ARKOSE LABS™

# 4 Modern Bot Attacks Targeting Bank Consumers

### Account Takeover (ATO)

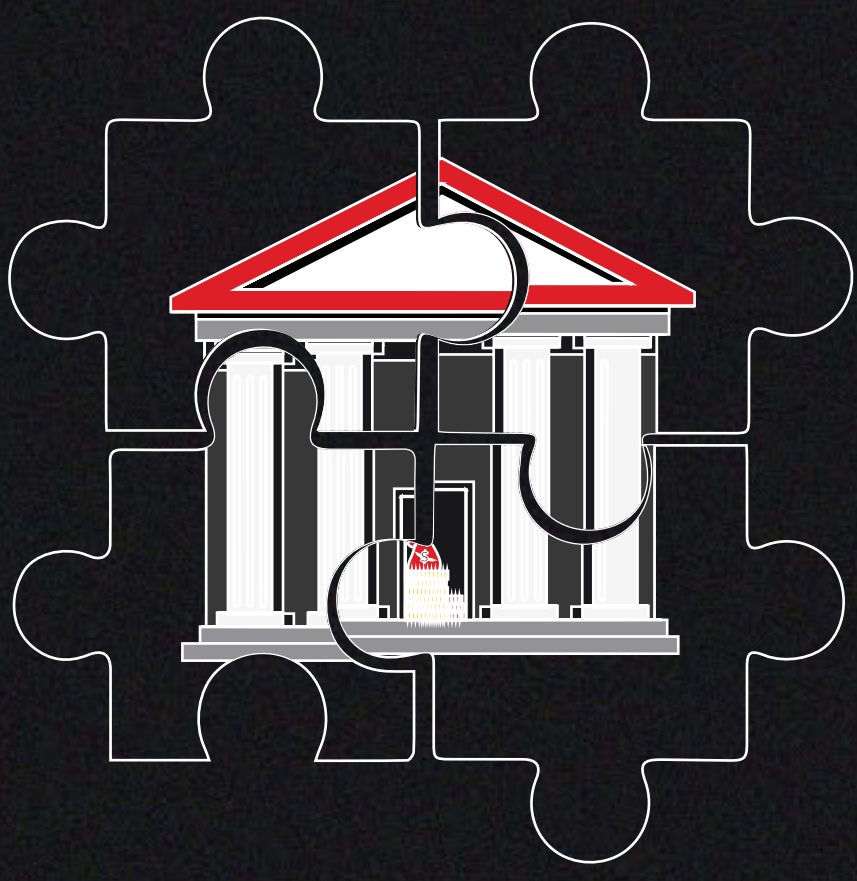
The #1 attack type for banks, ATO is a frequent starting point for identity theft. It drains your customers' life savings, acts as a conduit for application fraud, and sets up heinous downstream crimes like money laundering.

**$15.6**
**billion in reported U.S. losses[1]**

### MFA Compromise

Your customers are falling prey to phishing sites that closely mimic legitimate ones. Adversary-in-the-middle reverse proxy phishing attacks are especially dangerous because they allow bad actors to overcome your MFA security measures.

**15%**
**of credential-harvesting cases use MFA phishing kits[2]**



**$300K**
**lost to SMS toll fraud in just 12 hours[3]**

**$6.2**
**billion in reported fraud losses[4]**

### SMS Toll Fraud

SMS-based two-factor authentication (2FA) creates a major vulnerability as fake account sign-ups rack up massive charges via premium-rate SMS verifications. Attackers collude with rogue telecoms to split the profits, leaving your financial institution to foot the bill.

### New Account Fraud

Failure to stop new account fraud can drive up expensive KYC processes and systems that degrade website performance, gobble up resources, and divert your attention away from enhancing the consumer experience.

## How Arkose Labs Puts the Puzzle Pieces Together

Protect your consumers while delivering a great experience. Hostile actors attacking your login and registration flows pose a substantial threat to your bank — deploying bots, automated scripts, human fraud farms and AI-driven techniques at scale, at high speed and with increasing sophistication to evade detection.

Arkose Titan stops hostile actors before they make an impact, while preserving a seamless experience for genuine consumers. We help leading financial institutions — including 2 of the 3 largest banks globally — safeguard their highest-risk touch points by countering the most sophisticated attacks and making them economically unviable to continue.


[1]https://www.frbservices.org/news/fed360/issues/021726/fraud-mitigation-account-takeover

[2]https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf

[3]https://www.arkoselabs.com/resource/sms-toll-fraud/

[4]https://www.frbservices.org/news/fed360/issues/090225/industry-perspective-new-account-fraud


BOOK A DEMO

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America. 