BioCatch

Solution Brief

Behavioral Biometrics for Mobile

Lock Cybercriminals Out of Mobile Banking

Capabilities

- Continuous protection of banking sessions across mobile platforms
- Eliminate mobile channel blind spots with behavioral risk scores and visibility into detailed session activity
- Detect a broad range of mobile banking fraud threats

Benefits

- Decrease mobile fraud losses
- Build trust and drive retention by delivering a secure and frictionless mobile experience
- Increase revenue by offering more products and services via the mobile channel with confidence

In an age where the use of smart phones has skyrocketed and consumers require convenience more than ever, financial institutions continue to invest in mobile banking. In fact, the Federal Reserve recently predicted that ~96% of US financial institutions will offer mobile banking by 2021[1]. With nearly 2 billion mobile banking users worldwide[2], organizations see this as a perfect opportunity to improve customer satisfaction and in turn increase acquisition and retention.

Striking a Balance: Customer Experience and Security

As financial institutions continue to drive mobile banking efforts, customer experience isn't the only factor to consider. As the use of mobile banking rises, so do the number of threats. As reported in Verizon's 2020 Data Breach Investigations Report, 64% of mobile threat incidents were driven by financial motives. In this fast-moving environment where mobile banking and fraud intersect, financial institutions have no choice but to ensure their mobile banking experience is seamless and secure. The challenge, however, is that many traditional fraud prevention controls, such as multi-factor authentication, introduce friction.

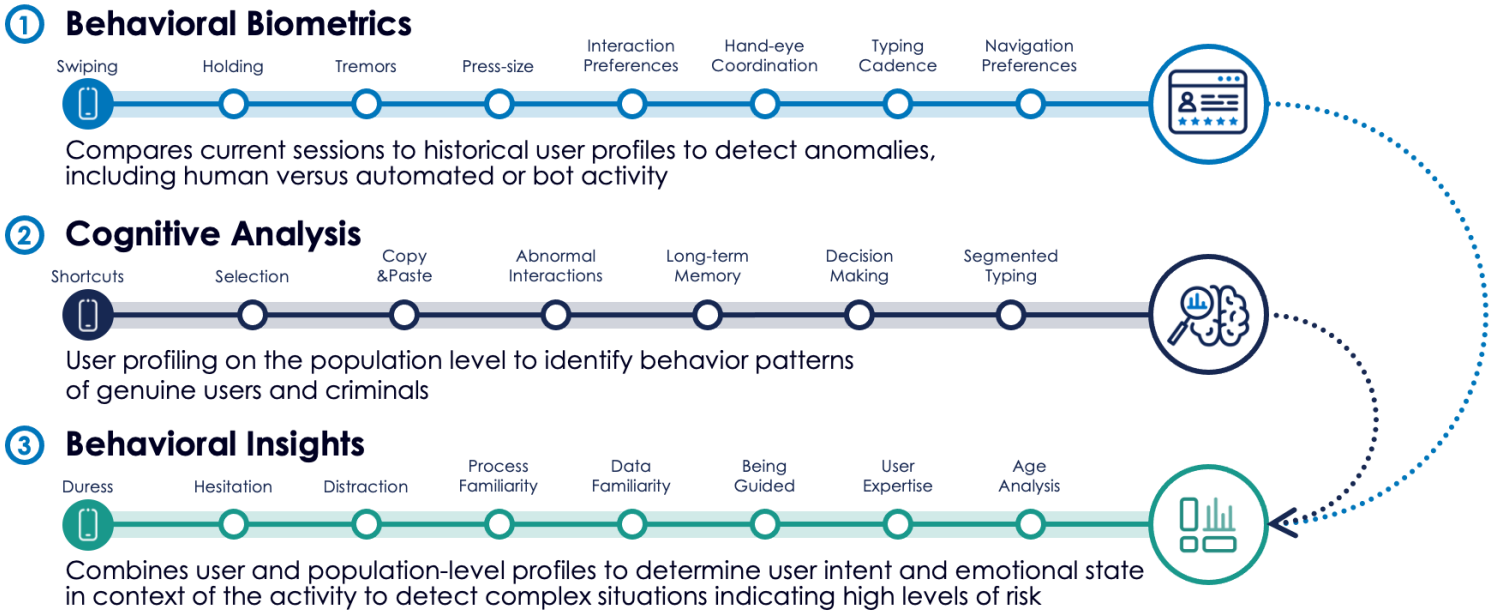
Behavioral Biometrics for Mobile

BioCatch delivers Behavioral Biometrics for mobile without user disruption by passively collecting and analyzing a user's physical and cognitive behavior.

The BioCatch Risk Engine is powered by machine learning algorithms that analyze a user's digital behavior. The model takes into consideration real-time mobile-specific interactions such as accelerometer, touch, orientation, and gyro to learn about unique behaviors including how the user holds their device, navigates, scrolls, taps, and slides to continuously protect the user throughout the mobile banking session. This data is profiled and analyzed on three levels.

