

# Mobile Identity and Authentication Account Takeover (ATO)

Add a layer of security to your customer authentication and prevent mobile identity fraud.



### Market Problem

Mobile phones can be exploited through multiple attack vectors, enabling bad actors to hijack phone numbers and impersonate customers. It is essential for businesses to have the proper preventative solutions in place to avoid SIM swap, SIM jacking, or porting fraud.

### Solution

ATO detection protects mobile authentication and communication for businesses and their customers. It identifies high-risk events, such as SIM swap and call forwarding enablement, by providing a yes or no indicator if these changes have occurred.

### Product Highlights

- Configurable risk window and timestamp data to span SIM swap fraud window, which typically occurs in the first 24-48 hours. ATO can allow up to a 72-hour window.
- High and low risk differentiator with API, providing yes or no response if a change has occurred.
- Levels of coverage available in 13 countries, with full coverages offered in the United States, Canada, Brazil, Netherlands, and South Africa.
- Zero-Knowledge API, only requiring yes or no change response.

### Benefits

- Reduces fraud costs that impact your business and customers
- Increases customer's trust and confidence in your brand
- Protects customers from an unknown person trying to access their data
- Provides an additional layer of security
- PSD2 compliant
- Seamless customer experience

## Account Takeover detection By the Numbers

**\$12K**

Average loss per account takeover

*Security.org*

**\$10B**

Total losses in 2022 from contact center fraud

*FBI*

**\$73B**

Reported in losses in the U.S. in 2022 from SIM Swap fraud

*Javelin Strategy & Research*

### Use Cases

#### Strong Customer Authentication

A bad actor tries to purchase an item online by impersonating a customer. The bad actor has acquired all the personal information needed to pass through the typical security and authentication measures. However, ATO identifies recent SIM changes, indicating an increased likelihood of malicious activity. Instead of allowing this transaction to occur, ATO notifies the business, who can in turn take further action to ensure the purchaser is not an imposter.

#### Protecting Data Access

Similarly, bad actors can try to access personal data, such as healthcare or financial information, through the same means. ATO identifies high-risk events early when other defense layers have been penetrated, keeping the customer's sensitive data from being exposed.

#### Open Banking Regulatory Compliance

This added protection of sensitive data is crucial and has been deemed necessary by Open Banking and Financial laws. Use ATO to comply with PSD2 and other regulations.

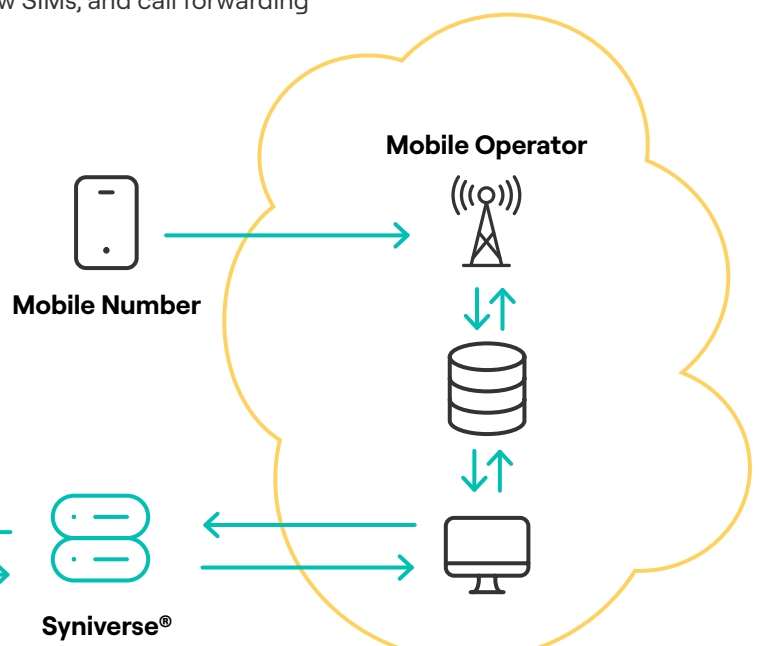
#### Conversational Commerce

While ATO adds a vital extra layer of security, it does so within a business's existing points of customer contact and does not impact the customer experience. Businesses can seamlessly integrate ATO with chatbots during customer conversations, to verify mobile identity before providing sensitive data or authorizing transactions.

### How It Works

#### Leveraging Mobile Operator & Porting Databases in Real Time

- Leverages porting & mobile network provisioning processes & databases.
- Mobile carriers need to provision porting, new SIMs, and call forwarding changes in their network.
- ATO leverages these capabilities in a standardized and privacy friendly way.
- To limit potential privacy abuse, Operators additionally use an approval process to validate end customers and use cases.



### The Syniverse Difference

Syniverse leverages authoritative data sources that are verified against government-issued identification, when possible. Syniverse is consistently trusted for our high-quality products and services because they are not only reliable but provide the highest levels of security. This is why 10 out of the top 50 Fortune 500 companies rely on us for messaging services.