NuData Security

mastercard.

Seamless Authentication

Identifying customers online without friction

Market Pain

Data breaches around the world have exposed an ocean of personal data. The series of U.S. breaches discovered in 2017 in the US, such as Yahoo, Target, Government Office of Personnel Management (OPM), Verizon, Anthem, and others, affect more than half of U.S. adults. In fact, 2017 had the highest number of breaches since 2005, according to the Identity Theft Resource Center, with 1,579 breaches exposing nearly 179 million personal records.

These breaches have exposed sensitive of information that includes Social Security numbers, names, addresses, contact information, motor vehicle information, passwords, credentials, tax information, and more. For most organizations, this breaks any authentication framework they may have in place. All identifiable information is no longer an accurate identifier, and a whole new approach is needed to identify and verify their customers online.

There were 1,579 breaches in 2017, exposing nearly 179 million personal records.

The consumer environment is also impacted by the rapid adoption of smart TVs, cord-cutters moving to IPTV, Android TV (NVIDIA SHIELD TV), smart thermostats, and the evolution of the connected home; more and more devices can be controlled remotely and even through voice, opening new gaps for fraud. These behavior changes are forcing the move away from the standard user ID and password combination that people are familiar with. While passwords and accounts continue to be the favorite target for cybercriminals, the security industry at large still hasn't a suitable replacement for the standard username and password authentication scheme.

For companies who want to strengthen security, their go-to solution is to step up verification adding friction to clients with challenging requests ("Re-scan your retina," "Name your married sibling's best man," "Name your favorite mathematics professor") in order to authenticate their identity. The consumer's response to this complex verification process has often been abandonment. Clients go back to the environments where they had a good experience. In the U.S. online retail industry, for instance, 41.6% of cart abandonment occurs at the payment stage*. Companies need a solution that can recognize good customers so they can safely remove friction.

Next Generation Authentication

Emerging technologies such as physical and passive biometrics combined with behavioral analytics are now taking center stage and picking up in adoption. Physical biometrics technologies measure personal physiological characteristics for unique identification and security. Physiological characteristics used for biometrics include face, fingerprints, and even

DNA. Physical biometrics can, and should, be combined with behavioral biometrics in a multi-layered approach for when risk is presented.

The real power is when these invisible layers, passive biometrics (such as voice recognition) and behavioral analytics (such as typing speed or device angle), are combined to identify your customer without adding any friction. Through them, online businesses can safely verify the correct human behind the device without requiring any personally identifiable information. This means that companies can safely reduce friction for those good customers and improve their experience.

While fraudsters can use stolen passwords and credentials, they are not able to mimic individual behaviors, biometrics or habits. The use of passive behavioral biometrics also addresses many of the existing gaps in the mobile user authentication process that make exploits much easier to spot. This is true when the device is being impersonated or has malware, or when the data is farmed via intercepted SMS messages and later used for identity crimes.

Passive biometrics and behavioral analytics are a unique way to not only identify the actual customer but to allow customers to do business quickly and easily.

How NuData Helps Companies Identify True Customers

It's all about trust. The next generation of authentication platform has to recognize customers by their behavior instead of relying on their credentials. NuData's flagship product, NuDetect, allows companies to identify their good users by their behavior. While fraudsters can steal and use personal identifiers, they are not able to simulate human behaviors.

NuDetect's real-time biometrics analysis continuously informs clients of fraud risk and gives them choices about what actions to take even before any account damage. This solution identifies machines from humans, then separates good machines from bad, selects known humans from unknown humans, and finally sorts unknown humans demonstrating low-risk signals from those with high-risk signals.

This technology allows companies to reduce friction on their good consumers and to give them an excellent experience while increasing friction only on those users who represent risk (see case study below). This new level of trust on consumers has allowed companies increase conversions, provide better customer experience, and save on fraud-operational costs.

Case Study

One NuData client, a large U.S. bank is leveraging NuDetect to recognize their good returning users seamlessly. Thanks to NuDetect, this bank is now able to offer:

- Eight million seamless user experiences a day without added friction.
- Enhanced security steps interjecting high-risk profiles only – less than 0.00001% of users.

*http://www.businessinsider.com/e-commerce-shoppers-abandon-carts-at-payment-stage-2016-3

NuData Security

mastercard