simility

TECH BRIEF

New Account Fraud - Know the True Identity of Your Users

According to statistics from Javelin Strategy & Research, account origination fraud remains one of the fastest-growing threats today for organizations ranging from banks to government entities. Total loss from this type of fraud rose by 50% to $3 billion in 2015 as compared to the previous year, doubling the number of victims—and the damage continues to grow.

Overview

The success of an online business depends on the growth in the number of new accounts registered. However, fake accounts created using stolen and fictitious information creates havoc by skewing subscriber data and forcing additional authentication procedures for legitimate customers--causing user friction and impacting the bottom line. Fake accounts can be created by spam botnets, scam artists, or manually by cybercriminals. Without an advanced tool, it is impossible to prove with absolute certainty who the user is. This makes account origination fraud one of the most challenging types of fraud—significantly impacting banks and online businesses.

How Simility Detects New Account Fraud

Simility provides powerful technologies that validate the identity of account applicants in near real-time. By producing accurate and holistic information about each applicant, Simility provides online businesses with the comprehensive data necessary to efficiently respond to the challenge of account origination fraud. Simility's multipronged fraud defense technology, encompassing device fingerprinting, web-session analysis, and third-party multi-factor authentication, can protect organizations from fake accounts.

Device Recon: Fraudsters constantly invent new ways to hide their identities, going to great lengths to appear as if they are legitimate users. Simility's superior Device Recon technology makes it extremely difficult for fraudsters to succeed. It begins by using device fingerprinting to flag when an identity can be traced to a known toxic device. Additionally, Device Recon uses machine learning to calculate a "fraud probability score" based on hundreds of device parameters and then predicts the likelihood of a fraudster's identity being tied to a device.

Session Analysis: Simility provides enriched click-by-click data of a new login request, providing deep insight regarding the entire HTTP request. 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.

Multi-Factor Third-Party Identity Authentication: Simility uses a third-party authentication system to validate all user-provided information. This can involve verifying email or residential addresses, phone numbers, payment details, Social Security numbers, or social-media information against available real-world identities.

The result is a series of data and history of any new user to reveal fraudulent and unethical practices. Simility compiles more than 400 points across various entities to identify threats in near real-time, giving an additional layer of security to online businesses and banks.

In addition to highly targeted alerts, Simility provides superior features to further enhance an investigator's ability to quickly and accurately discover and act on fake or fraudulent account registrations. Several, considerations are analyzed in tandem with a user's other online activity:

- **Was the new account mobile or online?**
- **Did the user register with an auto-generated or gibberish address like asdfjkasdf@gmail.com?**
- **Does the email domain or IP belong to risky subnet?**
- **Are multiple users doing signup from the same device?**
- **Are multiple signups associated to one session?**
- **Do login IPs trace to disparate geographies from the suggested address location?**
- **Are high number of transfers coming from the same device or IP?**
- **Is the time between signup and transfer very low?**

Answering these questions helps to generate a highly targeted alert that investigators consider required viewing.

Conclusion

Superior fraud detection technology from Simility can alert fraud investigators about accounts created using fake or stolen identities while removing the legwork needed to move forward quickly. With Simility, online businesses can consider keeping the door wide open for welcoming new users to their sites, while still protecting their good customers—and revenues.

Key Features of Simility

- Real-time matching of user-provided information to verify name, address, phone, payment, and email information
- Device identification with risk scores
- Online and behavioral information for identity verification
- Real-time location information
- Third-party data to approve authentic sign-ups, while flagging risky new sign-ups
- Easy rule editor for testing new rule

Key Benefits for your Business

- Reduced fraudulent account registration with fake or stolen identities
- Lowered cost of fraud, customer service, and fraud investigation
- Improved customer experience with minimal authentication steps
- Confident and improved decision making

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