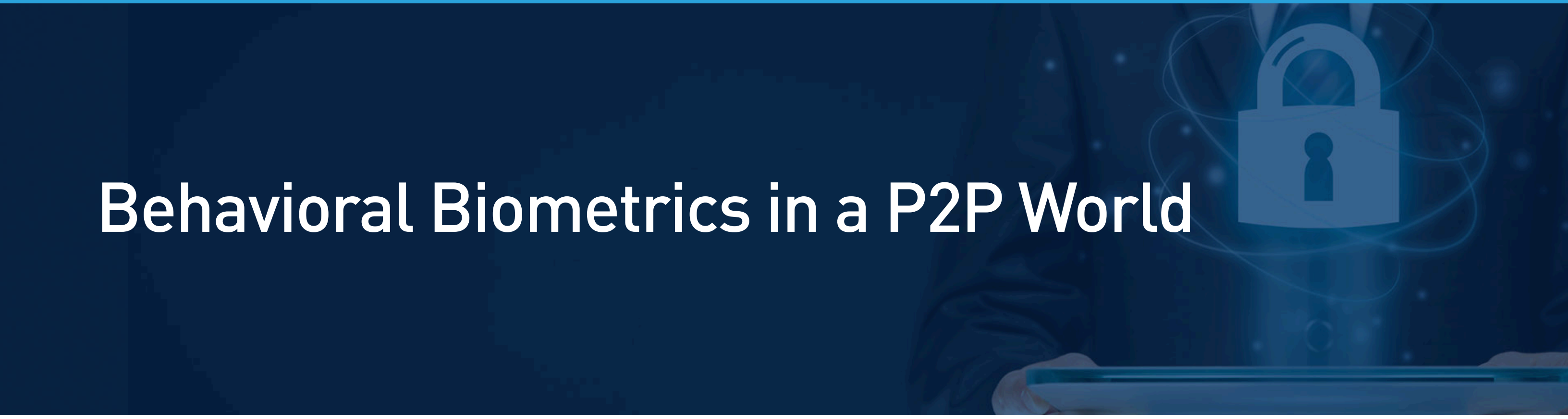
BIOCATCH
Less Friction. Less Fraud.

BioCatch Data Sheet



Behavioral Biometrics in a P2P World

What is Behavioral Biometrics?

Behavioral biometrics identifies people by how they do what they do, rather than by what they are (e.g., fingerprint, face), what they know (e.g. secret question, password) or what they have (e.g. token, SMS one-time code). Behavioral biometrics measures and analyzes patterns in human activities, capturing an array of human interactions between a device and an application, such as hand-eye coordination, pressure, hand tremors, navigation, scrolling and other finger movements, etc.

Mapping and monitoring these behavioral patterns passively and seamlessly throughout the users' time within the application, continuous authentication can indicate fraudulent behavior that occurs after the login, that is, after the two-factor authentication has been validated. With no disruption of user experience, this method also reduces the risk of false alarms, as opposed to traditional device ID or IP address validation and identifies threats immediately. This means stopping fraud in real-time and protecting consumers against the range of cyber threats.

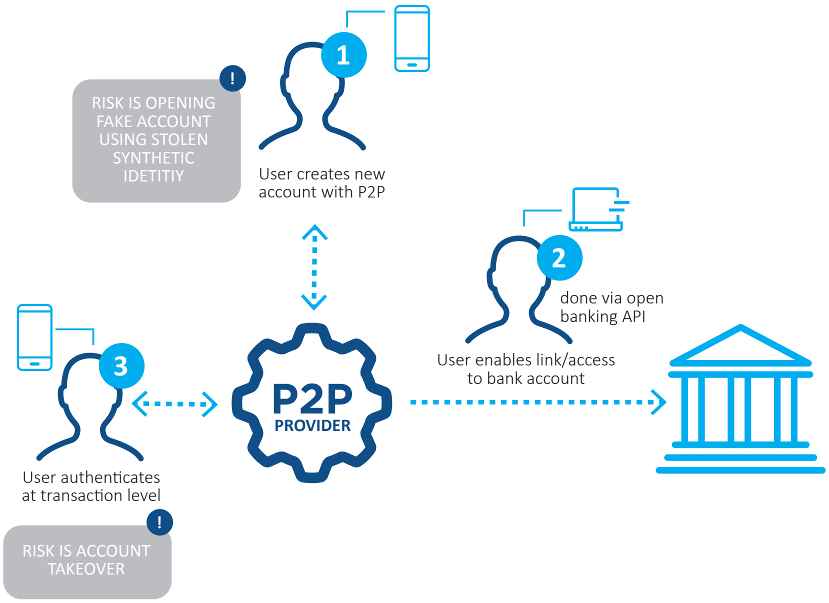
P2P: New Opportunities for Faster and Safer Payments

