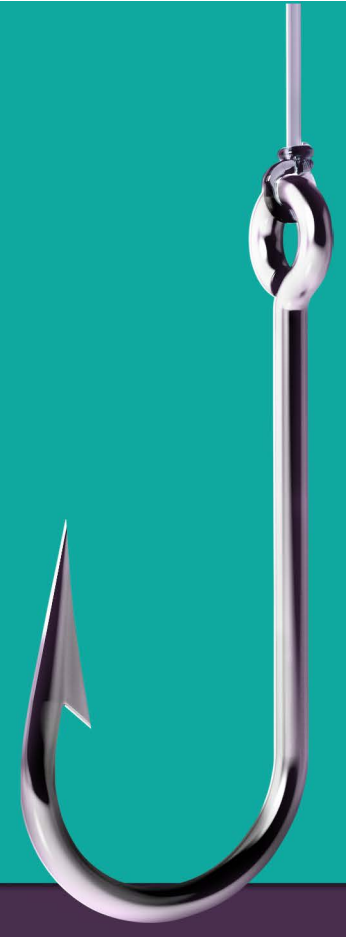
INCOGNIA™

Top 4 Contributors to Account Takeover

The end goal of fraudsters on mobile is account takeover (ATO). For fintech apps, ATO can result in funds being transferred out of a user's account. For mcommerce apps, ATO results in loss of funds from mobile wallets, gift cards and also chargebacks to the vendor.



Weak/reused passwords

Passwords are weak and create too much friction. As more and more internet-connected services have become available to help people perform day to day activities, remembering passwords has become increasingly challenging, leading users to start reusing passwords.

Password resets are the leading topic for all IT help desk calls.

30% - 50%

of all IT help desk calls are for password resets[2]

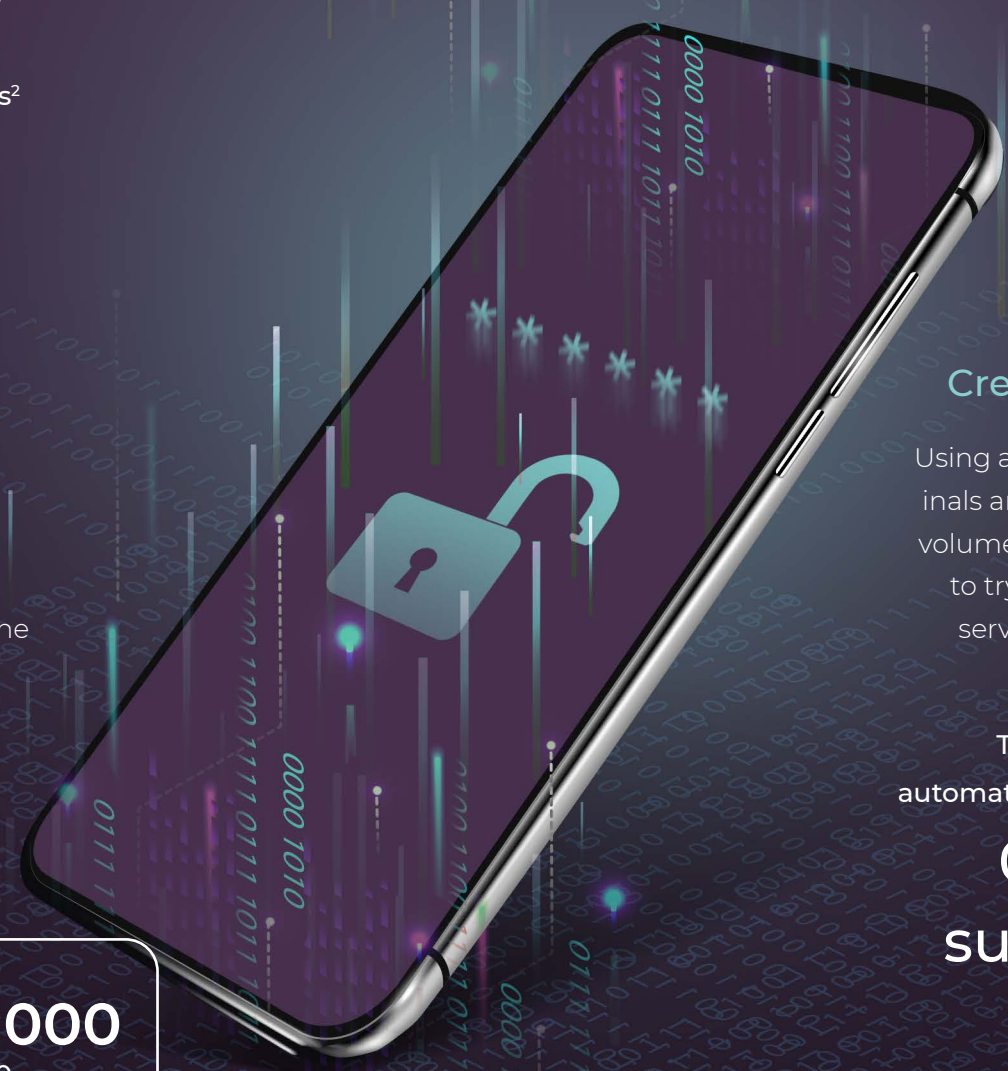
Social engineering scams

Social engineering covers a wide range of activities aimed at tricking users into sharing sensitive information that is then used to take over accounts and commit fraud.

Identity fraud was the largest contributor to fraud losses in 2020

$56B
total fraud losses

$43B
identity fraud losses



Data breaches

With frequent data breaches, passwords have become publicly available, enabling bad actors to take over online accounts with ease.

The number of data breaches in the US continues to climb.

662
2010

>1000
2020

Number of data breaches U.S.

Credential Stuffing

Using automation, cybercriminals are able to test out large volumes of leaked credentials to try to login in to as many services as possible, taking over accounts at scale.

Typical success rate for automated credential stuffing

0.5% to 3% success rate

About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication to banks, fintech, and mCommerce companies, for increased mobile revenue and lower fraud losses. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns and is a key enabler for Zero-Factor Authentication. Deployed in more than 150 million devices, Incognia delivers a highly precise risk signal with extremely low false-positive rates.