

Account Takeover (ATO) Fraud

The Problem and Solution

Account takeover (ATO) fraud is a type of identity theft in which a fraudster takes control of a legitimate customer's bank or online merchant account.



A Snapshot of the ATO Threat

#1

fraud scam

ATO attacks topped the list of 2021's five most common fraud scams.

Source: [Feedzai Q2 2022 Financial Crime Report](#)

\$11.4 Bn

Fraud losses related to ATO attacks reported in 2021 - up 90% from 2020.

Source: [Javelin](#)

40%

Share of ATO fraud activity that occurs daily.

Source: [Javelin](#)

80%

Increased share of new banking trojans - malware that enables ATO - reported in the first half of 2021.

Source: [Nokia](#)

\$635.4 Bn

Projected U.S. losses from all types of identity fraud (including ATO) by 2023.

Source: [Aite Report](#)

How ATO Fraud Impacts Victims

~50%

of ATO victims

know who compromised their account - an event known as "family and friendly fraud."

Source: [Aite Report](#)

38%

of U.S. consumers

experienced an ATO fraud event in the previous 2 years.

Source: [Aite Report](#)

30%

of identity theft victims

said it took longer than 100 hours to recover from the impacts of fraud.

Source: [Aite Report](#)

What Fraudsters Do After an ATO Attack

17%

Sent a wire transfer

15%

Change account contact information

15%

Use Zelle, Venmo, or other P2P services to transfer money

14%

Use bill pay or ACH to transfer money

13%

Use reward points to make purchases

Source: [Aite Report](#)

How ATO Impacts Banks

~33%

Of identity fraud victims

say their bank did not satisfactorily resolve their problems.

Source: [Javelin](#)

38%

Of ATO victims

closed their accounts at their bank where the fraud occurred.

Source: [Javelin](#)

12-13%

Of customers

are unlikely to do business with a bank where an account or loan was opened in their name.

Source: [Aite Report](#)

3 Steps to Prevent ATO Attacks

Step 1

Think Prevention-First

Reacting to ATO or detecting malware after an attack doesn't work anymore. Focus on stopping ATO attacks before they can do any damage.

Step 2

Know Your Users

Build a complete profile of your customers based on how they interact with a bank's system. Get to know them at both a behavioral and biometric level.

Step 3

Protect the Customer Journey

Silently authenticate customers at each interaction to ensure they are who they claim to be without adding friction to their experience.