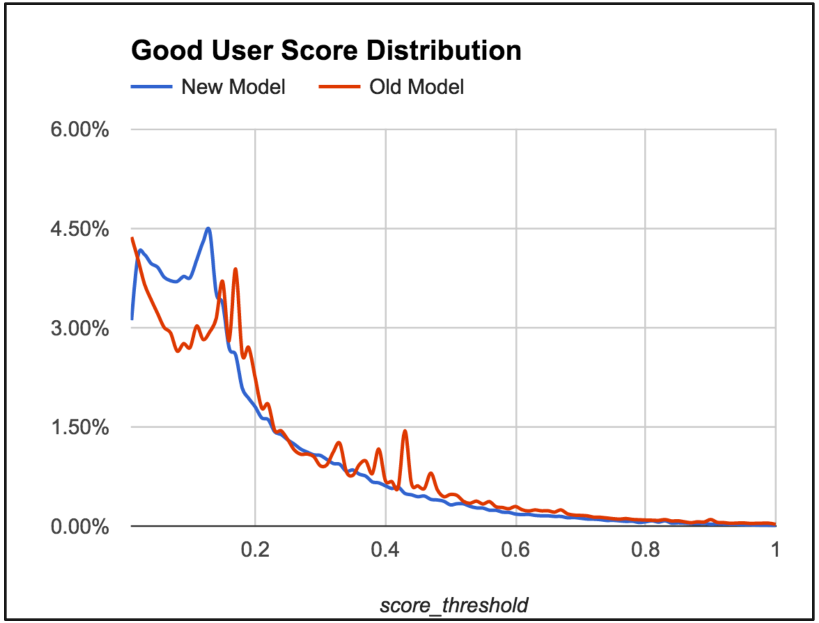
Yesterday I posted about having my limit lowered to $25 out of the blue. Hours later it reverted to $2000. Today I just logged in and it was $80. I update my case from yesterday and five minutes later my limits changed again(received emaill) and the limits were $1000 daily. $80 weekly.

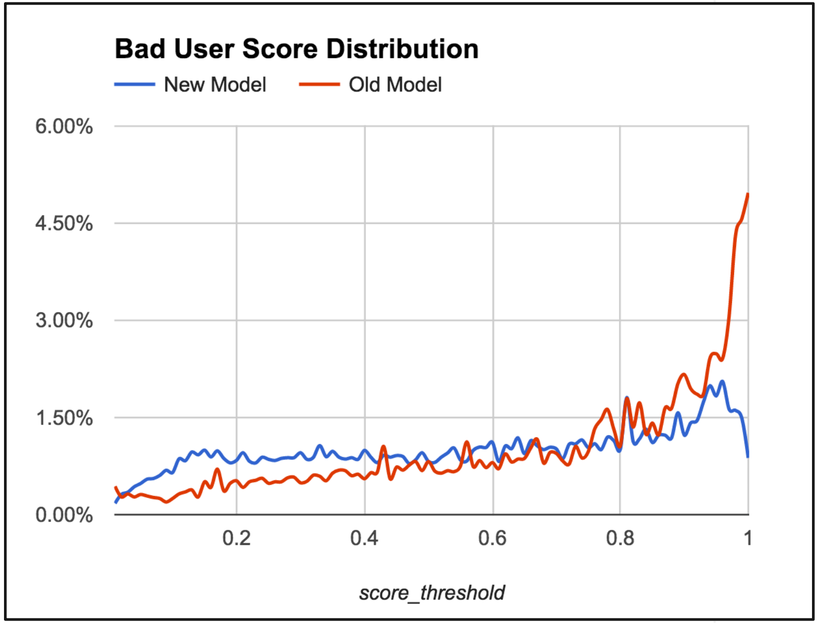
I just checked again and they are back at $2000

Model deployment — 1

Compare challenger model against production in shadow mode

- Deploy challenger model in shadow mode
- Compute distributions for user samples (good and bad)



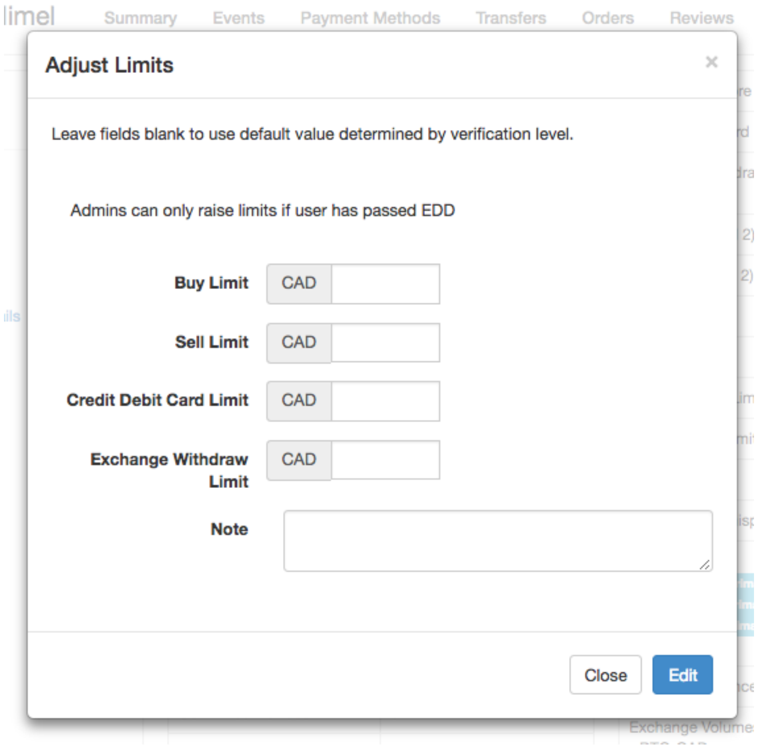


Model deployment —2

Estimate impact to whales (high $ value users)

Accept false positives if overall model accuracy goes up

- Lock their scores and purchase limits



Adjust Limits

Leave fields blank to use default value determined by verification level.

