Thomson Reuters™

How financial institutions and their customers can prevent account takeover fraud

In our increasingly interconnected world, fraudsters use digital technology in nefariously innovative ways. According to the U.S. Federal Trade Commission, fraud accounted for $10 billion in losses in 2023 due to online activity.

With identity theft and data breaches exploding, banks and other financial services organizations must better protect their customers from the impact of account takeovers (ATOs). An ATO is a form of identity fraud where the fraudster leverages a financial customer's existing credentials to take control of that customer's account. The impacts of a successful ATO can range from a one-time purchase to using the stolen account for money laundering and other illicit activity.

Here are four key approaches that financial services organizations can put in place in the battle against potentially disastrous ATOs:

1 Use a variety of transaction factors to confirm digital identification.

Two-factor authentication has been beneficial for protecting accounts. But with fraudsters constantly devising new methods of digital attacks, financial organizations need to add new lines of defense to verify customer identities. These lines of defense could include:

Fingerprint matching and retinal scans, which are already used by many banking entities.

Live facial verification, a newer-generation technology that can match a person making a transaction with an on-file photograph.

Behavioral biometrics and analytics that allow a financial organization to verify a customer's identity through their online behavioral patterns.

2 Adopt a risk-based approach to fraud detection and prevention.

Financial institutions should keep continuously current on new fraud risks so that they can establish proactive protocols and strategies, including technological innovations, to mitigate the impact of those risks.

3 Explore the use of AI-powered technology.

Artificial intelligence (AI) is another still-emerging technology, but it promises to enhance fraud prevention, in part by its ability to continuously "learn." This capability can allow financial organizations to better respond to and even anticipate new types of threats. Techniques such as behavioral biometrics will be incorporating AI and machine learning to further their effectiveness.

4 Engage customers in ATO prevention.

Financial institutions can educate customers about the dangers of digital ID theft techniques and thus be more vigilant about phishing emails, malware, and fraudulent phone scammers pretending to be bank representatives. In addition, a financial services organization should clearly inform customers about the use of any data-based ATO prevention techniques and assure them that their data is secure.

Phishing emails

Malware

Phone scammers

Preventing account takeover: New threats and new tools in digital authentication

Learn more about how financial organizations and their customers can better protect themselves from the potentially disastrous impact of account takeovers by reading the new white paper on preventing ATOs.

White paper

Thomson Reuters™