Account Takeover Protection

Keep your customer accounts safe – and protect against the fraudulent use of card-on-file payments.

Identify fraud at account creation and login – and monitor for suspicious account changes.

Account takeover fraud is on the rise

Account takeover fraud occurs when a cybercriminal exploits a victim's personal information stored with a merchant in order to take control of an existing account – or establish a new account – and goes on to use that account to carry out unauthorised transactions.

Merchants are popular targets because it is perceived that their security protocols are far less strict than, for example, a bank's.

Cybercriminals are using increasingly sophisticated methods to obtain access to accounts, including malware, SQL injection attacks, spyware, Trojans, and worms.

Account takeover attacks lead to fraudulent payments to merchants. They may also have far-reaching consequences on victims, ultimately undermining trust and loyalty among valued customers.

Storing card and account on file can lift checkout completion by up to 50%.[1]

[1] Business Insider Intelligence 2016

CyberSource®
A Visa Solution

Account Takeover Protection

The benefits

1. Protect online accounts from unauthorised access

Account Takeover Protection protects consumers and merchants from the fraudulent use of online accounts, while enabling merchants to streamline their site access for authenticated consumers.

Account Takeover Protection actively monitors new account creation and account usage behaviours of online websites helping businesses identify valid from high-risk sessions with more accuracy.

2. Avert fraud attempts – before they take place

Account takeover leads to fraudulent transactions. By identifying fraud before the purchase occurs, you can avoid the costs and risks associated with chargebacks.

A flexible rules engine enables you to flag suspicious activity based on customer behaviour and device attributes. You then decide whether you want to accept, reject, or challenge the users to authenticate themselves – before the event can occur.

3. Preserve customer trust and loyalty

Account Takeover Protection keeps customer accounts safe from fraudsters – and protects your brand by providing a secure account and purchase ecosystem.

Real-time decisions mean that account creation, login and changes will be seamless and safe. You can also identify valuable returning customers in order to ensure they enjoy a frictionless user experience.

Protect customer accounts

To help you distinguish valid from high-risk sessions more accurately during account creation, login and updates, Account Takeover Protection actively monitors new account creation and account usage behaviours of online accounts. As an extension of Decision Manager, Account Takeover Protection inter-operates with the reporting, rules and tuning tools to provide you with a fully integrated fraud management platform.

26% of data breaches were related to eCommerce.[2]

63% of these breaches involve the theft of payment data.[2]