Admins can only raise limits if user has passed EDD

Buy Limit	CAD	
Sell Limit	CAD	
Credit Debit Card Limit	CAD	
Exchange Withdraw Limit	CAD	
Note		

Production A/B Test

Is model with best AUC or Logloss also best in fraud rate?

- A/B test to compare Production model vs. Challenger model
- Compute fraud rate over 2-3 months
- Challenger model promoted to production if its better in fraud-rate

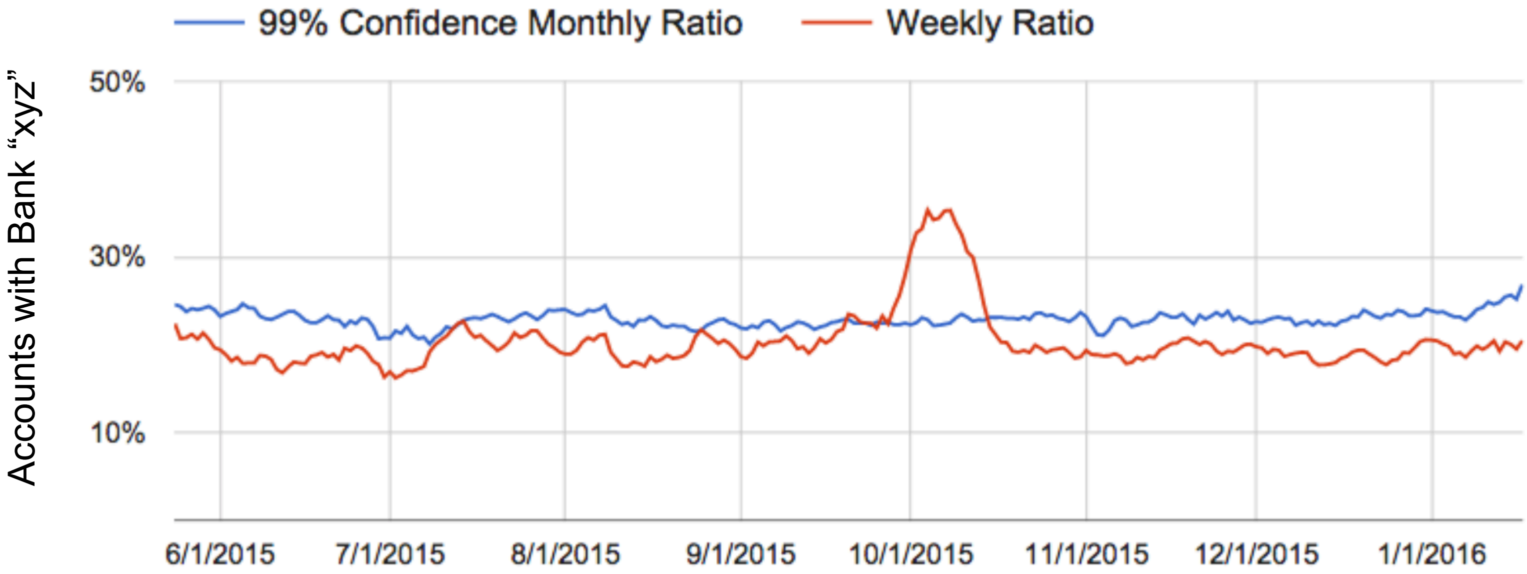
Unsupervised Machine Learning

Where does supervised machine learning fail?

- Problem:
  - Chargeback window is large (ACH: 60 days, Cards: 6 months)
  - Need to detect a new scammer trend before the window

- Unsupervised approaches to quickly extrapolate “human intuition”:
  - Anomaly Detection
  - Related user modeling
  - Rules engine

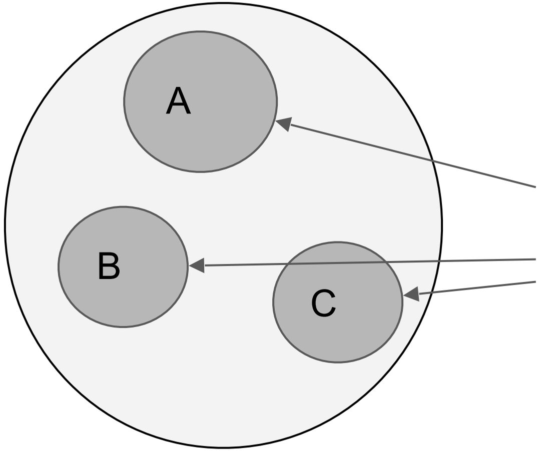
Anomaly Detection: Identify trends before chargebacks



Related Users Detection:
Identify accounts controlled by same individual

- Deterministic:

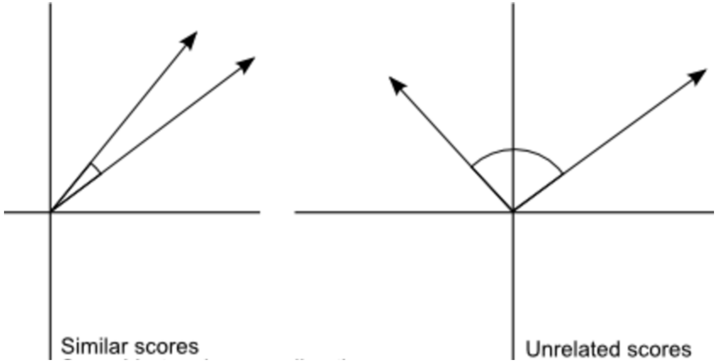
  Linking users by attributes



User clusters
- Normalized email
- SSN
- Bank account
- Credit card
- Driver’s License

- Probabilistic:

