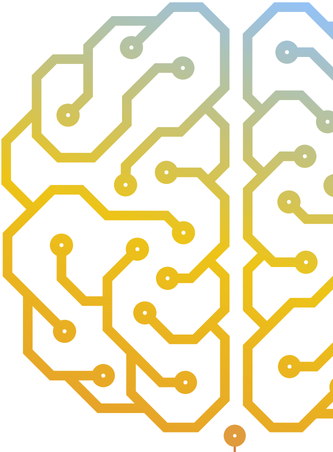
# BEHAVIORAL BIOMETRICS: EXPLAINED

The digital banking world is rife with sophisticated fraud. As fraudsters become more inventive with ways to trick users into giving up their personal information, how can we keep up to ensure the safety of bank accounts and assets?

**Behavioral biometrics is the way forward.**

## What is BEHAVIORAL BIOMETRICS?



**Behavioral biometrics** is a method for identifying unique and measurable patterns in a human's **behavior**, and is derived from the general premise that an individual person can be reliably identified by their behavioral habits and environments.

As a built-in functionality of the **HID Fraud**

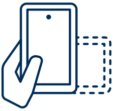
**Prevention and Risk Management Solution**, behavioral biometrics works as part of a broader, unique ecosystem that prevents fraud in real-time.

Unlike physical biometrics — which might include height, weight and unique fingerprints — **behavioral biometrics** is easily transferable to the digital world based on the user's digital interactions and the available data points, such as:

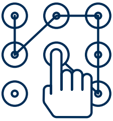
**The user's IP address**

**How the user interacts with an application**

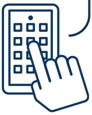
**Which device the user is on**



How the user holds the device

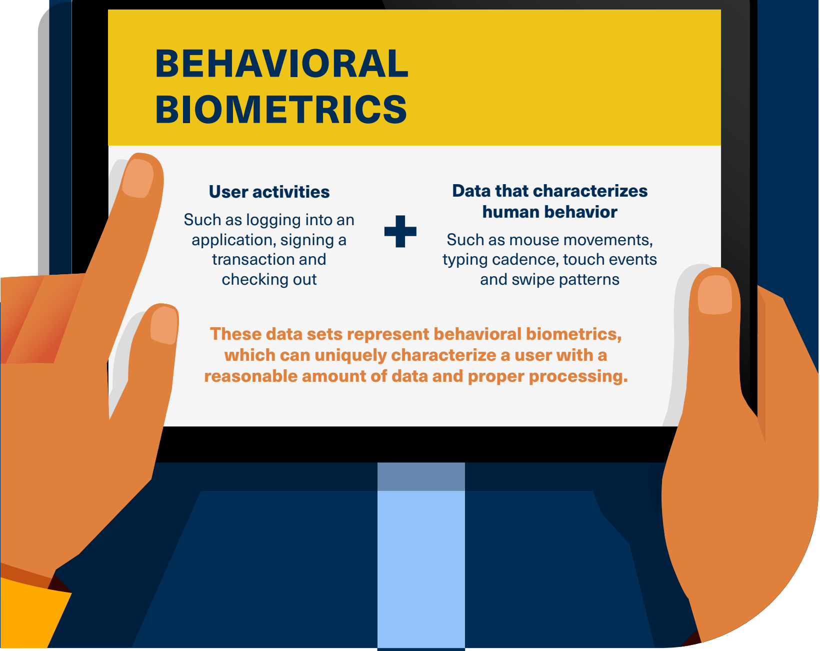


Keystroke and swipe patters



Touch events

Behavioral biometrics processes user behavioral data to form a profile. This profile is then used to validate and verify their identity and authenticate to facilitate their intent **— whether this be accessing their account or making a transaction.**



# BEHAVIORAL BIOMETRICS

**User activities**

Such as logging into an application, signing a transaction and checking out

+

**Data that characterizes human behavior**

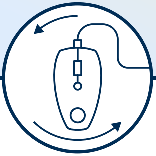
Such as mouse movements, typing cadence, touch events and swipe patterns

**These data sets represent behavioral biometrics, which can uniquely characterize a user with a reasonable amount of data and proper processing.**

# HERE'S HOW IT WORKS

Behavioral biometrics works by creating a **trusted user profile.** This is done by observing the user's behavioral patterns — such as mouse movements, keystroke dynamics and navigational patterns. This data can then be gathered via dynamic collection points in the background of an application.

