Account Takeover Protection

Identify suspicious account behavior and help keep your customer accounts secure.
What is Account Takeover Protection?

Account takeover occurs when a fraudster obtains a victim’s personal information and then changes login credentials or passwords. The fraudster then takes control of the victim’s account or sets up a new account and carries out unauthorized transactions.

CyberSource Account Takeover Protection defends consumers and businesses from fraudulent uses of online accounts. It helps identify high risk users at account creation and login, and also monitors for suspicious account changes.

KEY STATS

$800M of estimated loss by account takeover by the end of 2016

55% of consumers use the same credentials across all of their online accounts

$3 is the value of a single compromised account on the underground market

SOURCES
1 www.bankinfosecurity.com/interviews/conroy-i-2050
2 www.darkreading.com/endpoint/anatomy-of-an-account-takeover-attack/a/d-id/1324409
Account Takeover Protection Benefits

Protect online accounts from unauthorized access

Avert fraud attempts before they take place

Preserve customer trust and loyalty
How Account Takeover Protection Works

1. Access the CyberSource Business Center interface to easily configure your rules.

2. Create one or more profiles — groups of rules — for Account Creation, Account Login, or Account Update events.

3. Build rules for each profile, on hundreds of data elements around the device and user behavior.

4. Incorporate velocities around items in these rules.

5. Based on rule output, decide whether to accept, monitor, challenge or reject the user action.

6. Be supported on web and mobile devices, with SDKs for iOS and Android implementation in mobile apps.
Protect Customer Accounts

Cybercriminals are using increasingly sophisticated methods to obtain account access.

Unauthorized transactions undermine trust and loyalty among valued customers.

With **Account Takeover Protection**, you can help keep your customer accounts safe and protect against fraudulent card-on-file payments, while streamlining access for authenticated customers.
Why CyberSource?

Leverage the World’s Largest Fraud Detection Radar based on insights from over 68 Billion transactions processed by Visa and CyberSource, annually.

In 2015 we had 475,000 customers and managed 223 billion payments, which translates into approximately 1 out of every $10 spent online, worldwide.

The most connections to acquiring/issuing banks, worldwide, to monitor compromised account activity. 100+ global processor and acquirer connections.

Patented Real-Time Fusion Modeling enhance detection accuracy and enable fast, confident strategy adjustments.

Local dedicated risk teams that monitor trends and guide fraud management strategy located in Miami, Mexico City and Sao Paulo.