  Cosine similarity

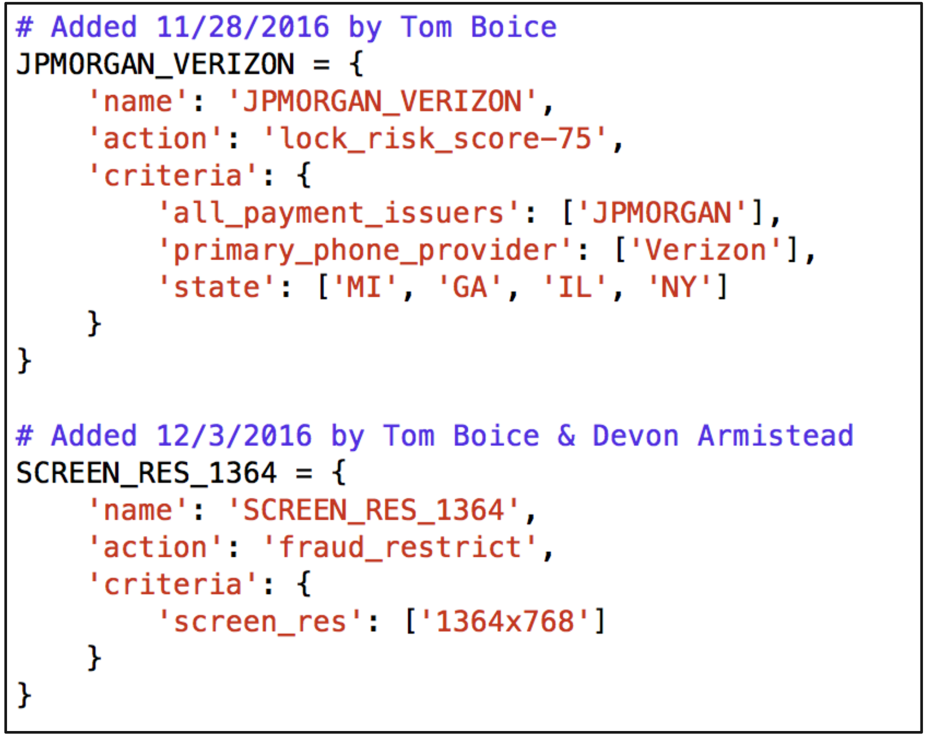


Custom Rules Engine

Create and retire rules quickly

Rule Actions

- Ban user
- Lock risk score to high value
- Require Facematch

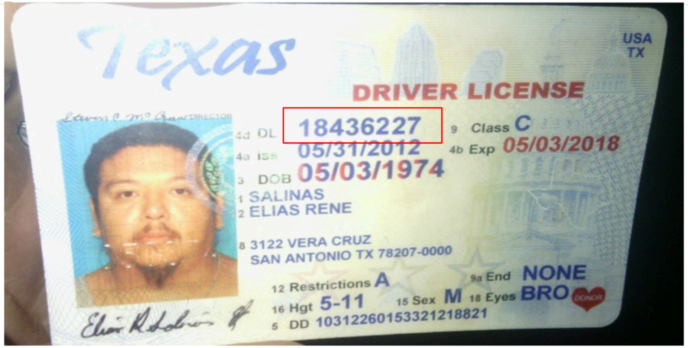


```
# Added 11/28/2016 by Tom Boice
JPMORGAN_VERIZON = {
    'name': 'JPMORGAN_VERIZON',
    'action': 'lock_risk_score-75',
    'criteria': {
        'all_payment_issuers': ['JPMORGAN'],
        'primary_phone_provider': ['Verizon'],
        'state': ['MI', 'GA', 'IL', 'NY']
    }
}

# Added 12/3/2016 by Tom Boice & Devon Armistead
SCREEN_RES_1364 = {
    'name': 'SCREEN_RES_1364',
    'action': 'fraud_restrict',
    'criteria': {
        'screen_res': ['1364x768']
    }
}
```

