BioCatch Inherence for Strong Customer Authentication

Supporting Your Journey to PSD2

Strong Customer Authentication: New Opportunities for Faster and Safer Payments

With constantly evolving technology, ever-present competition and limited resources, the payments industry has always been fast-moving. With the added burden of a global pandemic, resulting in increasing cybercrime and fraud and ever-tighter regulatory and political pressures, businesses must achieve resilience whilst maintaining the near frictionless and trusted digital experiences that customers have come to expect.

Whilst regulations, such as PSD2, try to preserve the integrity of the ecosystem by reducing fraud, regulators always grapple with long regulatory cycles. Fraudsters, unlike legitimate businesses, are not affected by these cycles, and global events, such as a pandemic, are conducive to criminal purposes. As criminals remain several steps ahead of regulations, consumers adopt new technologies, share more and more data, demand safety and expect their trust not to be broken.

Stop Criminals, Not Customers

With over a decade of experience analyzing digital behavior, the BioCatch platform has an unmatched ability to distinguish between genuine users and cybercriminals, protecting organizations and their customers against a broad range of threats. BioCatch takes a fresh approach by monitoring a user's physical and cognitive digital behaviors to detect fraud and identity theft and improve customer experience.

Genuine users innately behave differently than fraudsters; through continuous session visibility and advanced profiling capabilities, the BioCatch platform surfaces behavioral patterns that tell a story – one of cybercriminal or one of a genuine user.
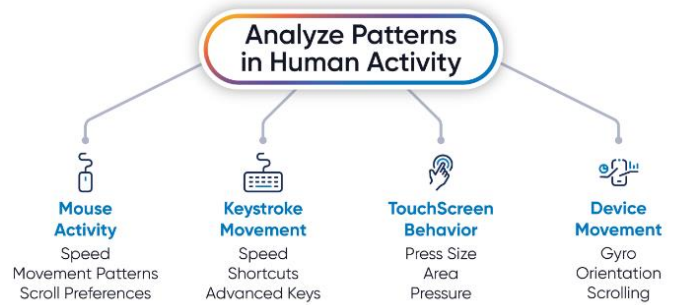

CYBERCRIMINALS vs GENUINE USERS

Cybercriminals:
- Don't present familiarity with data
- Repeatedly delete and fix errors
- Rely on copy, paste & automated programs
- Familiar with new account application form due to multiple applications

Genuine Users:
- Different pace & navigation patterns
- Display the use of long-term memory
- Hesitate on fields criminals confidently fill
- Use the AutoFill feature for personal details

