KEYLESS

Account Takeover Fraud

The Definitive Guide

Introduction

In an age where our digital identities shape our daily interactions, a formidable challenge has arisen – account takeover fraud. Making up 33% of all global fraud cases, it is one of the most widespread cybersecurity threats organizations face today.

The techniques fraudsters use to take over accounts have become increasingly sophisticated. Bad actors have continuously adapted their tactics to circumvent the latest security standards, making detection and prevention more challenging.

In this white paper, we will delve into all aspects of account takeovers, including what the most common examples are, what fuels them, and how they can be stopped.

What is account takeover fraud and why does it matter?

An account takeover occurs when someone gains unauthorized access to someone else's account and almost always leads to further criminal behavior - or fraud. Below we have included some of the most common consequences of account takeover fraud.

- Financial losses
- Exposure of personal data
- Identity theft
- Hold data ransom
- Spread of misinformation
- Reputational damage
- Regulatory penalties

What's needed to access someone else's account?

Typically, to carry out an account takeover, a fraudster will need to be able to access or fake at least one of four things: a username and password, a mobile phone number, an email account, and biometric data. These key elements serve as entry points for cybercriminals seeking to exploit vulnerabilities and gain unauthorized access. Let's delve into each of these factors in detail.

Username and passwords
The most common way for attackers to infiltrate accounts is through stolen or leaked username and password combinations. Weak or reused passwords compound the risk, making it crucial for users to adopt strong, unique passwords for each account.

Email accounts
Email accounts play a central role in online communication and account recovery processes. Attackers who gain unauthorized access to a victim's email account can reset passwords for various accounts linked to that email address.

Mobile phone numbers
Mobile phones are often used as a second factor for authentication through methods like One-Time Passwords (OTP) sent via SMS. By gaining control of the victim's mobile number, attackers can intercept SMS-based authentication codes, effectively bypassing an extra layer of security.

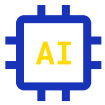
Biometric data
In cases where biometric authentication is used, such as fingerprint or facial recognition, attackers may attempt to compromise the biometric data itself. This could involve creating forged fingerprints or masks to bypass biometric sensors and gain unauthorized access to accounts protected by biometric authentication.

Three factors fuelling account takeovers

Account takeovers are no longer a new phenomenon, but there are certain catalysts that have contributed to their increasing share of the total fraud market today. We have listed the three most prevalent below..

The realm of data breaches is marked by an unsettling reality: an estimated 24 billion usernames and passwords circulate on criminal marketplaces, often on the dark web. Given that almost a third of internet users reuse the same password across 5 to 10 websites, fraudsters will buy credential sets in bulk and test them and try their luck on thousands of websites and apps in the hope of getting a match. More data breaches, more account takeovers.

Insufficient authentication protocols significantly fuel account takeover fraud. Typically weak authentication methods include passwords, OTP notifications, and email magic links. Passwords are easily guessed, stolen through phishing attacks, or obtained through data breaches. OTP notifications sent via text messages can be intercepted, while email magic links are at risk if a fraudster has gained control over a victim's email account.



Automation streamlines tasks using preset rules, while AI adapts intelligently, learning and making complex decisions. The fraudsters of today use both to launch attacks of unprecedented speed and scale. Cybercriminals leverage automation to systematically test stolen credentials taken from data breaches, while AI can be used to dynamically adapt attack strategies, such as rapid information gathering or random password generation.

How do account takeovers happen?

Phishing
Phishing involves sending fraudulent emails, messages, or communications that appear to be from legitimate sources, such as banks or trusted organizations. These messages often contain links to fake websites designed to collect sensitive information or malware. According to some estimates, over 3 billion malicious emails are sent every day.

Impersonation Scams
Phishing's sister scam, an impersonation attack involves pretending to be a person of authority, such as a company executive or a trusted service representative, to deceive victims into divulging sensitive information or performing actions against their interest. In 2022, £177.6M was lost to impersonation scams in the UK.