Case Study: “Verizon” Debit Card ring

Verizon Debit Card Ring



Texas

USA TX

DRIVER LICENSE

4d DL 18436227

9 Class C

4a ISS 05/31/2012

4b Exp 05/03/2018

3 DOB 05/03/1974

1 SALINAS
2 ELIAS RENE

8 3122 VERA CRUZ
SAN ANTONIO TX 78207-0000

12 Restrictions A

9a End NONE

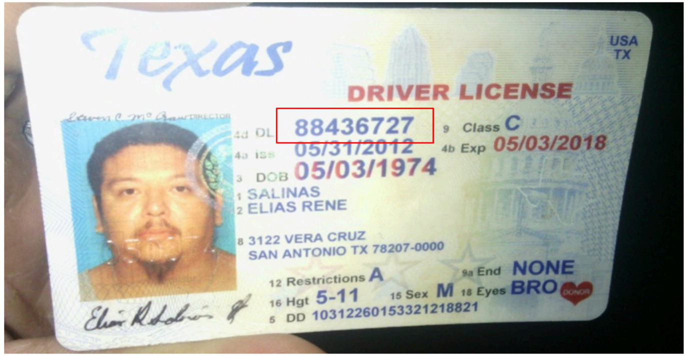
16 Hgt 5-11

15 Sex M

18 Eyes BRO

DONOR

5 DD 10312260153321218821



Texas

USA TX

DRIVER LICENSE

4d DL 88436727

9 Class C

4a ISS 05/31/2012

4b Exp 05/03/2018

3 DOB 05/03/1974

1 SALINAS
2 ELIAS RENE

8 3122 VERA CRUZ
SAN ANTONIO TX 78207-0000

12 Restrictions A

9a End NONE

16 Hgt 5-11

15 Sex M

18 Eyes BRO

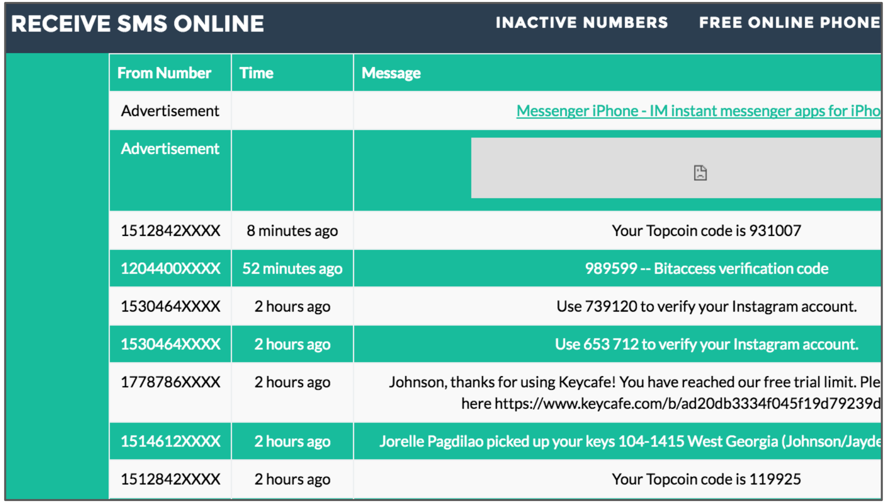
DONOR

5 DD 10312260153321218821

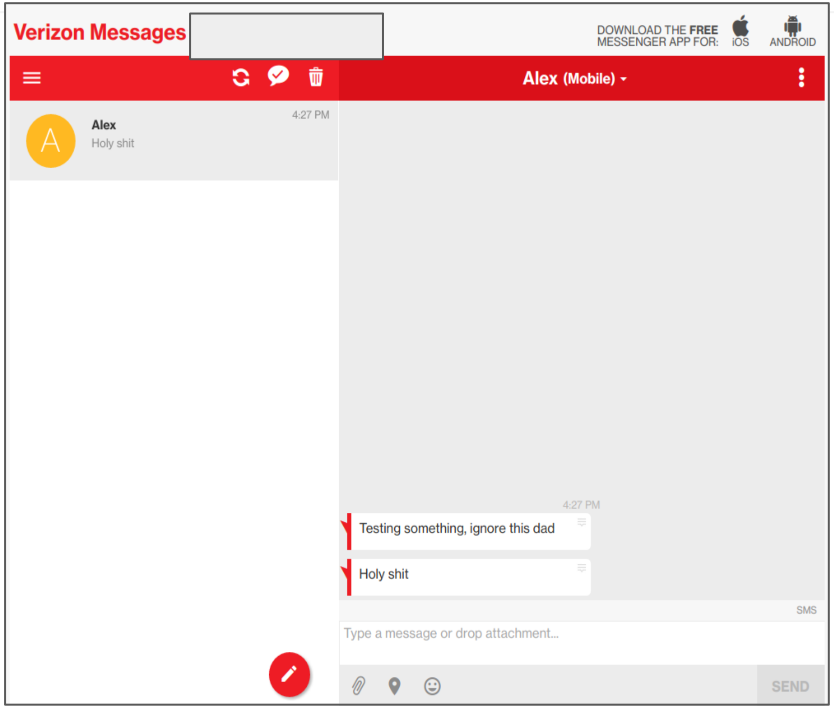
Ring Characteristics:

- Stolen debit cards
- Photoshopped IDs
- Stolen Verizon phones to verify account

No physical device needed to receive SMS 2FA tokens



From Number	Time	Message
Advertisement		Messenger iPhone - IM instant messenger apps for iPho
Advertisement		
1512842XXXX	8 minutes ago	Your Topcoin code is 931007
1204400XXXX	52 minutes ago	989599 -- Bitaccess verification code
1530464XXXX	2 hours ago	Use 739120 to verify your Instagram account.
1530464XXXX	2 hours ago	Use 653 712 to verify your Instagram account.
1778786XXXX	2 hours ago	Johnson, thanks for using Keycafe! You have reached our free trial limit. Ple here https://www.keycafe.com/b/ad20db3334f045f19d79239d
1514612XXXX	2 hours ago	Jorelle Pagdilao picked up your keys 104-1415 West Georgia (Johnson/Jayde
1512842XXXX	2 hours ago	Your Topcoin code is 119925



Verizon Messages
DOWNLOAD THE FREE MESSENGER APP FOR:
iOS
ANDROID
Alex (Mobile)
A
SMS
Type a message or drop attachment...
SEND

Alex 4:27 PM
Holy shit

4:27 PM

Testing something, ignore this dad

Holy shit

- SMS 2FA tokens received on temporary phones

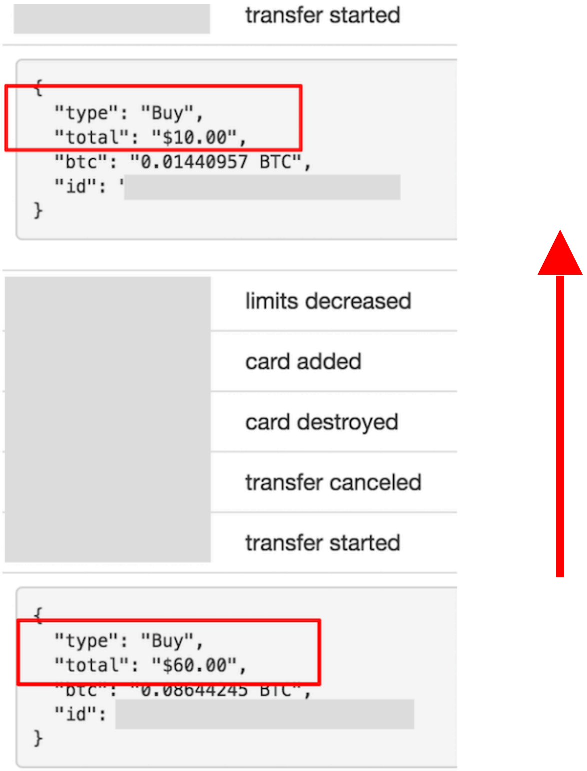
- SMS 2FA is readable online eg Verizon online portal
- ie SMS 2FA == telco password

Ring detected via Anomaly Detection

Ring Detection:

