SpyCloud

Account Takeover in Financial Services

Bob Lyle

VP, Mobile, SpyCloud

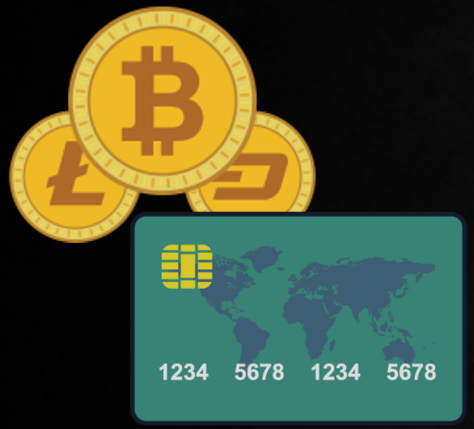
Chair, Device Security Group, GSMA

Philip Martin

Chief Information Security Officer

Coinbase

Fraud in the Financial Sector



$16.9B

2019 Fraud Losses Across 13M Instances

$46M AVERAGE FRAUD LOSSES PER DAY

15% Y/Y INCREASE IN FRAUD LOSSES

ACCOUNT TAKEOVER LEADS BANKS' DIGITAL FRAUD LOSSES

Source: Aite Group

Javelin 2020 Identity Fraud Report

SpyCloud

A Problem That Isn't Slowing Down

#1 **HACKING TECHNIQUE OVER THE LAST 4 YEARS**

300% **INCREASE Y/Y IN ATO ATTACKS**

40% **OF ATO FRAUD ACTIVITY OCCURS WITHIN 1 DAY**

Verizon 2020 Data Breach Investigations Report
2020 Digital Trust & Safety Index
Javelin 2020 Identity Fraud Report

SpyCloud

Enabled by Breach Data

162
FINANCIAL SERVICES COMPANIES IN THE FORTUNE 1000

95,108,228 **TOTAL EXPOSED ASSETS**

Email Addresses • Passwords • Phone Numbers • DOB
Addresses • Financial Assets • Social Handles ...

3.38M **CORPORATE CREDENTIALS**
Emails + Plaintext Passwords

375K **FINANCIAL ASSETS**
Credit card #, bank account #, and tax IDs

2.71M **PHONE NUMBERS**

SpyCloud

Corporate Credentials

What They Are

- Corporate email address + plaintext password pairs that have appeared in a data breach

How They Help Criminals

- Criminals can easily gain access to corporate systems, then exploit reused passwords to gain entry into personal accounts

SpyCloud

Financial Assets

What They Are

- Credit card numbers, bank account numbers, and tax IDs

How They Help Criminals

- Make fraudulent purchases
- Drain funds from accounts
- Resell card numbers and other stolen data to other criminals
- Collect victims' tax refunds

