Account Takeover in Financial Services

Bob Lyle
VP, Mobile, SpyCloud
Chair, Device Security Group, GSMA

Philip Martin
Chief Information Security Officer
Coinbase
2019 Fraud Losses Across 13M Instances

$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

Account Takeover: 89%

Source: Aite Group

Synthetic Fraud: 42%
Mobile RDC: 32%
First-party Fraud: 32%
CNP Fraud: 21%

Javelin 2020 Identity Fraud Report
A Problem That Isn’t Slowing Down

1. Hacking technique over the last 4 years

2. 300% increase Y/Y in ATO attacks

3. 40% of ATO fraud activity occurs within 1 day
Enabled by Breach Data

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

162 FINANCIAL SERVICES COMPANIES IN THE FORTUNE 1000

SpyCloud 2021 Fortune 1000 Breach Exposure Report
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
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
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
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 record found with phone number: Step-up authentication required
- No exposures found: Transaction proceeds
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.