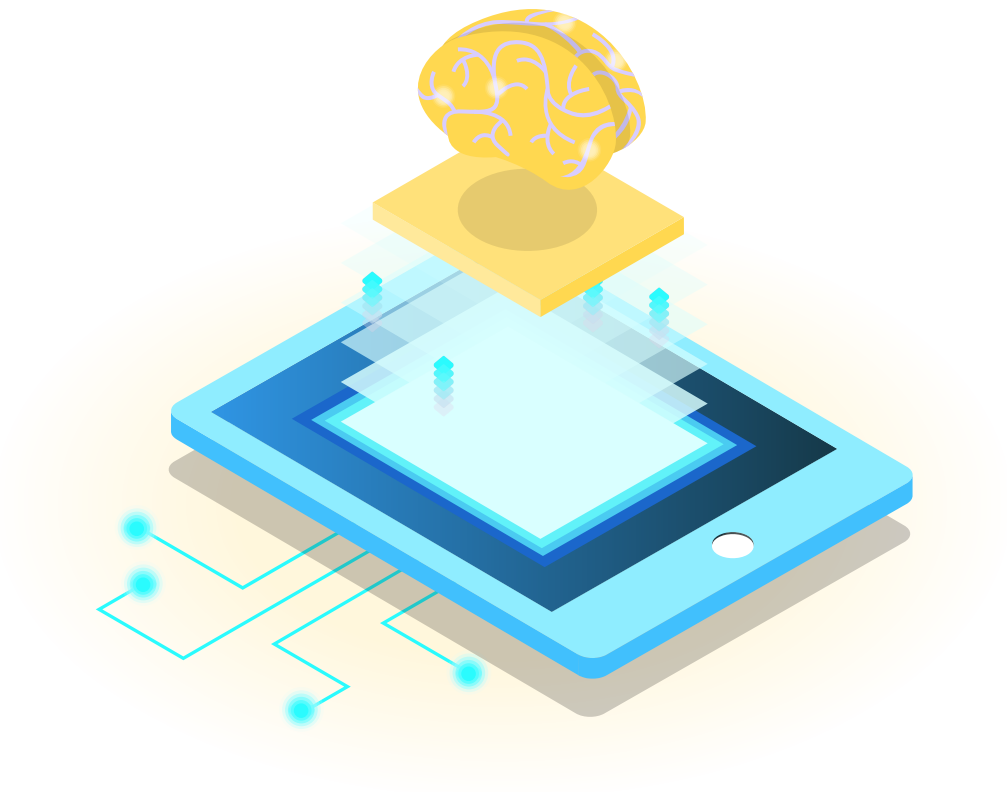
oscilar

The Ultimate Guide To Account Takeover Prevention While Reducing User Friction

Table of Contents



Introduction

Account takeover (ATO) is a form of identity fraud that affects businesses in all sectors offering digital products. Account takeover is where a fraudster takes full control of a legitimate account and uses it for fraudulent purposes. Once that access is achieved, the fraudster can use the account for all kinds of opportunistic and malicious ends. As part of the account takeover, the fraudster may change the user's password to lock them out, and change their email address and phone numbers so the good user doesn't receive any additional communication about activity on their account.

> According to Javelin Strategy's 2022 Identity Fraud Study, in 2021, traditional identity fraud losses—those involving any use of a consumer's personal information to achieve illicit financial gain—amounted to **$24 billion (USD) and affected 15 million U.S. consumers**. Additionally, the total identity fraud impact, by combining traditional identity fraud and identity fraud scam statistics, resulted in **$52 billion of loss affecting 42 million U.S. consumer victims** — 12.6% of the US population. The downstream effect of more data breaches? A rise in account takeover fraud.

Perhaps unsurprisingly, account takeover fraud is one of the fastest-growing forms of fraud and abuse. The damage done by account takeovers occurs on multiple fronts: negative PR, legal and compliance implications, a drop in the value of your customers, financial loss, and more.

How do account takeovers take place?

Account takeover is the result of a wide range of fraudulent activity, **allowing criminals to steal user credentials and crack open accounts on a large scale**. Account takeover attack patterns are becoming more sophisticated with fraudsters launching orchestrated, multi-step attacks that allow them to disguise their malicious intent. **Fraudsters use bots, human labor, or a combination of the two to maximize their profits**.