SpyCloud

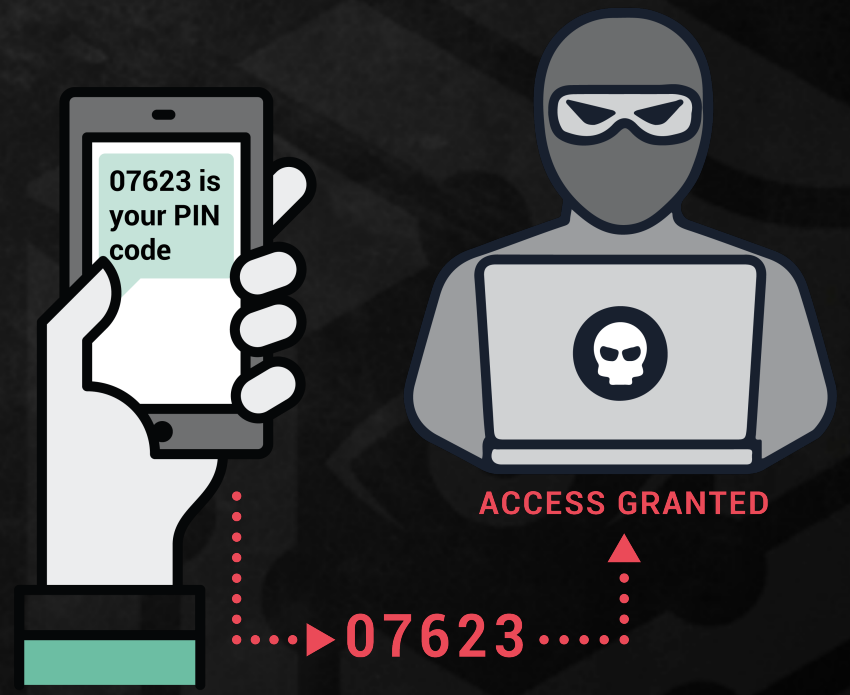
Phone Numbers

How They Help Criminals

- In combination with stolen credentials, criminals can use phone assets to bypass MFA with tactics like SIM swapping & phone porting

How They Help YOU

- Augment your account risk decision algorithms by using the phone number as the identity marker

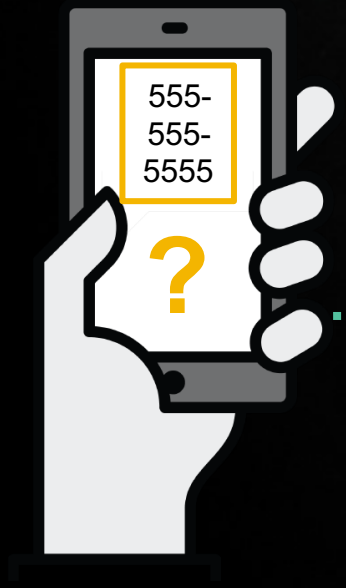


2.3 BILLION PHONE NUMBERS HAVE BEEN EXPOSED IN BREACHES

SpyCloud

Using Phone Numbers as Identifiers of Risk

Augment your account risk decision algorithms by using the phone number as the identity marker



Breach Exposure Check

10 breach records found with phone number + plaintext passwords

Transaction stopped

1 breach records found with phone number

Step-up authentication required

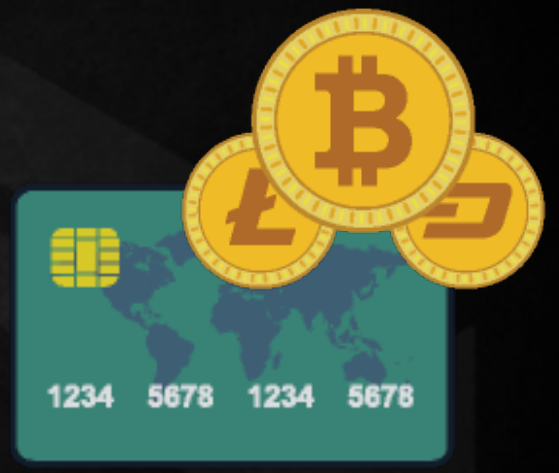
No exposures found

Transaction proceeds

SpyCloud

Account Takeover & Financial Fraud

How one fintech company uses **breach data** to inform their multi-faceted approach to ATO:



- **Credential check**
  Even with 2FA required for all consumers, resetting compromised credentials helps combat targeted ATO and reduce support tickets due to “partial logins”
- **Internal modeling**
  Adjust internal ATO models to identify high-risk users; ex, any recent breach exposure may increase risk of SIM-swapping, even without an exposed password
- **Root cause & trend analysis**
  Correlation of other potential accounts that may be affected
- **Infected user outreach**
  Since users with malware-infected systems are at very high risk of ATO and financial fraud, this enterprise takes a high-touch approach with users whose details appear in botnet logs.

__Thousands__ of users’ accounts have been protected to date, representing __tens of millions of dollars!__

SpyCloud