simility

TECH BRIEF

Stop Costly Chargebacks While Protecting the Brand by Mitigating Account Takeover Risk

The 2017 Identity Fraud Study conducted by Javelin Strategy & Research reported that the account takeover (ATO) incidence rate increased by 31% in 2016 from the previous year. This contributed to 61% increase in ATO losses totaling $2.3 billion, resulting in more than 20 million hours dedicated to resolving ATO fraud instances.

Overview

Data breaches are widespread. Even a single data breach from one site can be threatening, as many people (despite best cybersecurity practices) use one username and password for multiple logins. Cyber criminals are not only resorting to stolen data to gain control of legitimate users' accounts, but are also efficiently using malware and phishing to acquire personal identifying information.

Some of the world's biggest known data breaches—at Equifax, Adobe Systems, JPMorgan Chase, Yahoo, Fitbit, and Target—have affected tens of millions of users, exposing companies to subsequent cyber crimes such as ATOs and incurring further fraud losses. Financial services are among a larger set of online business groups that face increased threats from account takeovers.

How Account Takeovers Work

Thieves do their homework, perusing breached data and social media for clues about account holders' email addresses and other information. Then they attempt password cracking through bot networks, malware, spear phishing, or social engineering to access and effectively take over those lucrative accounts. Once equipped with an account number, a first name, and other basic information, fraudsters may even convince a call-center customer service representative to update and alter the primary contact channels for a given account.

Having compromised an account, fraudsters can take remote control and misuse the account in several ways: for example, by making unsolicited purchases, signing up for new credit cards and maxing them out, or making fraudulent transfers. Such actions saddle businesses with chargebacks, reputation loss, and diminished customer loyalty.

Most account takeovers go unnoticed as hackers use legitimate credentials to authenticate successfully, making account takeover fraud a challenge to detect. With its multi-layered fraud detection solution, Simility helps businesses identify suspicious logins and detects account access from hackers and botnets. Simility's solution offers real-time responses while avoiding additional authentication steps for legitimate customers.

How Simility Detects Account Takeover Fraud

By using proprietary rules and machine-learning algorithms to build profiles for normal user login and checkout behavior, Simility compares every login attempt and existing behavior profile with device fingerprints to detect anomalies and compute a fraud score. Using Simility's intuitive workbench, analysts are empowered to perform sophisticated link analysis to find related accounts and events, enabling them to take action upon entire networks. Further, manual actions taken by the analysts improve the core machine-learning models, activating additional components of fraud detection to continuously protect the business while reducing customer friction. This brings account takeover fraud detection to a whole new level.

Simility's account takeover features and technologies include the following:

Advanced Device Fingerprinting Technology: Simility's solution analyzes hundreds of characteristics and behaviors of each mobile, desktop, or laptop device, including browser settings, language, location, operating system, battery level, and even mobile emulation. Fraudsters can mask identifying properties like name, email address, or even Social Security number (SSN), but Simility's advanced device fingerprinting shows whether a device used to access an account is associated with fraud. In a different scenario, the device fingerprint can also help by showing whether the same device is being used to login a large number of user IDs. Also, the past history of violations associated with a device fingerprint can be brought to bear in stopping actors from logging in. By measuring a customer's unique interaction with each device, such as mouse movements, clicks, touches, swipe speed and more, Simility helps businesses to detect whether a device is associated with bots or remote administration tools.

Behavioral Intelligence: Simility effectively analyzes each user's behavioral information: what the user clicks and how he or she acts during the session and login information. Simility also considers the typical navigation and time patterns, along with other behavioral aspects. This builds a profile of normal behavior, allowing any abnormal or suspicious activity to stand out. All of these behavioral patterns can help protect consumer assets and effectively halt fraudulent activity without impacting the day-to-day activity of legitimate customers.

Session Analysis: Simility analyzes click-by-click data of every sign-up request, providing deep insight regarding the entire HTTP request through quantifiable parameters like the amount of time it takes an individual to log into an account, on-screen mouse behavior, the language used on a computer/tablet/phone, and how an individual types. Any observed anomalies in the behavior get flagged for the analyst to review. Simility computes scores for time spent on a page, time between pages, mouse movement, and keyboard patterns that show how legitimate users truly act. This helps to determine if a user's behavior is genuine or from a bot attack. Continuous session anomaly detection provides continuous assessment of the session risk, based on the analysis of behavior, device and environment, biometric data, and more. This significantly empowers internal transaction monitoring systems, providing means for early detection and automation and increasing detection rate. Risky transactions can be given high priority and followed up with a manual review, while legitimate ones can be processed automatically without any delays.

Optimized Risk Scoring: Simility scores each user upon login to the system based on various device parameters like device type, browser, screen size, screen resolution, time of day, IP address, geographical location, and session activity (such as statement downloads, email and password changes, or account added.) Additionally, Simility analyzes and scores the cross-channel behavior of a transaction to measure its riskiness. This makes it possible to dynamically assess the user's risk level and lets fraud analysts take further steps on a customizable decision template to block access, send for manual review, step up verification, or force password reset.

Conclusion

With integrated device, session, and behavioral intelligence, Simility provides multi-layered enterprise-grade protection from ATOs in a single solution today, and builds the foundation for omnichannel protection in the future. As a result, every transaction is assessed against enhanced, enriched profiles to quickly and easily distinguish between legitimate customer behavior and the unusual patterns that are the hallmark of both human fraudsters and computer malware.

Deploying Simility also gives you the essential foundation to move to a omnichannel fraud prevention solution over time. The aim is to possess a single view of each customer across all accounts, all channels, and all activity for profiling and analysis. By implementing a solution that provides this broad but detailed portrait of your customers, you can also protect your business against heavy chargebacks and expensive brand damage resulting from ATOs.

Key Features of Simility

- 360-degree view of each login with session, device, and behavioral biometrics
- Anomaly detection using proprietary rules and machine-learning algorithms
- Cross-channel Intelligence integration capabilities
- Risk-based scoring and customized decision- making for accelerated investigation and closure
- Easy rule editor to configure, test, and deploy new fraud schemes as and when required without the need to code

Key Benefits for Your Business

- Determine identities with confidence
- Increased scrutiny for suspicious login attempts while reducing friction for legitimate users
- Enhanced protection with cross-channel intelligence
- Eliminate chargebacks with trusted transactions

simility

About Us: Simility transforms fraud prevention with a versatile platform that combines the best of human analysis and machine learning. To learn more, please visit Simility.com

CONTACT US FOR A DEMO

Simility.com/demo