In recent years, Peer to Peer payments have shown a significant increase, passing the $120 billion mark (2017). Currently, one in three American consumers uses P2P apps to make instant payments to friends, relatives, service providers, or anyone they owe money. Since P2P account opening does not require identity verification, it is vulnerable to various types of fraud and threats including malware, social engineering, remote access, SIM swapping, call forwarding and other techniques. Using these techniques, the fraudsters are able to exploit two main points of failure:

- **Access to Account:** To enable P2P payments, banks provide access to payment accounts on the condition that the P2P provider has received permission from the bank customer to whom the account belongs.

- **Authentication:** Improving the security of direct payments requires strong customer authentication. To ease the customer journey, many P2P providers rely on device or knowledge information, and may only require a reauthentication in certain circumstances (a new location, or device is detected, or a new payment method is added).

BEHAVIORAL BIOMETRICS ADDRESSES THE RISKS IN THE P2P ECOSYSTEM



1
!
RISK IS OPENING FAKE ACCOUNT USING STOLEN SYNTHETIC IDETITIY
User creates new account with P2P
2
done via open banking API
User enables link/access to bank account
3
P2P PROVIDER
User authenticates at transaction level
!
RISK IS ACCOUNT TAKEOVER

To ensure consumer trust and stay active in the marketplace, the players across the ecosystem – banks, P2P providers, and others - must maintain very low fraud rates in order to stay active in the marketplace. In many ways, the P2P capability itself upends the financial ecosystem by holding various players responsible for different aspects of the payment process. This makes it difficult for all parties involved to prevent fraud and at the same time provide customers with a positive user experience.

Behavioral biometrics helps to prevent fraud while providing a frictionless user experience.

USE CASES FOR BEHAVIORAL BIOMETRICS IN A P2P WORLD

Open Banking

Need: P2Ps leverage banks to allow access to user accounts. The user will begin the journey on the P2P site or application and when asking to link the account, will be redirected to the bank website to verify identify and confirm the request to link.

Solution: Implementing BioCatch, the bank will be able to verify that it is the same user making the request and not an imposter or someone using stolen credentials (account takeover attempt).

Identity Proofing During Account Opening

Need: Eliminating fraud at the account origination process will ensure trust throughout the customer lifecycle. This is made increasingly difficult by the soaring cases of stolen and synthetic ID.

Solution: BioCatch maps criminal behavior throughout the initiation process using factors like *Application Fluency, Navigational Fluency* and *Data Familiarity.* Understanding the way fraudsters behave, allows the BioCatch system to identify human and non-human elements in a session in real-time and prevent a potentially fraudulent application from going through.

Authentication

Need: Given that 100% of fraud occurs in authenticated sessions, a session that relies on a prior authentication of known device or location is at risk of a remote account takeover as a result of malware, bot activity or social engineering.

Solution: BioCatch collects, measures and analyzes more than 2000 behavioral parameters to build robust behavioral profiles that cannot be mimicked, stolen or reverse engineered. this approach can be used for risk-based authentication that triggers escalations when behavioral anomalies are detected.

Benefits of Behavioral Biometrics:

- Facilitate safe transactions, secure safe payments and increase customer trust.

LESS FRICTION

- Better user experience. Passive.
- Strong customer authentication.
- Enable more functionality.
- Slash costs: Reduce friction-related costs.
- More transactions approved automatically.

LESS FRAUD

- Based on real user behavior (not estimated origins of threat).
- Prevents spoofing and account takeover through bots, RATs, and malware.
- Detects criminal behavior during account opening.
- Identifies precursors for cross-channel fraud.

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.

BIOCATCH™
Less Friction. Less Fraud.