NuData Security

mastercard

User Validation for New Accounts

Establishing trust from the beginning of the relationship - and continuously - to detect and prevent fraud

Overview

In any relationship, the word "trust" is a promise, an assurance that a relationship is strong and reliable. To a consumer, trust means that they will receive the goods or services they've purchased, in the time frame and of the quality that the seller has promised.

Trust has also become a singularly important word to merchants, financial institutions, e- and mCommerce vendors, and others transacting digitally.

The mass-scale move to online and mobile transactions over the last decade – as wonderfully convenient as it has been – has given rise to today's mega-breaches and personally identifiable information (PII) thefts. For merchants and financial institutions, digital identity trust is the promise that a consumer making a transaction is actually who they say they are, and not a thief or bot using stolen credentials to attempt fraud. In effect, trust has become the primary currency of the digital economy, and establishing the consumer's trusted digital identity is now the main goal for merchants and financial institutions (and if it isn't, it should be.)

Online Fraud Hits Historic Levels

35% of new accounts in 2017 were fake accounts created with stolen identities.

Mega-breaches and mass-scale PII leaks are facts of life, with consumers' personal data readily available on the dark web. The global threat environment is constantly evolving, and fraudsters' exploits are increasingly sophisticated. Every back-to-school or holiday shopping season sees the rise of both new threats and newly-honed, more damaging sophisticated ones.

These levels of fraud are set to keep growing. According to Identity Theft Resource Center*, 2017 broke a new record with 1,579 data breaches, exposing 179 million personal records. That's 340 records per minute. According to NuData analysis, 35% of new accounts in 2017 were fake accounts created with stolen identities.

Stolen PII and static passwords equip bad actors to successfully open new accounts, initiate applications for loans and credit cards, and conduct a broad range of online fraud, making user verification for new accounts imperative.

The company's challenge is how to identify if a new user is indeed a legitimate user, a fraudster, or a bot developed by a fraudster. Fraudulent account creation is a tool that bad actors use to monetize previously purchased identities from the black market. They either

create accounts manually or use automated malware that creates them. Then, for instance, they buy stolen credit card numbers and cycle them through to finalize purchases.

To make matters worse, bad actors use the low seasons to create the bulk of their fake accounts and then wait until the busier seasons to use them. High-traffic seasons are the perfect hiding place for bad actors since suspicious behavior is sometimes missed among the crowd.

The trust-as-currency movement is the inevitable response to the continual waves of compromised static data such as passwords, Social Security numbers or credit card data, and the resulting growth in online fraud.

The question that has emerged is: how to determine if a new user is actually the legitimate user?

Deeper Insight, Better Decisions

NuData Security's award-winning NuDetect can verify with extraordinarily high accuracy whether a new user is behaving suspiciously, anonymously or as the legitimate user would. NuDetect assesses hundreds of behavioral signals that together indicate a fraudulent or legitimate user profile, using machine learning.

New user behaviors are then shared to the cloud consortium of trusted intelligence, which processes over 500 billion behavioral events per year across its network. Through machine learning, NuDetect references the applicant's data to determine if their behavior is similar to other humans' in the same situation. NuDetect also spots and evaluates the subtle device interaction nuances that only humans can make, and that automated fraud attempts can't reproduce.

This real-time insight enables financial institutions, e- and mCommerce sites, and others offering online services to reduce or eliminate ambiguity in determining the legitimacy of good users in real time. By stepping up challenges during the onboarding process, or whenever circumstances call for a closer inspection, all legitimate parties in the transaction process are protected. This benefits good users who normally help shoulder the costs of fraud, mitigates the risks of account takeovers, and reduces the inconveniences of awkward and outmoded authentications.

NuData's insight lets merchants and financial institutions stop fraud before it begins, and enhances the good customer's experience and loyalty to the brand.

Case Study

A NuDetect customer, an international digital goods company, discovered an exploit in the first week of deployment that had already cost them more than $100,000. NuDetect demonstrated an 85-99% capture rate with less than 0.5% false positives for new account applicants.

*https://www.idtheftcenter.org/2017-data-breaches

NuData Security

mastercard