- Scammer wasn’t thorough
- Used same screen resolution: 1600 x 1200

Risk engine automatically raises risk score



[redacted] transfer started

```
{
  "type": "Buy",
  "total": "$10.00",
  "btc": "0.01440957 BTC",
  "id": '[redacted]
}
```

[redacted]

limits decreased

card added

card destroyed

transfer canceled

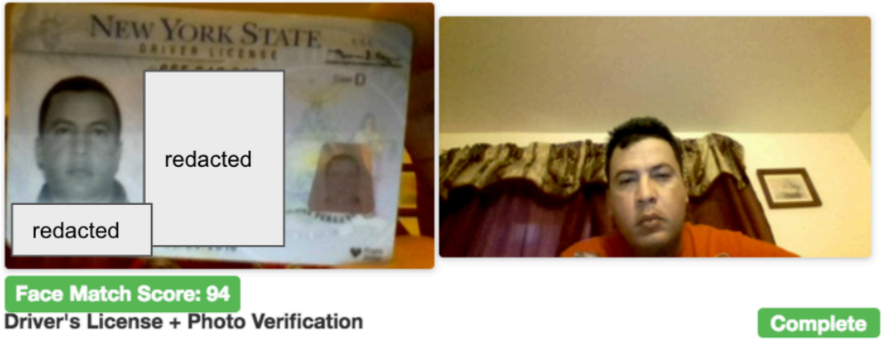
transfer started

```
{
  "type": "Buy",
  "total": "$60.00",
  "btc": "0.08644245 BTC",
  "id": [redacted]
}
```

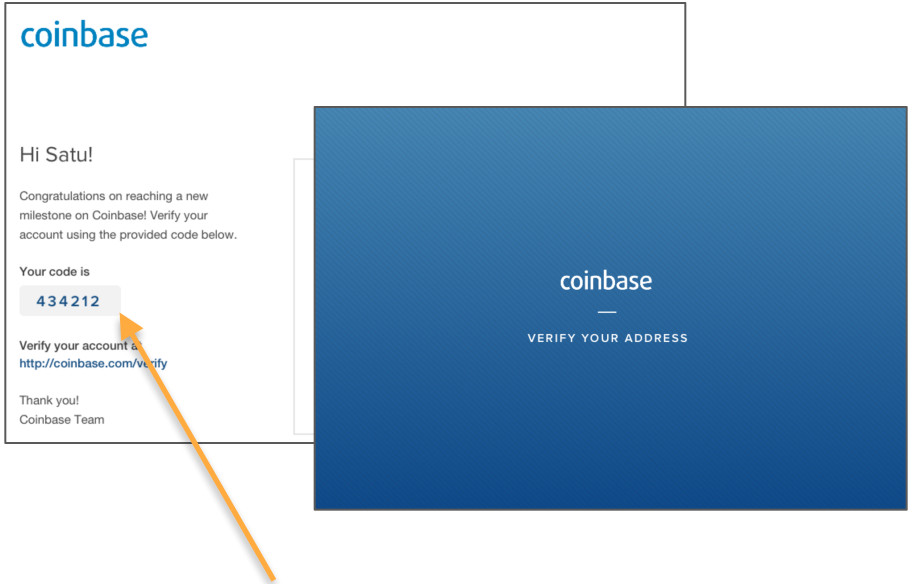
The games they play

Important to know user has the ID

Increasingly easy to obtain “stolen” IDs (Dropbox, social engineering scams)



Face Match: selfie + ID


coinbase

Hi Satu!

Congratulations on reaching a new milestone on Coinbase! Verify your account using the provided code below.

Your code is

434212

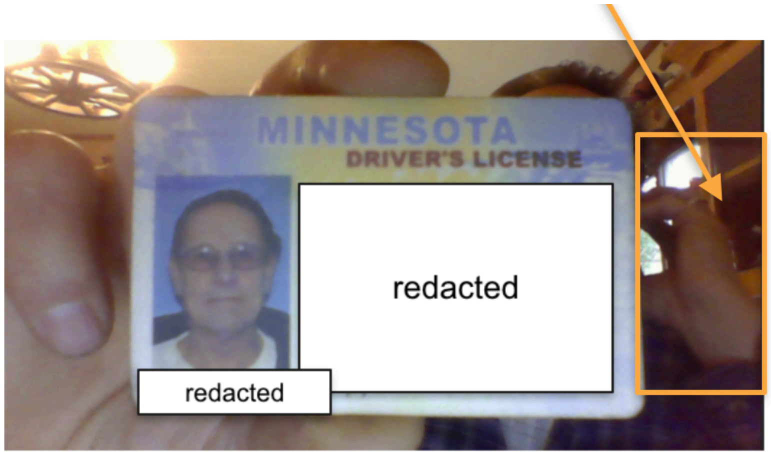
Verify your account a
http://coinbase.com/verify

Thank you!
Coinbase Team

Physical Address Verification:

Send a postcard to address on ID

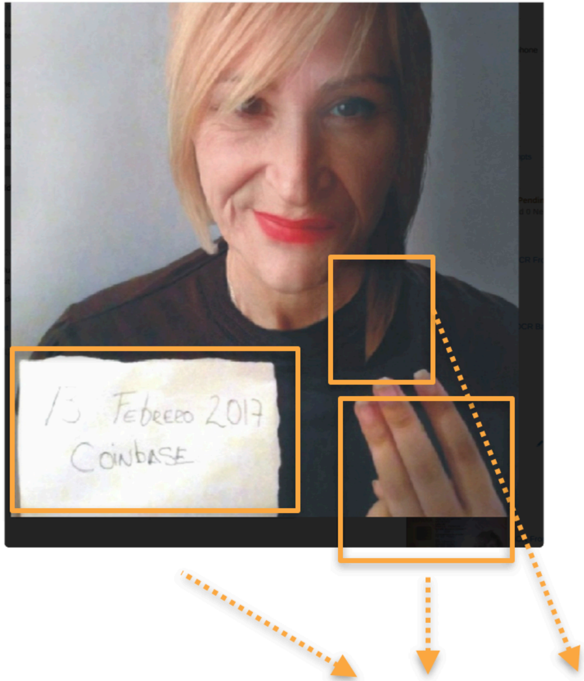
Romance / Tech Support Scams



phone inside image

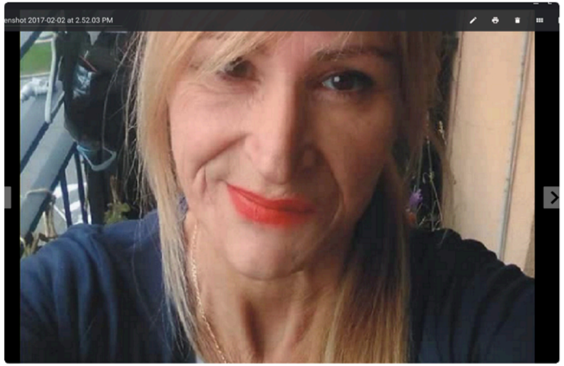
Selfie photos: Not fool proof

Photoshopped
image (notice hair)

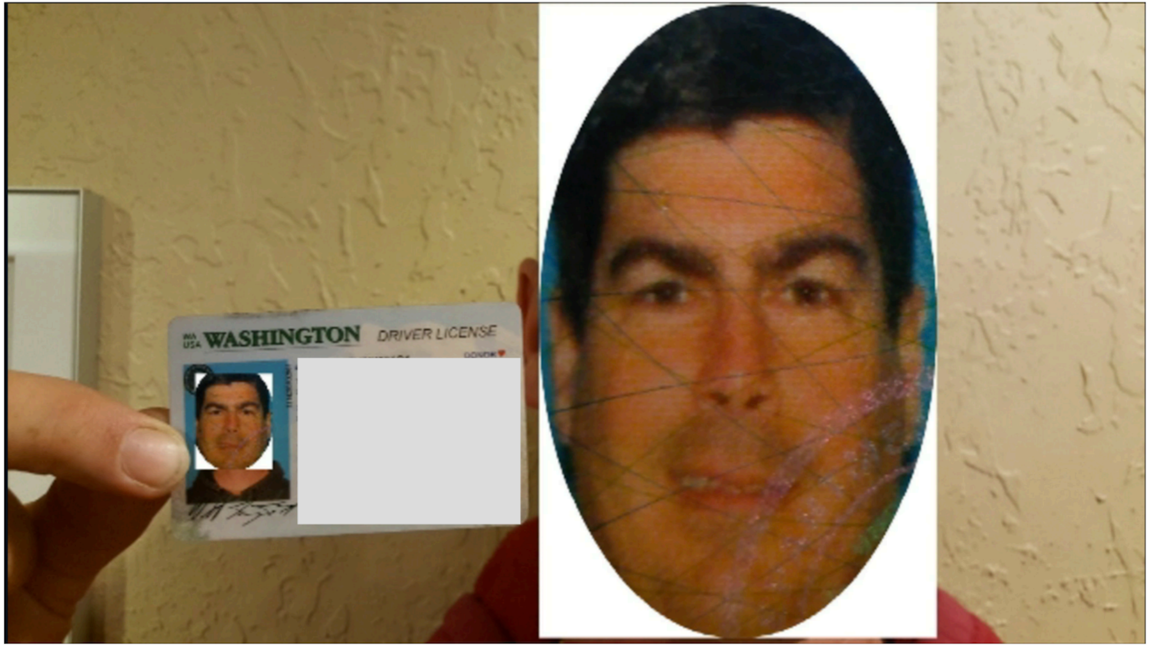


Photoshopped elements

Image scraped from
social media



Face Match for laughs



Account Takeovers

Two factor Authentication (2FA)

If you store anything of value online, you must have two factors:

- Something you know (strong password)
- Something you always have (physical device)

Unfortunately, this is how 2FA was implemented everywhere

“Something you always have (physical device)”

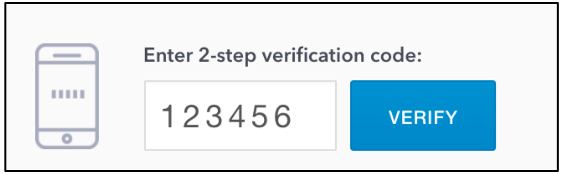
- Physical device was equated to phone number
- Easy to steal phone number:
  - Delivery attacks: read SMS online, SMS hijacking
  - Phone number theft: phone porting

Account takeovers using SIM Swap

1. scammer finds name, password and phone#

2. scammer ports phone# to device under his control

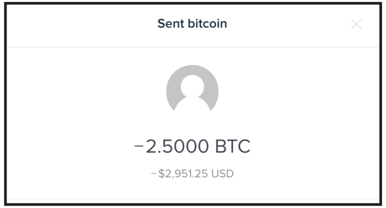
Don’t allow SMS 2FA



Enter 2-step verification code:

123456

3. scammer now receives 2FA codes via SMS



Sent bitcoin

−2.5000 BTC

−$2,951.25 USD

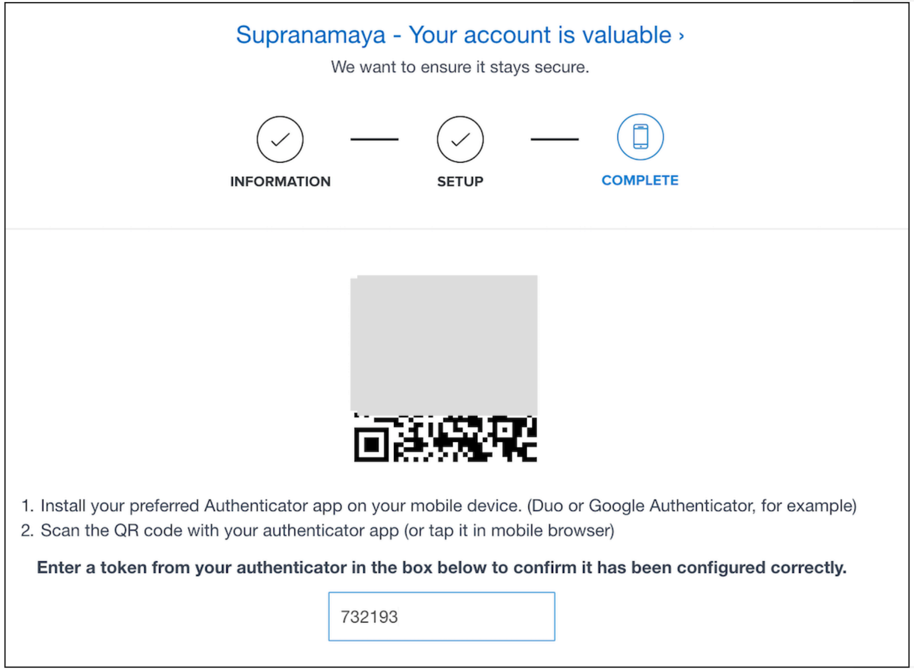
4. scammer logs in with password and 2FA and steals bitcoins

Recommendations for Coinbase users

Passwords: Use a password manager

2FA: install Google Authenticator

Why Authenticator / TOTP apps?



Supranamaya - Your account is valuable ›

We want to ensure it stays secure.

1. Install your preferred Authenticator app on your mobile device. (Duo or Google Authenticator, for example)
2. Scan the QR code with your authenticator app (or tap it in mobile browser)

Enter a token from your authenticator in the box below to confirm it has been configured correctly.

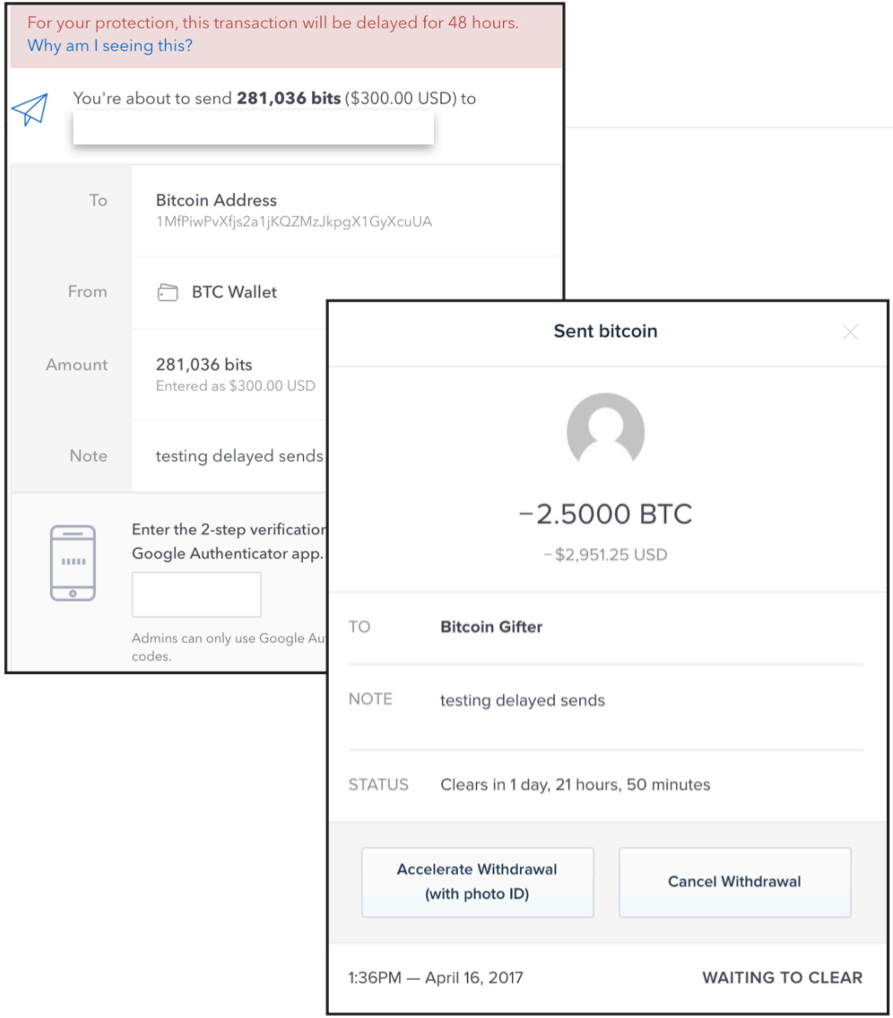
732193

Authenticator: nothing ever sent in the air

- Time-based One Time Password (TOTP)
- Secret set up once using QR codes

Detecting Account Takeovers

- Still need to protect SMS users
- Association Rule Mining to discover ML rules
- Detect suspicious withdrawals
- Delay for 48-72 hours



For your protection, this transaction will be delayed for 48 hours.
Why am I seeing this?

You're about to send **281,036 bits** ($300.00 USD) to

To: Bitcoin Address
1MfPiwPvXfjs2a1jKQZMzJkpgX1GyXcuUA

From: BTC Wallet

Amount: 281,036 bits
Entered as $300.00 USD

Note: testing delayed sends

Enter the 2-step verification
Google Authenticator app.

Admins can only use Google Au
codes.

