Solution Brief

Prevent ATOs Using Mobile Identity Verification and Authentication

Ensure consumer protection and build trust across the digital engagement journey

Zumigo

Solution Brief

Prevent ATOs Using Mobile Identity Verification and Authentication

Account Takeovers (ATOs) can happen at any point during the consumer's engagement with businesses. Attackers steal credentials and identities to gain monetary benefits. By verifying and authenticating the consumer's mobile identity using real-time, authoritative data sources, Zumigo helps prevent ATOs and identity fraud with a frictionless consumer experience.

The Real Threat of ATO Attacks

The risk of account takeovers (ATO) has surged over the years and is a concern for businesses. According to LexisNexis, in 2021, almost a quarter of identity-related fraud in North America was a form of ATO.

ATOs happen when fraudsters use stolen credentials to gain unauthorized access to user accounts where they can harvest personally identifiable information (PII); steal credit card information, cash, and loyalty points; purchase goods and ship to a different address; and access subscriptions at no cost, like streaming services. Such unauthorized access can result in negative impacts to the businesses, including:

- Financial loss due to unauthorized purchases that can end up as chargebacks
- Reputation loss due to unsatisfied customer experience
- Legal and compliance consequences due to exposure of customer information
- Increase in operational costs due to investigations, remediations and prevention of future attacks

Today, the most widely used identity authentication methods such as username and password, personal identification number (PIN) code, email address, and phone number are all easily hacked and readily available for purchase on the dark web. These credentials have become a common target for attackers and can be leveraged to inflict damage in new ways. Hackers can use stolen phone numbers to initiate ATOs against consumers even when they don't have physical possession of the phones. For example, an attacker could use the account recovery process to reset passwords in order to access accounts where they couldn't before.

Conventional security measures like passwords, two-factor authentication (2FA), or knowledge-based authentication (KBA) security questions are high friction and insufficient to stop the increasingly sophisticated tactics that cybercriminals deploy to commit fraud. Many of today's security solutions do not verify whether the rightful owner is in possession of the phone number being used for security validation before authorizing access to a privileged service, which leaves a gap in cybersecurity protection.

ATO Across the Consumer Journey

Many enterprises and organizations rely on multiple channels, including mobile, web and phone, to interact with their consumers for opening new accounts, making purchases, updating account information, accessing loyalty points, streaming audio and video content, etc.

At any point in this engagement journey, the threat of consumer information being hacked, or stolen credentials being used, is a concern. The

Zumigo

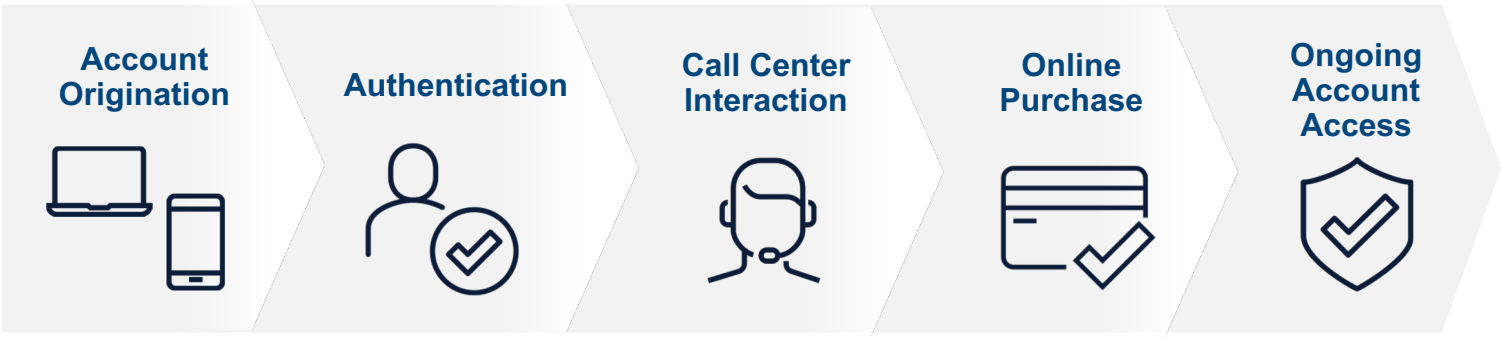

Fig 1: The Consumer Digital Engagement Journey

challenge, though, is that while protecting the consumer and the business against ATOs, the consumer experience cannot be ignored either.

Along every stage of the engagement journey, here are the ATO prevention requirements:

During **account origination**, when a new user is onboarding, the business needs to authenticate the identity to make sure the person opening the account is who they say they are. When consumers make **online purchases** or return to their accounts for **ongoing access**, their identity, payment methods, and other changes to account information should be verified to prevent unauthorized access. When an additional layer of verification is needed through the mobile phone number, phone possession and ownership have to be verified and **authenticated** to prevent fraud.

When the consumer contacts the **call center**, the caller needs to be verified that they are indeed the owner of the mobile phone that is in session with the call center, to prevent phone number spoofing and social engineering of consumer authentication.

ATO Protection Across Channels

Zumigo authenticates a consumer's mobile identity using authoritative data such as the consumer's mobile phone number, account activities, and other PII and behavioral information on file. Using real-time, definitive sources and through a layered approach, Zumigo can instantly detect fraudulent use of a consumer's identity for unauthorized account access and purchases.

Zumigo protects consumers from ATO attacks and businesses from fraud across mobile, web and call center channels.

Mobile App Channel

When a consumer accesses a mobile app for the first time, the consumer signs in with their username and password to verify account credentials. The consumer also enters their mobile phone number for Zumigo to match the mobile carrier assigned phone number and validate that it has a low risk profile.

Zumigo enables mobile number verification for devices on Wi-Fi by routing selective authentication requests over the mobile carrier's network. After verification, the SDK generates an asymmetric key pair in the secure enclave of the device. The private key is stored in the secure enclave and the public key, now associated with the verified mobile number, is shared with the server. Subsequent logins via the same device will bypass the sign-in process, resulting in a frictionless experience.

In the event of account or device changes, or if the transaction is high-value or high-risk, Zumigo can also send a SMS link for multi-factor authentication to a verified mobile number.

Web Browser Channel

A consumer can sign up for or sign into accounts via the web browser on either the laptop/tablet or smartphone. In the case of the smartphone, upon signing in with a phone number, Zumigo silently authenticates that the phone number in session

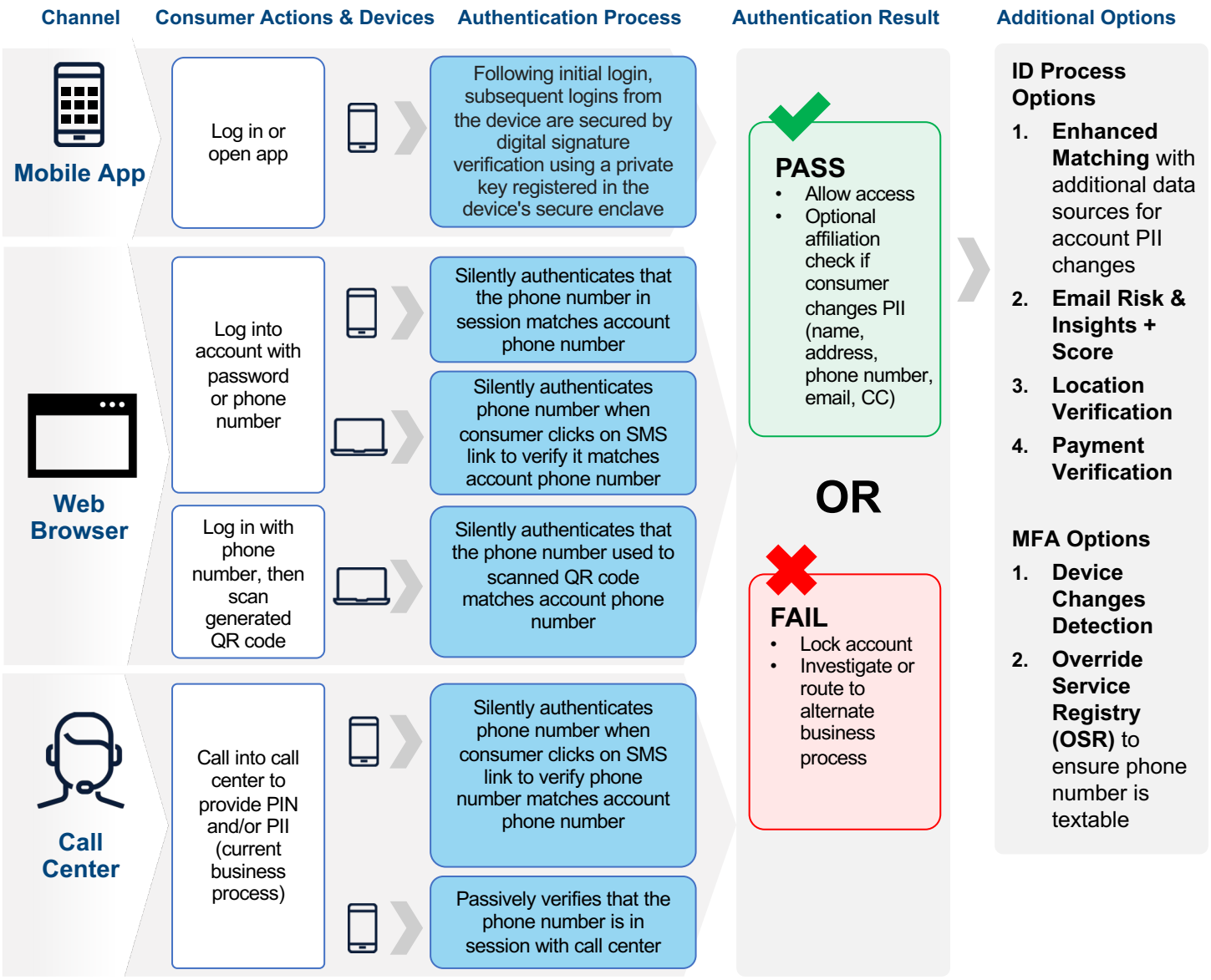

Fig 2: The Consumer Digital Engagement Journey

matches the mobile carrier assigned phone number. On the computer or tablet, Zumigo sends an SMS link or one-time passcode (OTP) to the phone number that was volunteered by the consumer. When the consumer clicks on the link, Zumigo silently verifies the phone number from the session and confirms that it matches the mobile carrier assigned phone number, or confirms the OTP that the user enters on the browser. These two methods ensure the consumer is in possession of the phone number, and that no fraudulent credentials are being used.

Zumigo can also transfer the trust of the mobile phone to the laptop or tablet as a way for the consumer to sign in without using a password. After entering the mobile phone number on the computer or tablet browser, a unique QR code is dynamically generated and displayed for the consumer to scan with their mobile phone. When scanned, Zumigo silently verifies the phone number from the mobile data session and confirms it matches the mobile carrier assigned phone number. Upon authentication, the trust of the mobile number is then transferred to the

computer/tablet for the consumer to continue accessing the account without using passwords to sign in.

Call Center Channel

Zumigo can passively verify that the display phone number being used is, indeed, in session with the enterprise care analyst, providing a frictionless experience for the consumer. Alternatively, instead of providing some form of PIN and/or PII for verification – which can be stolen and used to social engineer the consumer authentication – an SMS link is sent to the consumer's mobile phone. When clicked, Zumigo silently authenticates that the phone number matches the account phone number on file before the enterprise care analyst proceeds with the call.

Pass or Fail Next Steps

If the authentication passes, the consumer is allowed access to the account. Additional options can be added for high-risk or high-value transactions, such as whether any PII changes have taken place; email risk and validity; location verification; credit card information matches what is on file; or any device changes, such as SIM swap or port out, detected.

If the authentication does not pass, then the account is locked, pending additional business processes such as an investigation.

Zumigo Solution Prevents ATO with Minimal Friction

Zumigo Assure Authentication Solution enables seamless, secure sign-in for first-time and returning consumer sign-ins. It comprises the following products:

- ***Silent Authentication:*** Zumigo passively verifies the phone number from the mobile session and compares it to the mobile number supplied by the consumer on a mobile form. Upon authentication, Zumigo obtains details such as the name and address on file with the mobile carrier to pre-fill the mobile form, application, or checkout screen. Other information such as the mobile subscriber, mobile account, device details, etc. can be used for risk assessment.
- ***Strong Auth SDK:*** The SDK combines Silent Authentication (above) over Wi-Fi and device authentication. After a successful verification of the mobile number on the mobile app, the SDK generates an asymmetric key pair in the secure enclave, a hardware-based key manager. The public key is shared with the server and associated with the verified mobile number. The private key never leaves the secure enclave. On subsequent logins, the SDK uses the private key to digitally sign a challenge generated by the server to verify native mobile apps. The SDK has support for iOS and Android.
- ***Secure Multi-Factor Authentication:*** Zumigo provides different options to deliver one-time passcodes (OTPs) to consumers to authenticate whether the consumer has the phone in their possession, via SMS, SMS link, voice OTP (with multi-language support), and QR code. It can detect call forwarding, SIM swaps and porting scams so that the OTP is sent to the intended recipient.

Zumigo Assure Authentication Solution provides the first line of defense in preventing ATOs and identity fraud while eliminating mobile, computer and tablet authentication friction. Consumers can trust that their accounts are safe and protected, while enterprises and merchants can trust that their businesses are not impacted by fraud.

About Zumigo

Zumigo is on the frontline of digital identity verification that helps the world's largest enterprises protect transactions, devices and accounts. With a multi-layer approach, Zumigo validates users against a unique identity intelligence network that spans global carrier providers, authoritative third-party data sources, and payment information. **Learn more at www.zumigo.com**.