| [1] Source: The Financial Brand, Digital Banking Report Research, August 2020

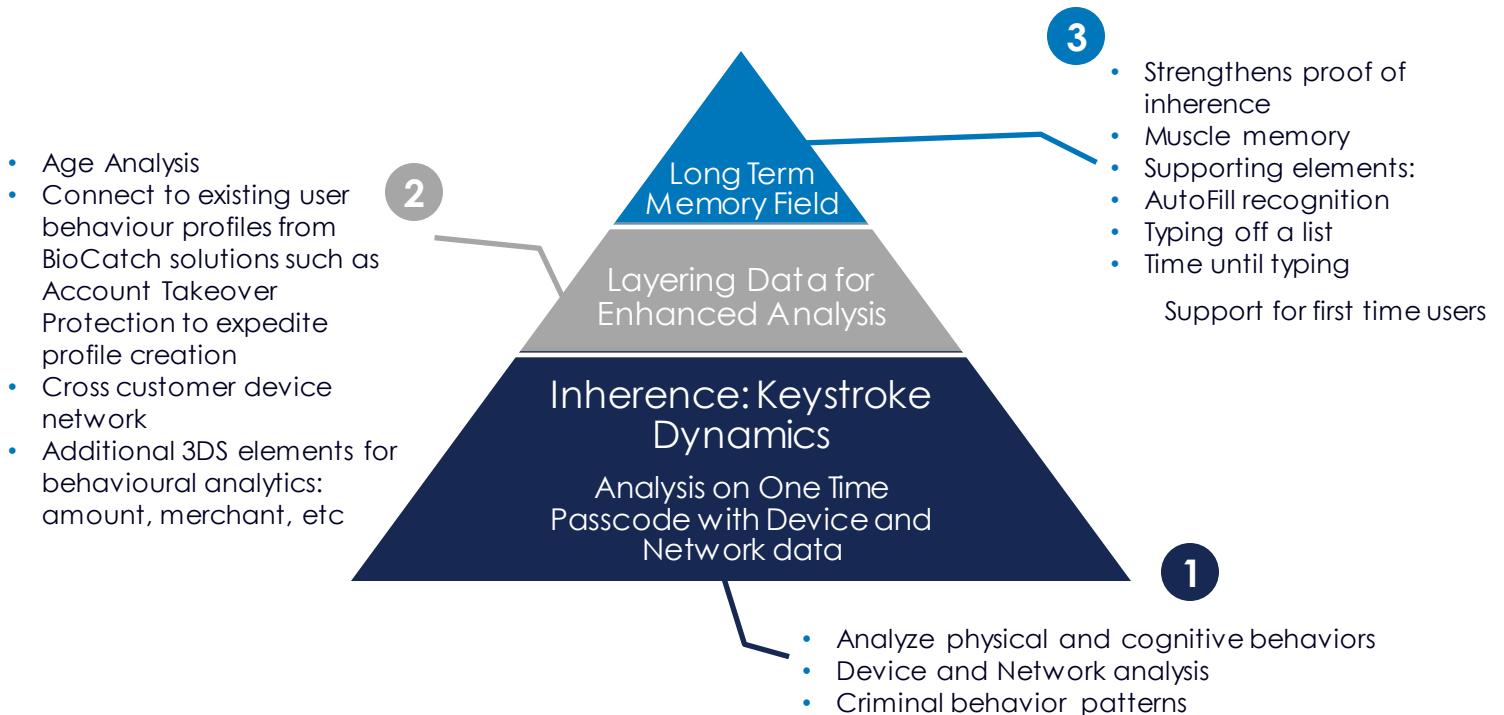# The Power of Behavioral Insights For A Frictionless SCA Flow

Digital behaviours are collected during the SMS OTP flow of the ecommerce journey to create a behavioural biometric profile. BioCatch profiles user behaviours such as mouse movements, typing cadence, swipe patterns or device orientation. The activity is then compared against the historical user profile for the individual account to provide a passive authentication layer and against population level patterns to identify statistically observed norms for "good" and "bad" behavior based on legitimate user and cybercriminal user profiles.

Analyze Patterns in Human Activity

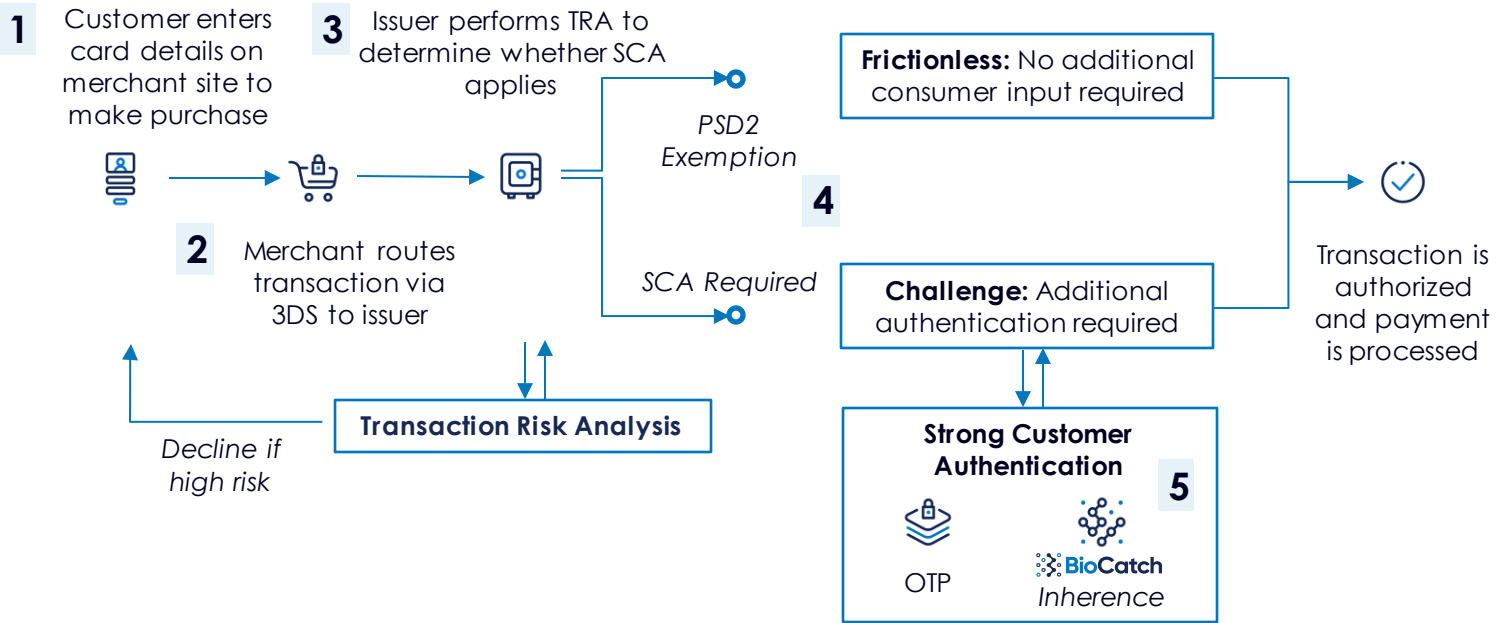| Mouse Activity	Keystroke Movement	TouchScreen Behavior	Device Movement
Speed	Speed	Press Size	Gyro
Movement Patterns	Shortcuts	Area	Orientation
Scroll Preferences	Advanced Keys	Pressure	Scrolling