Large-scale account takeover is mostly bot-driven, allowing fraudsters to mount multiple attacks for maximum ROI. Human labor is used to circumvent controls or to carry out more targeted attacks.

Attacks can vary by industry but, broadly speaking, account takeover attacks have the following lifecycle:

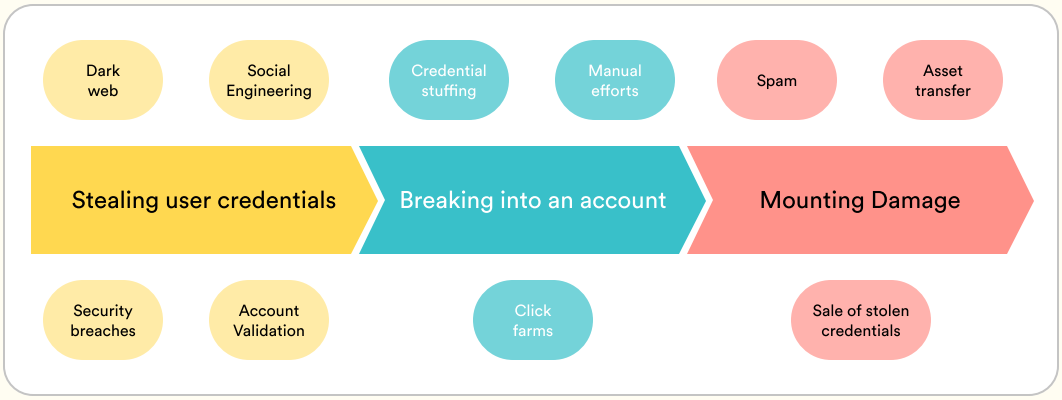


Figure 1. Lifecycle of account takeover attacks

Stealing user credentials

Attackers use a multitude of techniques to acquire user credentials as outlined below:

1 The dark web

An estimated **15 billion stolen credentials** are available on the dark web. Each leaked account credentials poses an account takeover threat to dozens of online accounts. Some fraud marketplaces even give additional details about the real user of the stolen credentials like their biography and location details to bypass security controls.

2 Social engineering

Social engineering attacks such as phishing entail tricking people into revealing user credentials like passwords or MFA codes. This is **a highly effective method of harvesting identity data at scale**; the costs can be dramatic as well.

3 Security breaches

Attackers can **break into a website, steal user credentials and use them to mount damage on the site**

4 Account validation

Fraudsters **manually exploit account registration processes for high-value accounts** to test whether an account identifier is valid or not. This lets them clean their list of stolen credentials before they attempt to use them for logging in.

Breaking into an account using stolen user credentials

1 Credential stuffing

Credential stuffing is a tactic used by cybercriminals to **obtain a list of credentials from a variety of password leaks**. And use bots to try multiple username and password combinations until a match is found.

2 Manual efforts

In this style of attacks, attackers **manually break into high-value accounts** using credentials stolen from any of the above methods

3 Click farms

In order to bypass bot challenges like CAPTCHA, **fraudsters hire low cost workers, mostly in developing countries, to mimic good users and login using stolen credentials**. Sometimes, in a hybrid mode, click farms are used along with bots, where a human worker is utilized only when the bot encounters a CAPTCHA.

Damage after account compromise

Attackers use a multitude of techniques to acquire user credentials as outlined below:

1 Spam

Attackers use stolen user credentials to create spam on the website often **causing brand damage to the company while also degrading user experience and trust**.

2 Transfer assets of value

A very common purpose of launching account takeover attacks is to transfer assets of value, be it money or NFTs, to themselves, thereby **causing financial damage to users**.

3 Sell the stolen credential to others

Stolen user credentials are materially **valuable on the dark web** making it a frequent use of account takeover attacks.

