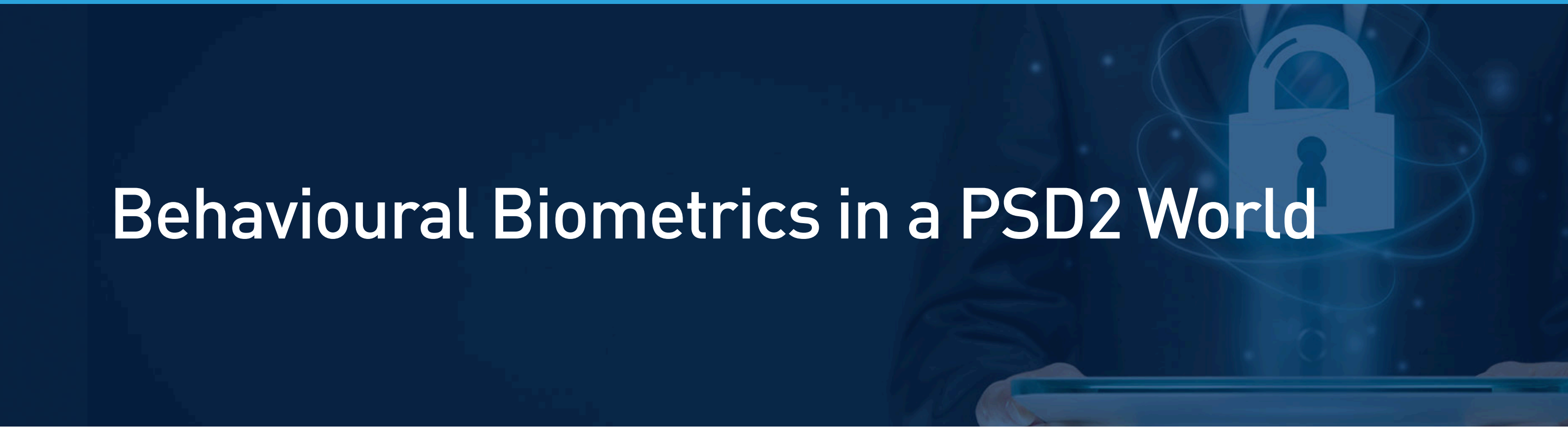
BIOCATCH
Less Friction. Less Fraud.

BioCatch Data Sheet



Behavioural Biometrics in a PSD2 World

What is Behavioural Biometrics?

Behavioural 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). Behavioural biometrics measures and analyses 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 behavioural patterns passively and seamlessly throughout the users' time within the application, continuous authentication can indicate fraudulent behaviour 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 a full range of cyber threats.

PSD2: New Opportunities for Faster and Safer Payments

Two major implications of PSD2 are *Access to Account* and *Strong Customer Authentication:*

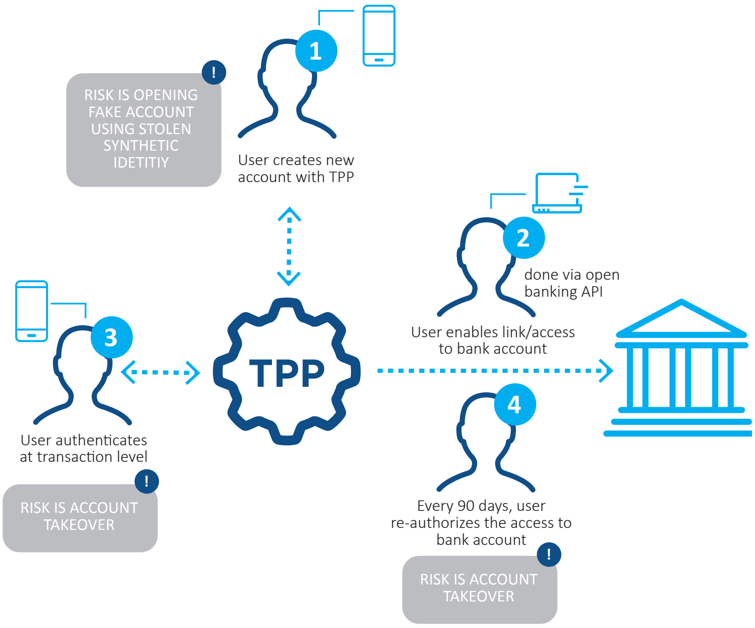
- **Access to Account (XS2A):** PSD2 opens the market for new payment players and creates a direct link between the TPP and the bank via an open API.

- **Strong Customer Authentication (SCA):** PSD2 requires that users be authenticated using at least two of the following independent factors: *Knowledge* – Passwords, PINs that only the user knows; *Ownership* – Cards, tokens, mobile phones that only the user has; *Inherence* – The user's physical or behavioural biometrics.

PSD2 also requires TPPs to meet strict criteria and maintain very low fraud rates in order to stay active in the marketplace. In many ways, these requirements upend 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.

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

BEHAVIOURAL BIOMETRICS ADDRESSES THE RISKS IN THE PSD2 ECOSYSTEM


1
User creates new account with TPP
!
RISK IS OPENING FAKE ACCOUNT USING STOLEN SYNTHETIC IDETITIY
2
done via open banking API
User enables link/access to bank account
TPP
3
User authenticates at transaction level
!
RISK IS ACCOUNT TAKEOVER
4
Every 90 days, user re-authorizes the access to bank account
!
RISK IS ACCOUNT TAKEOVER

USE CASES FOR BEHAVIOURAL BIOMETRICS IN A PSD2 WORLD

Open Banking API

Need: PSD2 requires banks to allow TPPs access to user accounts per approval via API. The user will begin the journey on the TPP site and when asking to link to 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). Moreover, after the 90-day token expires and the user is required to enroll once again, behavioural biometrics can be utilised for the authentication process.

Identity Proofing During Account Opening

Need: The TPP is required to meet certain fraud levels to maintain certification and status. Eliminating fraud at the account origination process will ensure trust throughout the customer lifecycle.

Solution: BioCatch maps criminal behaviour 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 account from being created.

Authentication

Need: Strong Customer Authentication requires a strong element that is based on Inherence ("Something You Are"). This element must be unique, personal and produced solely by the genuine user to support *Risk-Based Authentication.*

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

Benefits of Behavioural 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 behaviour (not estimated origins of threat).
- Prevents spoofing and account takeover through bots, RATs, and malware.
- Detects criminal behaviour during account opening.
- Identifies precursors for cross-channel fraud.

About BioCatch

BioCatch is a cybersecurity company that delivers behavioural biometrics, analysing 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.