Customers increasingly use digital channels to easily access their accounts for shopping, banking, and more. Storing personal and payment information in online accounts has not only made transacting more convenient for customers, but it has also made these accounts an attractive target for fraudsters.

**GROWING FRAUD**

Waves of new data breaches continue to supply the dark web with an abundance of sensitive customer information. Using legitimate login credentials purchased on the dark web or obtained through social engineering, spoofing techniques, malware, and botnets, fraudsters gain unauthorized access to customer accounts in order to misuse or mine them for information. Upon gaining access to a user’s account, fraudsters can steal contact and payment information, transfer funds, make purchases, alter user information, and more.

**THE DILEMMA**

Account takeover attacks can have detrimental consequences for businesses, including damage to brand reputation, lower customer lifetime value, and loss of customer trust. Yet, account takeover continues to present challenges for many businesses because it involves the use of legitimate customer credentials, which makes it less likely to raise immediate suspicions.

Customers look to businesses to protect their accounts and safeguard their information. Thus, it is critical for businesses to be able to accurately differentiate between trusted customers and fraudsters in real time to prevent and stop account takeover before it leads to more serious consequences for both the business and customer.

At the same time, today’s digital users are accustomed to seamless online experiences. Businesses need to consider the customer experience along with their fraud and risk strategy, as fraud detection that comes with increased friction can lead to more incomplete transactions and lost revenue.

**THE NEED FOR REAL-TIME CONTEXTUALIZED AUTHENTICATION**

To effectively tackle account takeover fraud, businesses need to make better use of data in order to gain a holistic view of the end user behind a login attempt. Fraud prevention solutions based on data lake technology can provide businesses with the flexibility to combine various data sources and easily incorporate new data feeds as they emerge. Data analytics and machine learning capabilities can then help businesses effectively manage and make sense of data to automatically detect and block account takeover attempts in real time.

**SIMILITY ADVANTAGE**

Simility’s industry recognized Adaptive Decisioning Platform is an end-to-end fraud prevention and risk management platform built with a data-first approach to provide a 360-degree view of the end user, helping to protect the customer journey. The powerful platform combines data from multiple sources, enriches that data, and then leverages best-in-class machine learning and
Simility, a PayPal service, offers real-time risk and fraud decisioning solutions to protect global businesses. Simility’s offerings are underpinned by the Adaptive Decisioning Platform built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence and big-data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems. Built by industry veterans, Simility is trusted by some of the world’s leading consumer brands across financial services, payment processors and commerce merchants. For more information on Simility, visit Simility.com

ABOUT SIMILITY

Simility helps a large marketplace reduce friction and costs by providing device data for 99% of login traffic, thereby reducing the need for step-up authentication by 25%*

*Results are specific to this marketplace. Other results may vary by industry, customer, and use case.

SCHEDULE A DEMO SIMILITUDE.COM/DEMO

COPYRIGHT © SIMILITY 2019. All Rights Reserved.

analytics to continually detect anomalous patterns and generate actionable insights. The platform is a flexible, intuitive, and visually configurable solution that can be deployed in 12-16 weeks. Some of the key features that help businesses fight account takeover include:

Extensive Data and Intelligence
Simility’s purpose-built data lake can combine structured and unstructured data, transform and enrich that data, and generate insights. Hybrid data management provides greater agility, and dynamic ontology helps provide accurate insights to build smarter rules.

Big Data Enabled Machine Learning
Quickly adapt to changing fraud attacks by easily adding, modifying, and optimizing rules, and know the statistical impact of changes before adopting them. Simility’s state-of-the-art machine learning engine adapts, strengthens, and quickly reacts to help detect new fraud schemes.

Effective Decision Orchestration
Organizations require strong, but frictionless authentication in order to strike a balance between delivering a streamlined customer experience and minimizing fraud. Simility enables organizations to determine strategies based on inputs, such as manual rules, model scores, and derived features, to create an optimized decisioning process tuned to their specific business goals.

Robust Link Analysis and Visualization
Simility reduces complexity through a unified, single analytics view. Custom workflows can be created and deployed in minutes. Sophisticated data visualization with slicing-and-dicing features helps identify patterns and relationships while screening for fraud. By utilizing Simility’s graphics database and Device Recon capabilities, businesses can visualize the relationships of their customers and the devices they use. This enables businesses to approach fraud dynamically, treating good customers with a streamlined experience and adding layers of protection when necessary.

99%