Limitations of existing approaches

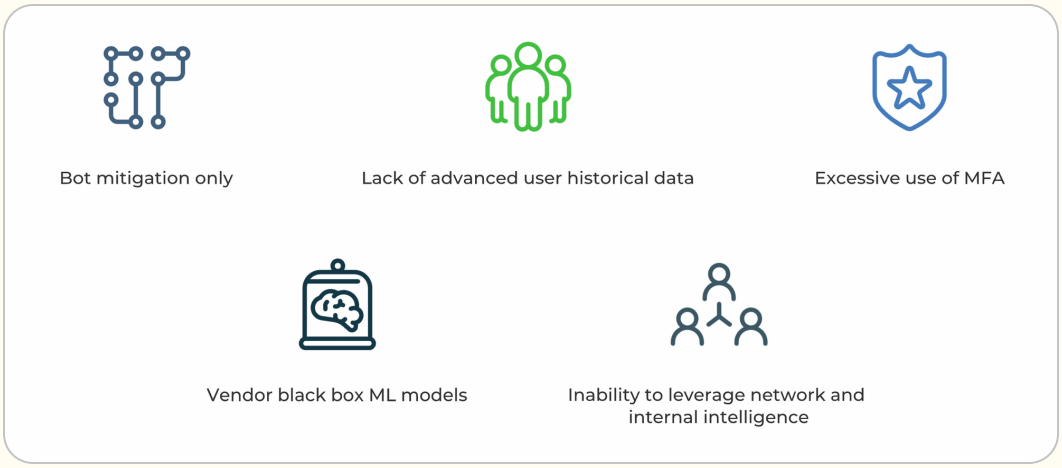


Figure 2. Limitations of existing approaches

1 Bot mitigation capability only

It is easier to discern bots from humans. The challenge arises while discerning good users from fraudulent (human) ones. Most account takeover approaches adopt simplistic detection practices that lend themselves to narrowly performing bot mitigation only. Such approaches typically involve **rules only** or **simplistic ML** features and models. While these might be easier to get started with, they are **fundamentally less effective in detecting sophisticated account takeover attacks**.

2 Lack of advanced historical user behavior data

Conventional account takeover approaches utilize **simplistic historical features** such as the user's browser id and **IP address history** that detect new IP addresses or new browsers used while logging in. This method **might have a good recall but suffers from low precision**; resulting in introducing friction for a large number of users. Advanced historical user behavioral features are required for striking a balance between user friction and catching fraud.

3 Excessive application of Multi-Factor Authentication (MFA)

While **MFA provides maximum fortification, using it as a one-size-fits-all approach blocks good users at a considerable rate introducing unwanted friction in the user experience**. Token-based authentication has become increasingly expensive and fraudsters have found ways to elude it at scale. **Fraudsters will bypass SMS verification using social engineering**, whereas genuine customers run the risk of being blocked or blacklisted when they have bad mobile reception or are operating from similar areas to fraudsters.

4 Vendor black-box machine learning models

Several 3rd party tools offer account takeover risk scores using black box machine learning models that offer limited or no explainability. As the sophistication of account takeover attacks experienced by the business increases, the **occurrence of high false positives and limited customization offered by black box machine learning models holds back fraud detection efforts significantly**. Ultimately, custom machine learning models trained on the data available to the business coupled with historical user behavior analysis is the most effective approach.

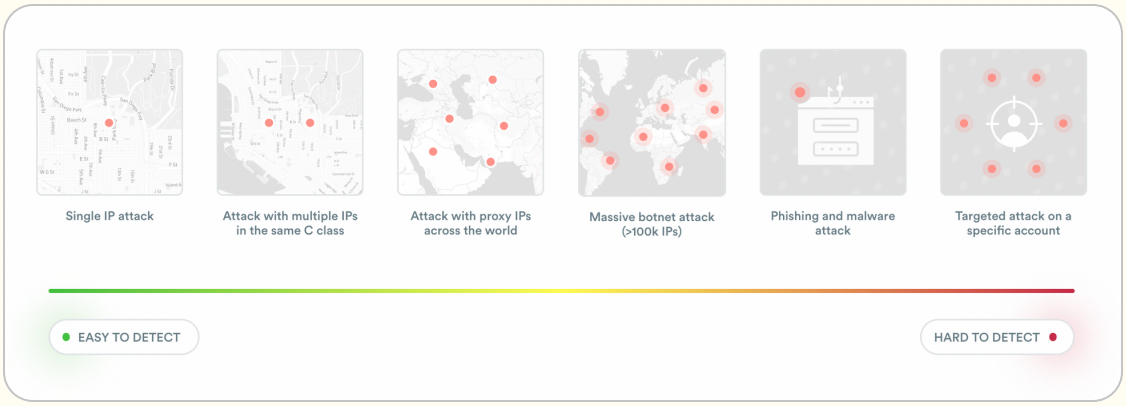
5 Inability to leverage internal and network intelligence