If the BioCatch score reaches a pre-determined threshold and correct OTP entered, 2FA is complete. BioCatch also offers a layer of entry of familiar information in order to apply additional confidence to the authentication flow.

Contrary to traditional fraud controls that heavily rely on elements that are subject to compromise or change, user behaviour can never be stolen, spoofed, or replicated.

BioCatch for SCA in: A Three-Layered Approach

- Age Analysis
- Connect to existing user behaviour profiles from BioCatch solutions such as Account Takeover Protection to expedite profile creation
- Cross customer device network
- Additional 3DS elements for behavioural analytics: amount, merchant, etc

3
- Strengthens proof of inherence
- Muscle memory
- Supporting elements:
- AutoFill recognition
- Typing off a list
- Time until typing

Support for first time users

2

Long Term Memory Field

Layering Data for Enhanced Analysis

Inherence: Keystroke Dynamics

Analysis on One Time Passcode with Device and Network data

1
- Analyze physical and cognitive behaviors
- Device and Network analysis
- Criminal behavior patterns

Securing New Users: By adding a long-term memory field for new users with no pre-existing profiles, BioCatch can determine whether the behaviour displayed belongs to a genuine user or cybercriminal by identifying patterns of knowledge with data, use of remote access tools, and other patterns correlating with "good" or "bad" resulting in lower false rejections and enhanced detection. Once profiles are created, this field can be removed to enhance customer experience.

BioCatch in the 3D-Secure flow

1 Customer enters card details on merchant site to make purchase

2 Merchant routes transaction via 3DS to issuer

3 Issuer performs TRA to determine whether SCA applies

PSD2 Exemption

SCA Required

4

Decline if high risk

Transaction Risk Analysis

Frictionless: No additional consumer input required

Challenge: Additional authentication required

Strong Customer Authentication **5**

OTP

BioCatch *Inherence*

Transaction is authorized and payment is processed

Tackling the Most Sophisticated Threats

Through advanced profiling capabilities, the BioCatch platform detects even the most subtle signs of criminal activity, providing a greater breadth of coverage against the **most sophisticated attacks** including:

Bots & Aggregators

Malware

Social Engineering Voice Scams

Remote Access Tools

Mobile Emulators

Stolen Account Credentials

The BioCatch solution detects key behavioural indicators that align with popular attack methods, such as automated patterns which can indicate account takeover via bot or malware, and surfaces anomalies that can suggest a human imposter, such as dominant hand change and expert user patterns.

BioCatch

BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch

Tel Aviv | New York | Boston | London | São Paolo | Santiago | Mexico City | Melbourne | Mumbai | Singapore