[1] Source: 2019 Results from the Mobile Banking and Payments Survey of New England Financial Institutions
[2] Source: 2019 Juniper Research

Solution Brief



Combating all types of Mobile Banking Fraud

BioCatch combines behavioral insights with mobile-specific contextual data to deliver optimal fraud protection. The BioCatch platform detects a broad range of fraudulent activity including malware, Remote Access Tools, mobile emulators, social engineering scams, and device theft.

Social Engineering Voice Scams

In social engineering fraud scenarios where the genuine user performs a fully authorized transfer under the influence of a cybercriminal, their behavior will show consistencies across many aspects. However, the BioCatch platform detects behavioral signs of distress, dictation, and hesitation by monitoring activity such as tap timing and mobile device movement. In addition, BioCatch leverages a call status functionality that enables the solution to detect if a user is on a call during a mobile banking session.

Malware & Remote Access Tools

By examining the applications on a user's device including when they were installed, the solution gains greater visibility into fraud as a result of malware applications and legitimate applications allowing remote access. Application information coupled with behavioral indicators such as those that align with RATs including latency, tap events with near-zero touch area, and lack of device movement, is invaluable to a holistic risk assessment.

Mobile Emulators

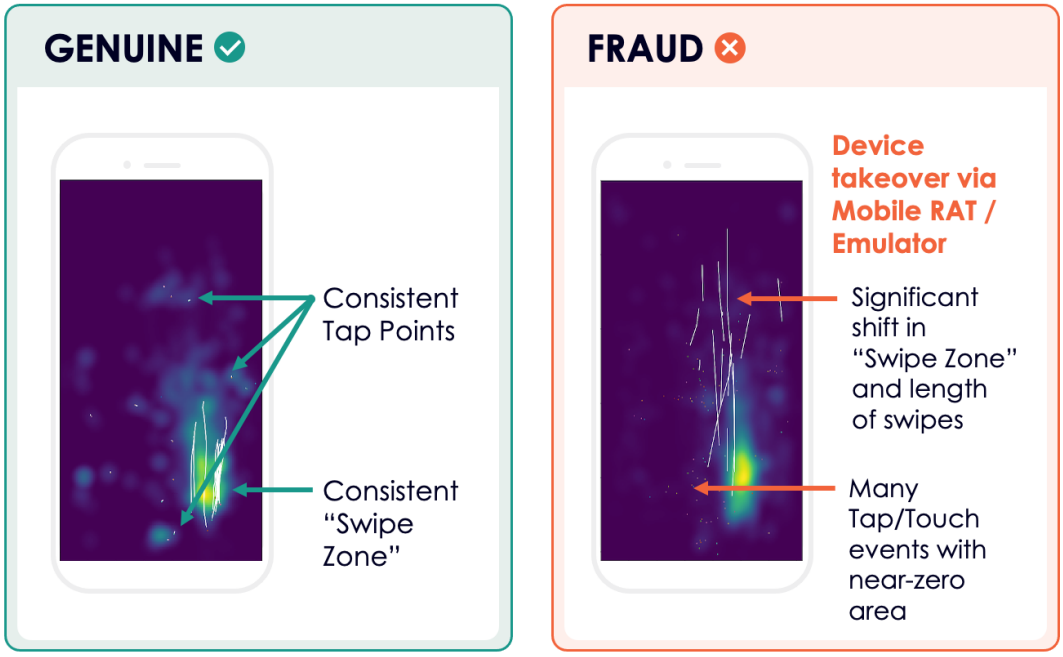
The BioCatch platform monitors for the use of mobile emulators - a virtual instance that is used to mimic a user's mobile device and perform account takeover. BioCatch detects fraudulent sessions run over mobile emulators based entirely on behavior. For example, by cross-correlating Accelerometer data and touch events, the solution can detect instances where there is no physical device or touch movement at all.

Device Theft

By continuously monitoring a user's physical and cognitive behavior and leveraging deep learning mechanisms, the BioCatch platform generates an anonymized user profile. These historical insights enable the solution to detect instances where a user's current behavior shows significant variations from their unique user profile. Even in a scenario where a cybercriminal has access to the user's genuine device, user behavior can never be stolen, spoofed, or replicated.

Delivering Actionable Insights

The BioCatch platform delivers real-time session risk scores and detailed mobile session activity is logged and visualized in the BioCatch Analyst Station. These insights empower fraud operation and analyst teams to act quickly and confidently without impacting the experience for genuine customers.



Mobile Behavioral Anomalies

Banishing Friction

BioCatch is truly frictionless from deployment and beyond, allowing financial institutions to add user functionality to their mobile banking experience without adversely impacting customer engagement or introducing additional risk.

The BioCatch solution secures mobile banking sessions conducted within mobile browsers or applications across Android and IOS devices and protects against Account Opening and Account Takeover attacks. Behavioral data collection is enabled by embedding the BioCatch SDK/JavaScript into a mobile application or website. In addition to supporting native mobile applications, BioCatch offers out-of-box connectors to support applications developed using popular application frameworks including Ionic and React Native.

BioCatch

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, over 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch