



ACCOUNT TAKEOVER PROTECTION

Defend Account Integrity, Inspire Customer Loyalty

Identity-centric commerce protection reveals the 'who' behind account activity

From expedited checkout to special offers and rewards, customer accounts are a major driver of loyalty and retention. In fact, the benefits of account creation are so compelling that the average consumer has over 150 online accounts in their name.

Of course, very few consumers are actively using 150 accounts – the majority of these accounts have been abandoned or long forgotten. Given the 65% of consumers who recycle passwords across multiple accounts, this widespread consumer data has created the perfect storm for Account Takeover (ATO) fraud.

By leveraging automated bots and stolen credentials, fraudsters can easily launch large scale ATO attacks across thousands of merchants – matching credentials with accounts and accessing stored financial information to either make fraudulent purchases or continue scheming efforts across additional merchants.

And because many of the attributes of an ATO transaction appear to be from the cardholder themselves, it is incredibly difficult to detect. Without insight into who's behind account-driven activity, there's little you can do to stop from rolling out the red carpet for customers and fraudsters alike.

79%

Increase in ATO

\$16B

Annual cost of ATO

22%

Consumers who have been the victim of ATO fraud

Solution Overview

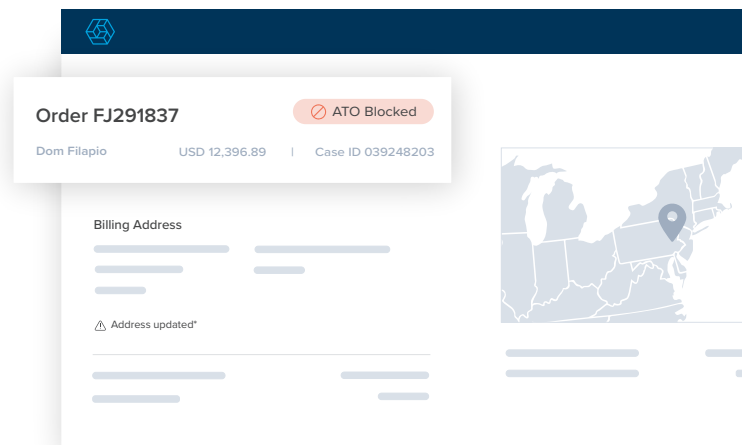
Signifyd's ATO Protection product monitors consumer behavior across the Commerce Network to build a constantly evolving profile of each shopper. These insights can be leveraged by merchants to deploy custom ATO protection at login while also allowing Signifyd to accurately detect anomalies in purchasing behavior and stop fraudulent orders as a result of ATO at checkout.

¹ [Dashlane](#)

² [South Florida Reporter](#)

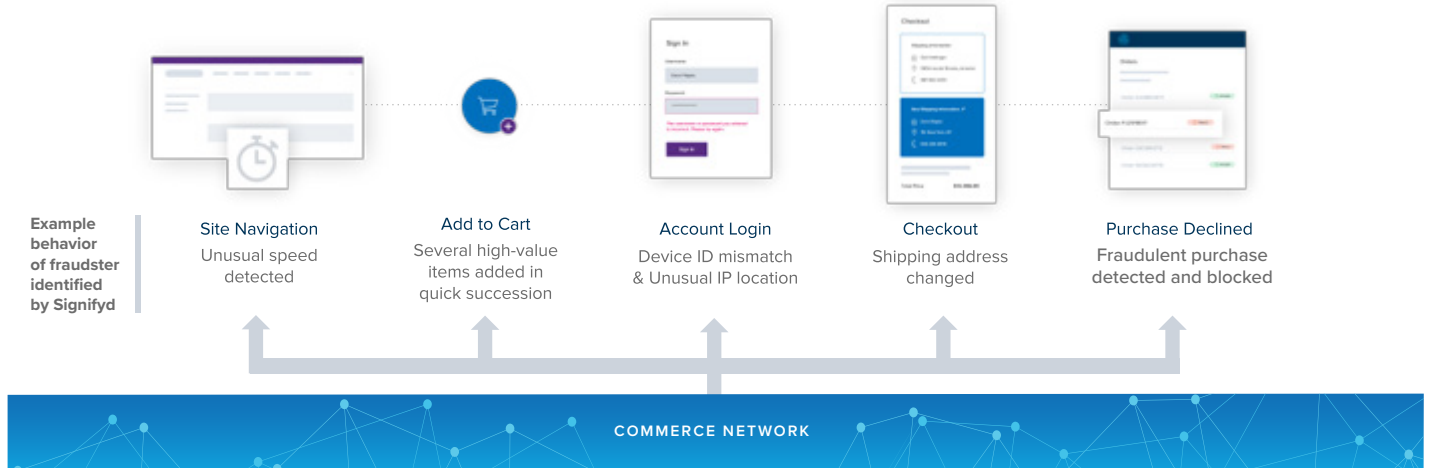
³ Signifyd internal data

⁴ [Security.org](#)



How it works:

Merchants customize protection at login while fraudulent orders are blocked at checkout



It starts with the world's largest **Commerce Network**. Signifyd monitors ATO trends across our network to safeguard merchants from emerging attacks.

Network insights are combined with behavior and device data to identify suspicious account activity. Signifyd compares this data to the account holder's digital footprint across the network to detect anomalies.

Merchants customize protection at login. Configurable ATO policies give merchants full control over how and when friction is introduced at a critical juncture in the shopper's journey.

Fraudulent orders are blocked instantly. By analyzing how a transaction moves from login to checkout, Signifyd can accurately distinguish a fraudster and the true account holder, blocking the transaction before the purchase can be completed.

Features & Capabilities

- Login policy creation, testing, and monitoring in Decision Center
- Best-practice login policy templates combined with expert guidance from Signifyd's risk intelligence team
- Automated login workflows such as accept, reject or challenge
- 2FA / Multi-Factor Authentication integrations

Key Benefits



Defend Brand Integrity

Block suspicious login attempts to mitigate brand-damaging account takeovers.



Reduce Friction At Login

Recognize good customers instantly and get them to checkout faster with a streamlined login experience.



Eliminate ATO losses

With every approved checkout transaction backed by a 100% financial guarantee, you'll never pay another ATO chargeback again.

“

“Fraudsters know you are looking for specific behaviors and what they do is increasingly resemble legitimate clients. If you only know what a shopper does within your business you are missing a part of the movie. And to see the full movie, machine learning tools and agile providers like Signifyd constantly monitoring this data is key.”

— CARLOS MADRONA, MANAGING PAYMENTS METHOD AND FRAUD DIRECTOR, MANGO

GET IN TOUCH visit us at signifyd.com/contact