BIOCATCH
Less Friction. Less Fraud.

Dramatic Reduction in New Account Fraud

Case Study

One of the major retailers in Latin America experienced a surge in online fraud and review costs. Here is how they changed the game.

The rapid migration of the payments industry to chip-and-PIN has forced criminals to change their strategy and focus on new account or online credit card fraud. At the same time, the efficiency of many of the traditional fraud detection tools has deteriorated over the years as fraudsters wised up to these controls. The result: new account fraud is skyrocketing.

The Latin American online retailer in our case study acknowledged the fact that traditional solutions were just not enough, and turned to behavioral biometrics. BioCatch was able to detect new user fraud in real-time, lower the review rates considerably, and provide immediate ROI.

Before using BioCatch the retailer used traditional anti-fraud solutions such as:

- Data checks: shipping info, order details.
- Device and network reputation: known genuine and fraudulent devices and IPs.

Despite these fraud detection solutions the retailer continued to experience increased online fraud, together with a decrease in approval ratings which resulted in significant losses.

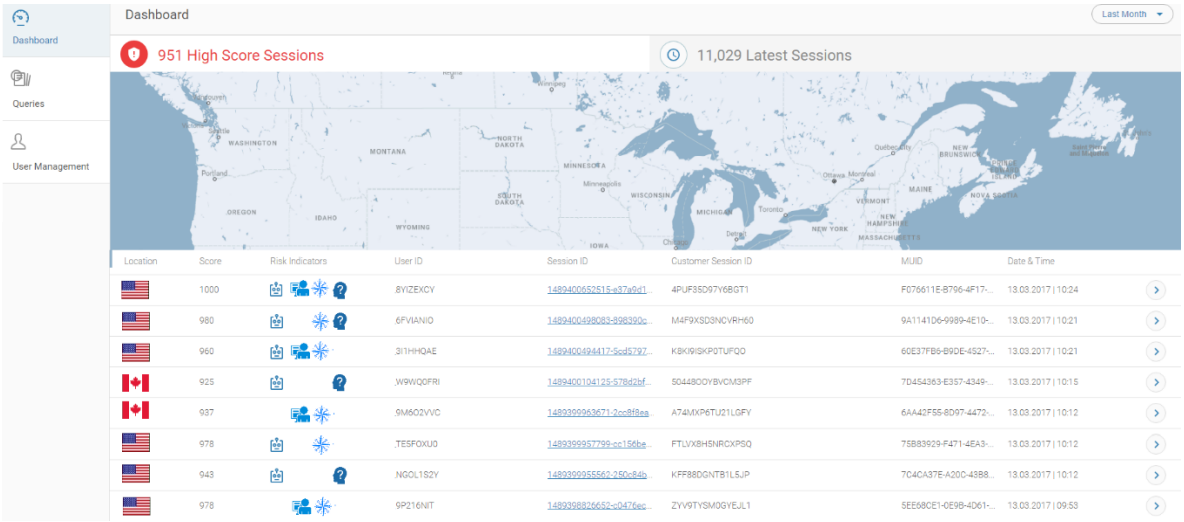

Figure 1. BioCatch Analyst Station for fraud detection

In 2016 the retailer deployed BioCatch's behavioral biometrics technology as a new safeguard against new user fraud.

Preventing New Account Fraud with Behavioral Biometrics

BioCatch maps user behavior throughout the online account creation process. Relevant use cases include applying for a credit card online, using a credit card for the first time on an online retail site, opening a checking account (new to bank) or registering to an online banking service (new to online banking).

In all these cases there are stark differences between honest users and dishonest criminals. They include:

Navigation Fluency: Most fraudsters operate on scale to repeatedly attack a site. Therefore, they are highly familiar with the site and/or complete the checkout form**.**

Expert Users: Fraudsters often use advanced computer skills that are rarely seen among real users. Common examples include keyboard shortcuts and function keys.

Low Data Familiarity: Fraudsters exhibit several behavioral traits when they enter in stolen personal information. For example, when typing long strings of data they need to pause after several keys and look back at the list, as they use short-term memory as opposed to genuine users who use their long-term memory.

The Need

To reduce new user fraud-related losses, accept more applications/payments and review less suspect cases.

The Solution – Key Benefits

Once BioCatch's solution was deployed, the Latin American retailer saw immediate results:

- Savings of more than $200K per month.
- $1.8M in fraud saved in the Black Friday weekend - the busiest time of the year.
- 85% less false alarms when compared to their regular controls.
- Immediate detection of automated (robotic) attacks.

About BioCatch™

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader.

The company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks and e-Commerce websites across North America, Latin America, and Europe. For more information, please visit www.biocatch.com

BIOCATCH
Less Friction. Less Fraud.

Contact Us

www.biocatch.com info@biocatch.com @biocatch www.linkedin.com/company/biocatch