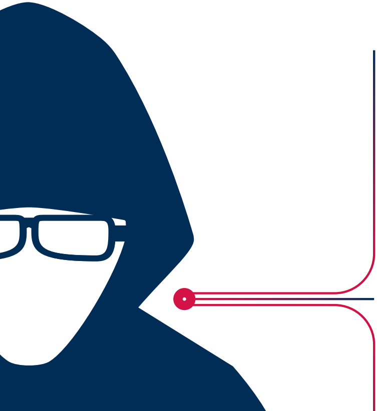
**Mouse Movements**



**Keystroke Dynamics**

**Navigational Patterns**

## WORKING TO DETECT SUSPICIOUS ACTIVITY AND PREVENT FRAUD



Behavioral biometrics applies machine learning algorithms to create a user-specific profile using the multitude of inputs gathered while a user interacts with a specific application.

This profile is continuously updated, improved and enriched in real time, so it can be used to uniquely and seamlessly identify a user.

These markers, augmented with user-specific information such as location, device, time and navigation patterns, deliver the best contextual value resulting in a high fraud detection rate and decreased number of falsely rejected users.

## HOW IS IT SECURE?

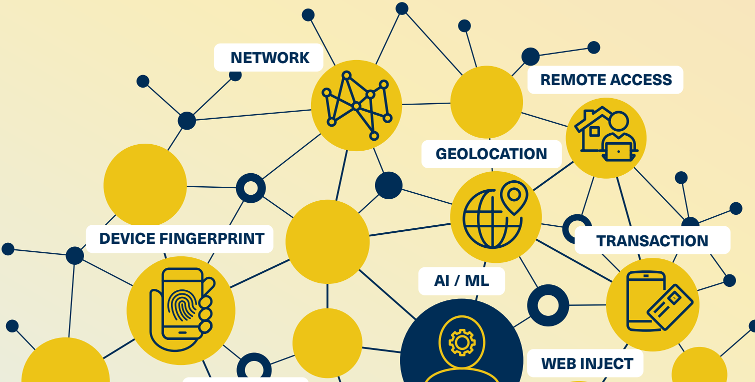
**Fraud Prevention** — By detecting suspicious activity, behavioral biometrics facilitates safe and secure online experiences while reducing business fraud risk. For a complete way to detect and prevent fraudulent activities before they occur, behavioual biometrics also serve as part of HID's wider Fraud Prevention and Risk Management Solution for ultimate security.

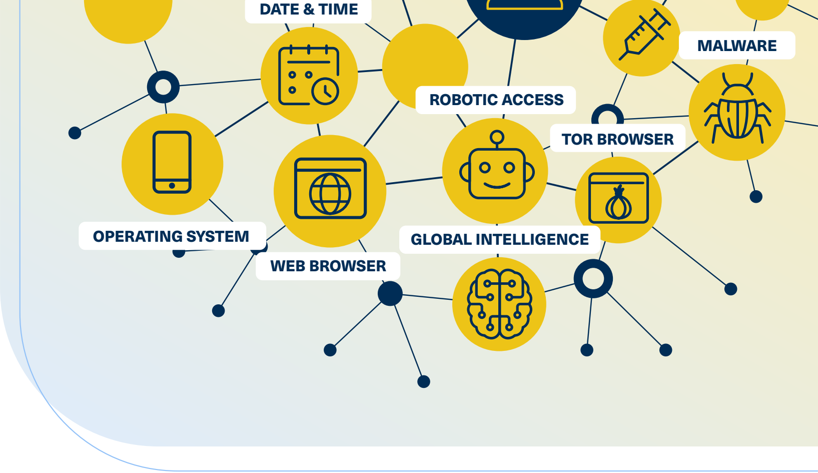
**Simple Compliance** — Behavioral biometrics helps banks to stay compliant with regulations where adherence is needed to Strong Customer Authentication (SCA). The approach is recognized by regulators, such as the European Banking Authority (EBA), and can be used in compliance with data protection regulations around the world, like GDPR.

# THE BENEFITS

## Of behavioral biometrics within an integrated consumer journey

- **No additional devices needed** to create and compare individual profiles, unlike other biometric authentication techniques, such as fingerprinting, retinal scan and voice recognition
- **A better user experience** as it works unobtrusively in the background of an active application
- **Seamless, frictionless re-authentication** without password pain and the need for old-fashioned hardware tokens or SMS OTPs





**Want to learn more about leveraging a complete risk management solution?**

Read the **“The Ultimate Guide to Risk Management Systems”** now>>

©2025 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID and the HID Global are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

2025-03-25-iams-behavioral-biometrics-ig-en PLT-06644

HID