Businesses often use a single risk-based fraud detection solution to mitigate fraud. Due to the ever-evolving nature of fraud and the natural limitations on the decisioning data available to any single provider, such single-dimensional probabilistic risk assessments are largely ineffective at mitigating fraud holistically. **A better approach is to leverage 3rd party tools, that have intelligence from a large number of attacks, in conjunction with internal historical user behavior data**. Typically, it is best to leverage network intelligence for features that are costly for fraudsters to change such as IP addresses and devices.

6 Static CAPTCHA

Traditional CAPTCHAs are **designed to address large-scale untrained bots and can fall victim to trained automation and human fraud attacks**. Machine vision technology enables bots to recognize and complete photo-based challenges at scale. As CAPTCHA challenges get more complicated, they also introduce unwanted user friction. Moreover, they are largely offered as a black box solution, with limited opportunity for customization and a lack of visibility into the reasons that traffic is challenged.

Solution



Account takeover attacks use a multitude of methods ranging from naive methods using single IPs to using bots to advanced methods targeting specific accounts using social engineering. **The most effective account takeover mitigation product must come with out-of-the-box features to address the entire spectrum of attack methods.**

See Oscilar in action!

Get a Demo

1 Adaptive risk-based approach to account takeover prevention

An adaptive approach to risk-based authentication is required that considers factors beyond the traditional **2-factor methods of SMS, email, and authenticator applications**. User's historical behavior analysis and population pattern analysis, when combined with machine learning models trained on advanced features for detecting account takeovers allow the use of the appropriate action—be it a CAPTCHA, MFA, or simply an allow/deny outcome—based on the overall risk of an account takeover attack. Together this **constitutes an adaptive identity validation strategy**. The result is an innovative approach to user identity validation while reducing user friction.

2 Historical user behavior analysis using a central platform

User's historical behavior analysis, when performed across the entire customer journey, is key to finding anomalies in the user's activity during an account takeover. A user's historical patterns of IP address, networks, locations, devices, as well as, population pattern analysis for new users are key factors used to perform adaptive identity validation. This **requires integrating user activity data from a multitude of internal systems and applications into a central platform that holistically tracks the user's behavior** (fraudster or not).

3 Network and internal intelligence

The ability to integrate 3rd party data—obtained from a multitude of attacks—along with internal user behavior data is key to the accuracy of account takeover detection. This is because attackers typically target multiple businesses making network intelligence particularly effective. Integrating such network intelligence with internal historical user behavior data **requires utilizing an advanced data platform that can integrate data from a variety of 3rd party tools** and join that with internal data sources while enabling historical user behavior analytics on the combined dataset.

What does an effective account takeover prevention product entail?