Man-in-the-Middle Attacks
In man-in-the-middle (MITM) attacks, attackers intercept and manipulate communications between a user and a target, effectively eavesdropping on sensitive data exchanges. A general term, MITM attacks are a common way to perform real-time phishing, where time-sensitive authentication methods such as SMSs are used.

Credential Stuffing
In credential stuffing attacks, cybercriminals capitalize on the common practice of reusing passwords across multiple accounts. Attackers obtain lists of stolen username and password combinations from previous data breaches and attempt to use those same credentials on various online platforms. Did you know that in the first 90 days of 2022 Okta reported over 10 billion credential stuffing cases?

SIM Swapping
In credential stuffing attacks, cybercriminals capitalize on the common practice of reusing passwords across multiple accounts. Attackers obtain lists of stolen username and password combinations from previous data breaches and attempt to use those same credentials on various online platforms.

How can we reduce account takeovers?

As long as there are accounts, there will be account takeovers. However, with the right strategies and security measures in place, they can be substantially mitigated. Implementing a multi-layered approach to security is key to safeguarding accounts and sensitive information. There are many effective strategies that can help prevent account takeovers, including stronger authentication mechanisms, regular security audits, real-time threat detection, device management, monitoring third-party applications, and patch management.

Among the various preventive measures, one of the most effective is implementing stronger authentication as it stops would-be fraudsters at the front door. No access, no ATOs. Below, we delve deeper into the different types of authentication, highlighting their advantages and disadvantages.

In the evolving cybersecurity landscape, the need for secure and user-friendly authentication methods has become paramount. As we discussed before, password-based systems are not longer sufficient to stop the attackers of today. This led to the creation of the category of passwordless authentication.

The five most popular passwordless authentication methods

Below, we've detailed the top five most popular passwordless authentication methods. For each, we've evaluated their security effectiveness against ATOs, user-friendliness in implementation, and, when applicable, privacy considerations. We've also outlined their common usage scenarios (consumer or workforce) and identified whether they are multi-factor solutions.

Multi-Factor Authentication (MFA) elevates security by necessitating users to authenticate using two or more of three unique factors: inherence (biometrics), possession (tokens or devices), and knowledge (passwords, PINs, or OTPs).

		Advantages	**Disadvantages**
Biometric Authentication	Biometric authentication relies on unique physical or behavioral traits like fingerprints or facial features. They are often used by both employees and customers.	Biometric authentication offers exceptionally high security due to the difficulty of replicating user data and is the only method that proves the genuine identity of the person authenticating. It also offers strong user experience as biometrics cannot be lost or forgotten.	If not properly implemented, biometric authentication can raise privacy concerns. Some forms of biometrics are also bound to the device - if lost, users must re-enroll. Others still do not offer true identity assurance.
Hardware Token Authentication	Hardware tokens are physical devices that generate unique codes. They are typically used for employees rather than in customer environments.	Hardware tokens also provide an exceptionally high level of security as they are separate from devices and immune to malware attacks.	Hardware tokens do not prove the identity of the person authenticating. They are also easily lost and relatively costly.
App-Based Authentication	App-based authentication utilizes smartphone apps for methods like QR code scanning or push notifications. They are used in both workforce and consumer environments.	The primary advantage is user convenience. Smartphones are ubiquitous and users are accustomed to interacting with apps.	The device becomes the single point of failure. If said device is lost, the account often needs to be recovered. they also do not provide true identity assurance.
Email Authentication	Email-based authentication sends users one-time login links to their registered email addresses. Most commonly these are used in customer environments for password resets.	This approach is user-friendly, eliminating the need for users to remember passwords. It is also multi-factor and already very widespread.	The security of email accounts becomes paramount. If an attacker gains access to the account, they could potentially access multiple accounts linked to that email. No identity assurance.
SMS OTP Authentication	Phone number-based authentication involves sending one-time OTPs via SMS or phone calls and is typically used in customer environments.	SMS OTPs offer strong multi-factor security as users must know their passwords and possess their physical phones to authenticate.	This method is prone to SMS vulnerabilities such as SIM swapping and man-in-the-middle attacks, and does not provide identity assurance.

Which is best?

Hardware tokens, app-based, email-based, and phone number-based authentication all present valuable alternatives, but biometric authentication emerges as a compelling choice.

Biometric authentication has several advantages over alternative methods. Chiefly, it is the only method that is able to guarantee that the person authenticating is the same person that enrolled. A simple example is with hard tokens.

Anyone with a hard token can authenticate themselves pretending to be the original person. Biometric templates also carry an advantage as they cannot be lost or forgotten and are exceptionally hard to replicate.

This said, biometrics can raise privacy concerns, and not all biometric technologies can provide true identity assurance. This is because the extent to which each technology addresses these varies greatly. Let's look further into biometric authentication technologies and their individual effectiveness against stopping account takeovers.

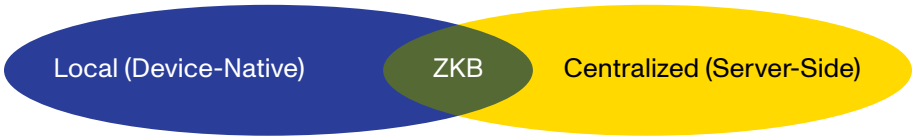
Biometrics: face or finger?

Facial biometrics offer distinct advantages over fingerprint biometrics when it comes to thwarting account takeovers. While both methods are highly secure, facial biometrics excel in usability, a crucial factor in preventing fraudulent access attempts. The ubiquity of modern devices, including phones, tablets, and laptops, equipped with built-in cameras, contrasts with the limited prevalence of built-in fingerprint sensors. Requiring only a quick glance for authentication, the simplicity of facial biometrics also encourages broader user adoption and reduces friction in the authentication process. Additionally, facial recognition can be executed from a distance, enhancing convenience and user comfort. These combined factors make facial biometrics a robust and user-friendly option for countering account takeover attempts, fostering a secure yet accessible digital environment.

Not all biometrics are created equal

Within the landscape of biometric authentication, two dominant methodologies have emerged for managing and processing biometric data: local and centralized systems. Local systems, exemplified by the likes of Apple's Face ID, operate by retaining and processing biometric information exclusively on the user's device. This localized approach ensures a heightened level of privacy, as the sensitive biometric template remains confined within the user's possession. While this local storage strategy offers robust privacy protection, it comes with the drawback of reduced usability in situations where the device is lost or stolen. Additionally, cross-device compatibility is often limited in these scenarios. A user with an Apple product will not be able to authenticate on an Android device.

On the other end of the spectrum, centralized systems take advantage of cloud-based infrastructure to store and process biometric data remotely. This cloud-centric approach offers unparalleled convenience, as users can authenticate themselves across different devices with ease - all that's required is a front-facing camera. In case of device loss, the biometric data can be conveniently retrieved from the cloud. However, this convenience comes at the cost of potentially compromised privacy. Entrusting cloud service providers with sensitive biometric information raises valid concerns regarding data security, as unauthorized access or breaches could lead to the exposure of personal and even health-related data.



Zero-Knowledge Biometrics: the future of passwordless authentication?

A new approach, Zero-Knowledge Biometrics (ZKB), aims to combine the benefits of both systems. ZKB offers the privacy of local biometrics with the convenience of centralized ones. ZKB doesn't store biometric data on devices or clouds. Instead, it transforms data before leaving the device, maintaining privacy. The transformation uses Secure Multi-Party Computation (SMPC), enabling computations on encrypted data without revealing it.

With SMPC, multiple parties can analyze data without exposing it, analogous to two millionaires comparing wealth without revealing actual values. The biometric data remains private from not only the cloud provider but the authentication solution provider as well - an industry first.

This groundbreaking innovation is the first biometric authentication solution to favor both privacy and usability, and currently stands as one of - if not the - strongest defense against account takeovers in the authentication market today. For information on how biometric MFA can help your organization stop ATOs, visit keyless.io

KEYLESS