BIOCATCH™
Less Friction. Less Fraud.

BioCatch Data Sheet

Mitigating the Risk of Insurance Fraud with Behavioral Biometrics

How BioCatch Mitigates the Risk of Insurance Fraud

- Recognizes human and non-human cyberthreats against legitimate accounts and insurance policies through behavioral biometric profiling.
- Authenticates users passively, continuously and without friction, mitigating the risk of account takeover in post-login sessions with actionable risk scores and threat indicators.
- Supports increased functionality in the digital channel by lowering the risk of fraud and reducing the costs of escalations and step-up authentication.

The global insurance market is a multi-trillion-dollar market worth more than $4.5 trillion in gross insurance premiums (2015)[1]. In 2016, the gross insurance in premiums in the U.S reached $2.67 trillion with $1.5 trillion in paid claims[2].

Fraudsters have set their sights on these claims and are looking for new and inventive ways to get funds diverted to them. As the use of digital channels in the insurance industry becomes more prevalent, fraudsters turn to social engineering, malware and remote access attacks to fool unwitting victims. According to the Federal Bureau of Investigation (FBI), the annual cost of insurance fraud is approximately $40 billion, costing the average American family $400-$700 in increased premiums[3].

Fraudsters use several tactics to conduct their activities, including: using stolen/synthetic identities to obtain fraudulent policy applications, take over legitimate accounts to file false claims or change payee information to receive insurance funds.

Behavioral Biometrics for Insurance: How It Works

BEHAVIORAL BIOMETRIC PROFILING: The BioCatch solution collects and analyzes over 2000 behavioral parameters including hand-eye coordination, pressure, hand tremors, navigation, scrolling and other finger movements, etc. To optimize user profiling, the system detects the behavioral parameters that are most strongly associated with the user meaning that, for those parameters, the user does not behave like the rest of the population. Each person's profile is comprised of unique behavioral features and can be linked across devices.

INVISIBLE CHALLENGES™: This patented technology, refers to tests that are invoked into an online session without the user's knowledge, but that elicit subconscious responses that can be used to distinguish a fraudster from a legitimate user. Since the user is unaware of the challenge, there is no way for a human or bot to mimic or predict the response.

ACTIONABLE RISK SCORE & THREAT INDICATORS: The BioCatch solution searches for different kinds of fraudulent activity – criminal behavior, malware, bots, RATs, aggregators, etc. – and analyzes the behavior in a session to compare against the user's behavioral profile. Real-time alerts are generated and the activity is logged and visualized in the BioCatch Analyst Station.

[1] Plunkett Research Website, "Insurance Industry Statistics and Market Size Overview, Business and Industry Statistics", (Accessed: 9.8.17).

[2] Organization for Economic Cooperation and Development (OECD), "Insurance Markets in Figures: Insurance SectorShows Diverging Trends in Premiums Worldwide", (Accessed: 9.8.17).

[3] U.S Federal Bureau of Investigation (FBI) Website, "Insurance Fraud", (Accessed: 9.8.17).

USE CASES

Identity Proofing

In the case of account opening fraud, there is no known user, and by extension, no existing user profile. Yet, when opening a new deposit or credit card account, fraudsters behave quite differently than legitimate users, and these patterns can be recognized by the BioCatch platform. For example, fraudsters experience surprising familiarity with the online application process, their fluency patterns are distinctive, they have all the required information at hand and never spend time researching it, and yet, the way they input information suggests it does not belong to them.

Simply put, the way fraudsters interact with specific fields can be very uncharacteristic when compared to the behavior and cognitive choices exhibited by legitimate applicants. Going beyond just looking for robotic behaviors in the application process, BioCatch can pick up on the differences between human interactions as well in real time and provide an alert before a potentially fraudulent application goes through.

Continuous Authentication

Continuous authentication is a capability that can prevent payment hijacking and insurance claims from being diverted to false identities. The BioCatch Continuous Authentication Module develops behavioral biometric profiles of online users and matches those profiles continuously, with patented, Invisible Challenges techniques, to validate the identity of the after the login and prevent account takeover and other cyberthreats.

Fraud Prevention

BioCatch's Fraud Detection Module offers a new level of detection and protection against malware, bots, aggregator and other Remote Access Trojans. Each of these behave differently than a human being, meaning that they exhibit their own unique behavioral patterns that can be identified. Many of today's RATs are human, tricking victims via social engineering into logging into their own accounts and then taking over. Analyzing hundreds of human and non-human behavioral parameters every second, BioCatch's patented technology is able to detect an anomaly in a session in real-time. This capability is also a very effective tool in combating insurance payment hijacking by social engineering schemes and remote access tools.

About BioCatch

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. 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. For more information, please visit www.biocatch.com.

Less Friction. Less Fraud.