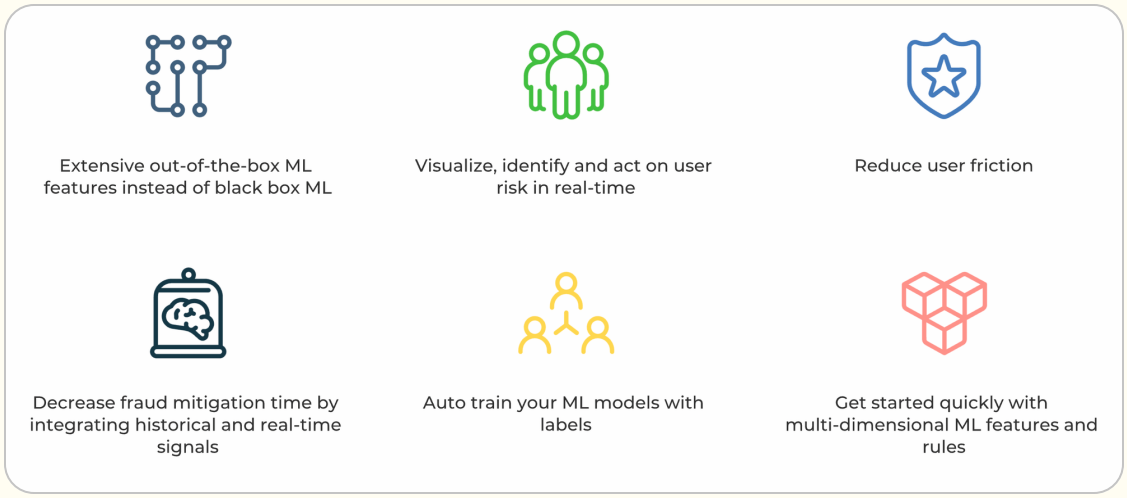


Figure 3. Effective account takeover prevention

1 Extensive out-of-the-box features and rules instead of black box machine learning models

There is precedent for what the most effective account takeover detection strategies use in the form of rules, as well as, features used for training machine learning models. Such features must address the entire spectrum of account takeover attack methods versus merely addressing bot attacks. **Rather than spend time doing manual feature engineering, an effective product must allow creating features and rules for a wide variety of account takeover scenarios based on your user authentication data**—such as authentication attempts—along with outcomes of user authentication and challenges.

Additionally, analyzing and deploying effective out-of-the-box rules that can be run in trial mode in a few clicks is a must to reduce fraud mitigation time.

2 Visualize, identify and act on user risk in real-time

How do you know someone is who they say they are? **Every user authentication attempt must return a customizable verdict in real-time**—allow, challenge, deny, or a custom action configured by you—enabling you to prevent account takeovers in real-time.

3 Reduce user friction

Don't want to subject your users to MFA for every login? State-of-the-art feature capabilities are required—such as graph features, link analysis, anomaly detection on user behavior—that let you to build accurate rules and ML models to fight fraud with minimal user friction. Following are examples of **attributes of user behavior that should be taken into account**:

- **Location anomalies**
- **Proxy IPs and VPNs**
- **Device fingerprints**
- **Botnets**
- **User behavior anomalies**

4 Get started quickly with multi-dimensional out-of-the-box features and rules

Identifying sophisticated ATO attacks requires using signals from multiple parts of the user journey besides just logins. Additionally, a large number of features are required to capture user behavior and device characteristics. Manually analyzing these high dimensional features is error prone and inefficient. **A product, powered by ML, should offer out-of-the-box functionality to easily analyze and use these features in rules and ML models**.

5 Decrease fraud mitigation time by integrating historical and real-time signals

The majority of time between account takeover activity and account recovery is spent on finding fraud patterns in historical data and applying that to the right accounts. **An effective account takeover prevention product integrates historical and real-time signals in a continuous fashion allowing computation of risk signals and flagging compromised accounts in real-time**.

6 Automatic and fast retraining of models

ATO attacks quickly adapt to existing rules and models thus the faster a product can react to the changing fraud patterns, more the ATOs can be prevented. Even though the outcomes of security challenges—like MFA—completed by users are available in realtime, typically ATO rules and ML models are rebuilt manually resulting in a delay of several weeks. **A product with online ML learning using information from challenges solved is far superior in its ability to react to new and adaptive fraud patterns**.

Detect fraud sooner than your customers

Account takeover fraud is on the rise and the effects can be far-reaching. The profits of fraud feedback into the criminal ecosystem, funding the **drug trade, human trafficking, and terrorism**. A single identity breach can open the door to thousands of fraud attacks, making it imperative for businesses to prioritize fraud prevention throughout their operations. **To deliver the best customer experience it is important to balance robust security with positive UX**.

Account takeover attacks are launched using a variety of techniques ranging from naive approaches using single IPs to using bots to employing advanced methods targeting specific accounts using social engineering. **Oscilar allows you to find anomalies across multiple dimensions and remediate fraud before your users notice**. To enable this, Oscilar comes with out-of-the-box ML features and models to address the entire spectrum of attack methods with capabilities such as no-code real-time feature engineering, self-service customizable rules engine, link analysis capability and anomaly detection on user behavior.

If you'd like to learn more about Oscilar's approach to to preventing account takeovers, drop us a note!

Get a Demo