HOW TECHNOLOGY IS DRIVING ACCOUNT TAKEOVER INDUSTRIALIZATION

ARTICLE HIGHLIGHTS

- **Account takeover** is becoming an industrialized process powered by automation, artificial intelligence (AI) and organized criminal ecosystems.
- **Fraud-as-a-Service** and **generative AI** have lowered fraud barriers, enabling larger-scale, sophisticated attacks.
- **Static passwords** and **basic multi-factor authorization** may be insufficient against adaptive AI-driven threats. Layered, dynamic defenses are essential as a result.

Account takeover fraud seems to be transforming into an industrialized, technology-driven operation (Off-site). What was once a manual crime of opportunity is now powered by automation, artificial intelligence and organized service models. Fraud-as-a-Service platforms provide ready-to-use toolkits, infrastructure and support, enabling even low-skilled criminals to launch large-scale fraud campaigns. Generative AI amplifies this threat by producing convincing attack narratives, deepfake videos and synthetic voices that mimic legitimate interactions with alarming accuracy. Specialized software and malware has the ability to potentially bypass traditional authentication controls and overwhelm financial institution defenses at scale. These innovations have lowered barriers to entry, accelerated attack speed and expanded global reach – making account takeover a highly organized, adaptive and profitable criminal enterprise.

FRAUD-AS-A-SERVICE: CRIME AS A SUBSCRIPTION

The rise of Fraud-as-a-Service has accelerated the threat of account takeover (Off-site). Criminals are beginning to run their fraud operations like legitimate businesses, even offering technical support to their customers. They sell ready-made fraud kits that include everything needed to break into accounts, such as fake websites and automated tools. This makes it easier for criminals with little technical skill to launch large-scale attacks against financial services organizations. These kits often include tools to test stolen passwords, hide locations and move money quickly, making attacks faster and harder to detect.

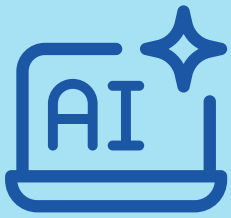
How criminals use Fraud-as-a-Service to commit account takeover:

1. **Buy a fraud kit online that includes phishing templates and automation tools**
2. **Send fake messages or set up fake banking sites to trick customers**
3. **Use stolen details to log in and change account settings**
4. **Move money through multiple accounts to avoid detection**

HOW TECHNOLOGY IS DRIVING ACCOUNT TAKEOVER INDUSTRIALIZATION

AI-POWERED THEFT: MAKING ACCOUNT TAKEOVER EASIER

Modern technology, such as AI, can accelerate every step of the criminals' workflows. AI can execute scams faster and make them more believable. Criminals use AI to generate multilingual scripts, synthesize voices for phone scams and summarize leaked datasets to find high-value targets. AI also can generate fake images or videos that look real, helping criminals impersonate bank employees or customers.



How criminals use AI technologies to commit account takeover:

1. **Create realistic emails or texts that look as though they are from a trusted institution**
2. **Call victims using AI-generated voices that sound human and legitimate**
3. **Deceive victims into sharing security codes or approving fake transactions with more polished phishing content**
4. **Use stolen details to take over accounts with credential stuffing — automated login attempts using stolen usernames and passwords — and lock out the true account holder**

SOFTWARE DESIGNED TO STEAL INFORMATION

Specialized malware is built to capture keystrokes and other device interaction, including passwords, security codes and session tokens. Browser-focused modules extract saved passwords, autofill data and session cookies, enabling immediate impersonation without reauthentication. Some programs use keyloggers (surveillance software or hardware) that secretly record everything the user types, while others grab saved passwords from browsers. Mobile keyloggers can read text messages or app notifications to steal one-time codes. Once criminals have this data, they can log in while minimizing detection and reduce triggering alerts.

How criminals use malware to commit account takeover:

1. **Deceive victims into downloading malware through fake links or attachments**
2. **Collect passwords, security codes and session tokens**
3. **Use stolen tokens to log in without needing a password**
4. **Change account details and transfer funds before detection**

HOW TECHNOLOGY IS DRIVING ACCOUNT TAKEOVER INDUSTRIALIZATION

AUTOMATED BOTS: OVERWHELMING SECURITY

Bots are automated software applications that perform repetitive tasks over the internet, including mimicking online human behaviors. These behaviors can include mouse movement and navigation paths to evade simple bot detectors. Criminals use bots to industrialize attacks against authentication and payment endpoints, as well as test thousands of stolen passwords, reset accounts and complete transactions at speed and scale. Automated bots are increasingly sophisticated and can solve or circumvent CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) security measures using machine learning or outsourced human-solving services – platforms that employ real people to solve CAPTCHAs. While CAPTCHA was designed to remove one of the most common barriers to automated attacks, it does not always help do so. Once successfully evading a CAPTCHA, bots simulate legitimate actions, such as logging in, browsing or initiating small transactions, so their activity blends in with normal customer patterns. This can make it difficult for fraud detection systems to distinguish between genuine users and malicious automation. In addition, when bots operate at low velocity or distribute actions across multiple accounts, they may avoid triggering anomaly-based alerts.

How criminals use bots to commit account takeover fraud:

1. **Deploy bots to test stolen passwords across thousands of financial institutions' online banking portals**
2. **Use bots to trigger password resets**
3. **Log in and change account details automatically**
4. **Initiate transfers or payments without manual effort**

ADVERSARY IN THE MIDDLE: HIDING IN PLAIN SIGHT

Adversary-in-the-middle attacks work by silently intercepting and relaying communications between the legitimate account holder and the financial institution, allowing the criminal to capture credentials, session tokens or multi-factor authentication challenges in real time. Because the attacker sits between the legitimate parties, both sides believe they are communicating directly with each other, making the criminal's intrusion extremely difficult to detect. Identity and location can be further obscured by chaining virtual private networks (VPNs) or device emulation layers to replicate screen sizes, language settings and time zones to match expected profiles. Some criminal operations pair this with subscriber identity module (SIM)-swap-driven rerouting of short message service (SMS) codes with "push fatigue" tactics that bombard users with approvals until one is accepted. Criminals also can create fake websites that look identical to legitimate ones.

HOW TECHNOLOGY IS DRIVING ACCOUNT TAKEOVER INDUSTRIALIZATION

When customers enter their login credentials on these fraudulent sites, criminals can capture sensitive information, such as usernames and passcodes, which then can be used to access the customer's actual account on the real website. This makes the attack look legitimate and helps criminals bypass multi-factor authentication.

How criminals use adversary-in-the-middle attacks to commit ATO:

1. **Set up a fake website that mirrors a real financial institution's legitimate site**
2. **Deceive victims into logging in through the fake site**
3. **Capture login details and security codes during the process**
4. **Use those details to take over accounts and move money**

CONCLUSION

Account takeover may be evolving into an industrialized cybercrime model, driven by automation, AI and organized service ecosystems. Fraud-as-a-Service platforms, generative AI and advanced malware have transformed attacks from isolated incidents into scalable, high-speed operations that exploit systemic weaknesses.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, use of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.