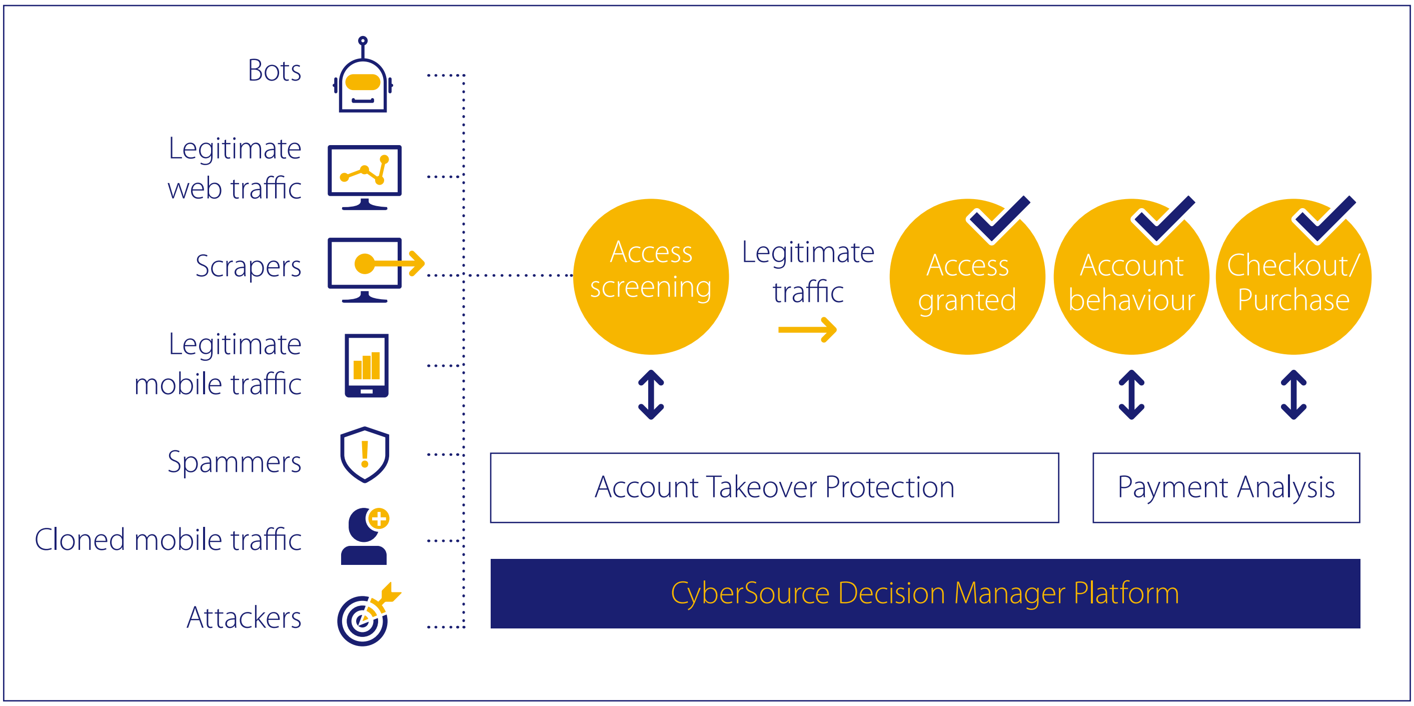
[2] Trustwave 2017 Security Report

Account Takeover Protection – how it works

Account Takeover Protection allows you to build rules to screen customer account events – such as account login or creation – on your website or mobile app. It allows you to:

- Access the CyberSource Business Center interface to easily configure your rules.
- Create one or more profiles – groups of rules – for Account Creation, Account Login, or Account Update events, such as password changes.
- Build rules for each profile, based on hundreds of data elements around the device and user behaviour. These could flag anomalies about the machines accessing your systems, such as jailbroken devices or suspicious proxy IP activities. CyberSource can access cross-merchant device data, providing insight into past device usage.
- Incorporate velocities around items in these rules, such as number of times a device is used in conjunction with username, password, name, billing address, phone number, and credit card information.
- Decide whether to accept, monitor, challenge or reject the user action – based on rule output. For instance, events originating from new devices for existing customers could be challenged, requiring users to verify their identities before they are allowed to create, access, or change data in their accounts.

Supported on web and mobile devices, with SDKs for iOS and Android implementation in mobile apps.



Why CyberSource?

- Our platform is built on a secure Visa infrastructure with the benefits and insights of a $427 billion global processing network.
- We offer payment acceptance in 190+ countries – and accept 137 currencies.
- We have 100 acquirer processor connections. This is increasing by 20+ each year.

In 2017 we:

- Managed 277 billion payments
- Managed approximately 1 out of every $10 spent online, worldwide
- Served 456,313 customers worldwide
- Provided x200 the visibility into fraud patterns[3]

[3] Based on the average number of transactions for a top merchant

Find out more about our Multi-Phased Fraud Management Platform at **www.cybersource.co.uk/strengthenyournumbers**

Contact us

Email. europe@cybersource.com www.cybersource.co.uk

CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast $427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues and mitigating risk. For acquirer partners, CyberSource provides a technology platform, payments expertise and support services that help them grow and manage their merchant portfolio to fulfil their brand promise. For more information, please visit cybersource.com.

CyberSource®
A Visa Solution