KEY DRIVERS OF ACCOUNT TAKEOVER FRAUD IN TODAY'S LANDSCAPE

User authentication has become more complex with the rise in digital banking and payments. Recent trends reveal not only an increase in account takeover fraud losses, but also in the frequency and sophistication of account takeover schemes. These trends are driven in part by the combination of consumers' expanded digital footprints, criminals' wider access to user data, and emerging technologies that can make account takeover easier to automate. This article examines some of the key drivers for account takeover fraud today.

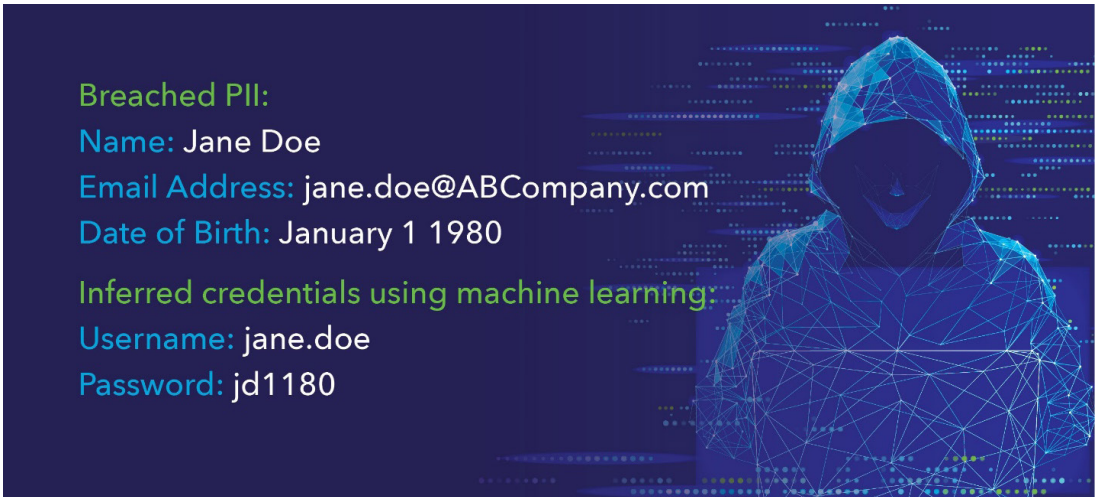
WHY ACCOUNT TAKEOVER FRAUD IS GROWING

Data breaches have become almost commonplace. In recent years, large-scale data breaches have become more frequent (Off-site), exposing billions of information pairs and sensitive customer information to criminals and fueling credential stuffing* attempts. Users' poor password management (Off-site) – including reused and weak passwords – often makes this technique successful for account takeover attacks.

***Credential stuffing** is when criminals systemically test passwords for a given username until the correct combination is identified.

Breached data can also be incorporated into phishing messages to more convincingly deceive victims into sharing their financial account credentials.

New tools are available to automate account takeover attacks. Originally, criminals typically worked manually or with simple scripts to carry out credential stuffing. Today, they rely on adaptive artificial intelligence (AI) technologies to conduct credential stuffing with more sophistication and at greater scale, enabling high-volume, repeatable login attempts. Bad actors may leverage machine learning to intelligently pair or infer credentials based on email addresses and personally identifiable information (PII).



KEY DRIVERS OF ACCOUNT TAKEOVER FRAUD IN TODAY'S LANDSCAPE

The increased sophistication of scripted attacks also has allowed bots to perform tasks that emulate human behavior (e.g., mouse movements, typing patterns or browsing behaviors). As a result, traditional bot detection may now be less effective in identifying account takeover risks.

Generative AI has increased the ease and effectiveness of social engineering. Before the era of generative AI, phishing messages often were filled with typos and grammatical errors, or their tone was unusual or strange. With the emergence of generative AI-based tools, criminals can create highly polished content in any language that often is difficult to distinguish from valid correspondence, enabling more effective deception of victims into willingly providing their account credentials. Furthermore, generative AI has helped facilitate more effective impersonation of account holders to their financial institutions. Today, deepfakes* can be produced more quickly and convincingly using generative AI. With these tools quickly evolving, deepfake technology may become even more sophisticated over time.

***Deepfakes** are synthetic media used to convincingly imitate a person's appearance, voice or mannerisms.

CONCLUSION

The wide availability of personally identifiable information, new tools to automate account takeover, and the use of generative AI to make phishing and impersonation more sophisticated have contributed to the persistent threat of account takeover fraud for financial institutions. Given evolving uses for automation and AI in the fraud ecosystem, account takeover is likely to be a continued challenge for financial institutions and their customers. To help combat it, financial institutions can leverage a layered approach to enhance account takeover detection and prevention. See Module 3 for a more detailed look at available approaches, technologies and techniques.

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, utilization 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.