Sent bitcoin

−2.5000 BTC
−$2,951.25 USD

TO: **Bitcoin Gifter**

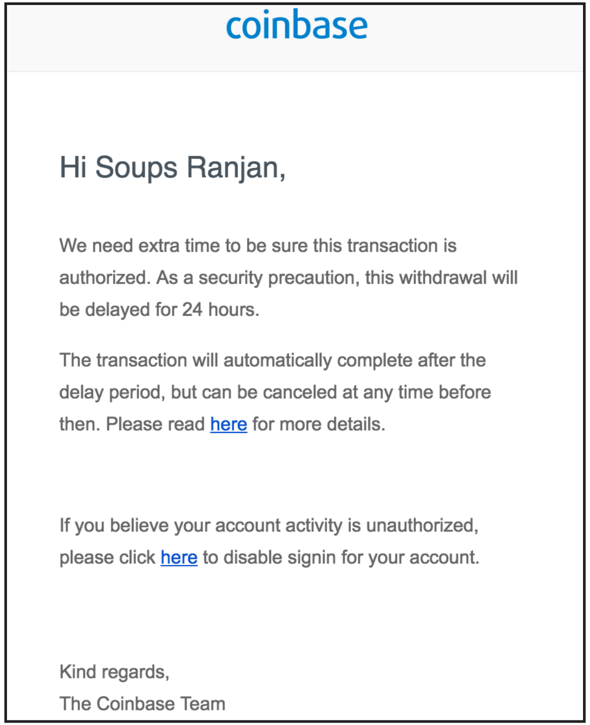
NOTE: testing delayed sends

STATUS: Clears in 1 day, 21 hours, 50 minutes

1:36PM — April 16, 2017 WAITING TO CLEAR

Victim of account takeover

- Victim receives SMS / email
- Can lock their account



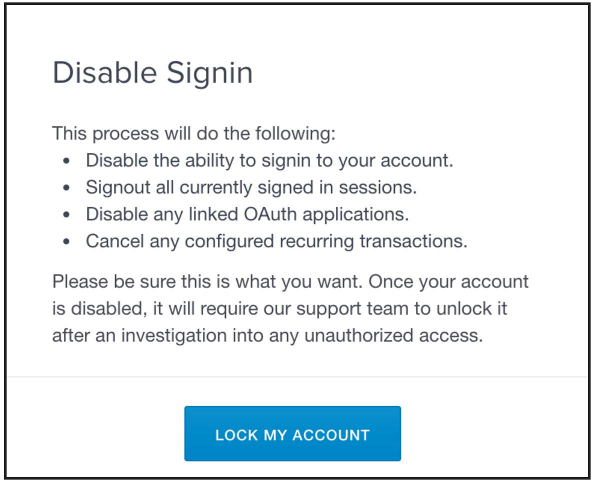
Hi Soups Ranjan,

We need extra time to be sure this transaction is authorized. As a security precaution, this withdrawal will be delayed for 24 hours.

The transaction will automatically complete after the delay period, but can be canceled at any time before then. Please read here for more details.

If you believe your account activity is unauthorized, please click here to disable signin for your account.

Kind regards,
The Coinbase Team



Disable Signin

This process will do the following:

- Disable the ability to signin to your account.
- Signout all currently signed in sessions.
- Disable any linked OAuth applications.
- Cancel any configured recurring transactions.

Please be sure this is what you want. Once your account is disabled, it will require our support team to unlock it after an investigation into any unauthorized access.

Protecting yourself online

Securing non-Coinbase sites

If you have Gauth on Coinbase, you are all set!

But many online sites still only support SMS based 2FA:

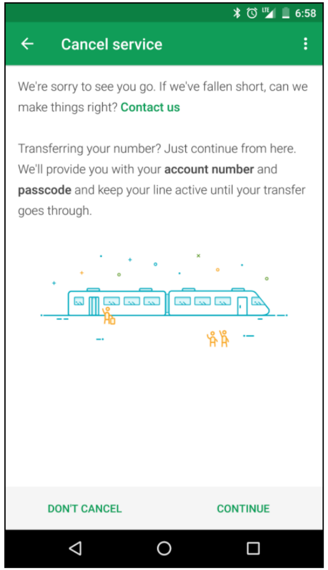
Call up telcos and put a **SIM lock:**

- Tell them you are already compromised
- ask them to only allow porting when you are in-store & ask for your ID

If on Android phone, **move to Google Fi:**

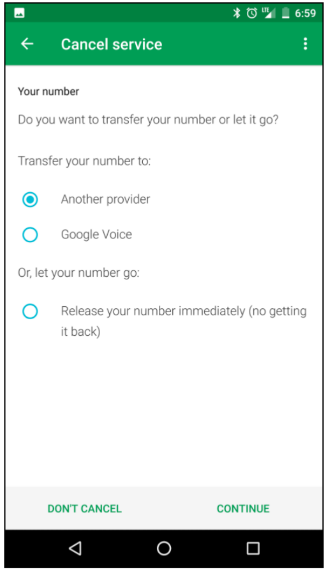
- No call centers, no social engineering

Google Fi - one more thing



We're sorry to see you go. If we've fallen short, can we make things right? Contact us

Transferring your number? Just continue from here. We'll provide you with your **account number** and **passcode** and keep your line active until your transfer goes through.



Your number

Do you want to transfer your number or let it go?

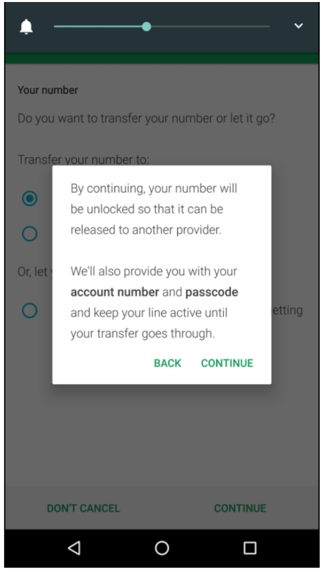
Transfer your number to:

● Another provider

○ Google Voice

Or, let your number go:

○ Release your number immediately (no getting it back)



By continuing, your number will be unlocked so that it can be released to another provider.

We'll also provide you with your **account number** and **passcode** and keep your line active until your transfer goes through.

Gmail + Google Fi => 2 factors reduced to 1

- both factors only protected by Google password
- With that password, attacker can stil port your Google Fi phone number
- Protect your Google account like a bank
- Use Gauth or Yubikey behind Google

SMS two-factor is Dead!

Data & Risk team

We are hiring:
data eng, data analysts, ML eng

soups@coinbase.com

https://medium.com/@soupsranjan