BIOCATCH
Less Friction. Less Fraud.

INVISIBLE CHALLENGES

by BioCatch, The Cognitive Biometrics Company.

October, 2014

White Paper

1

EXECUTIVE SUMMARY

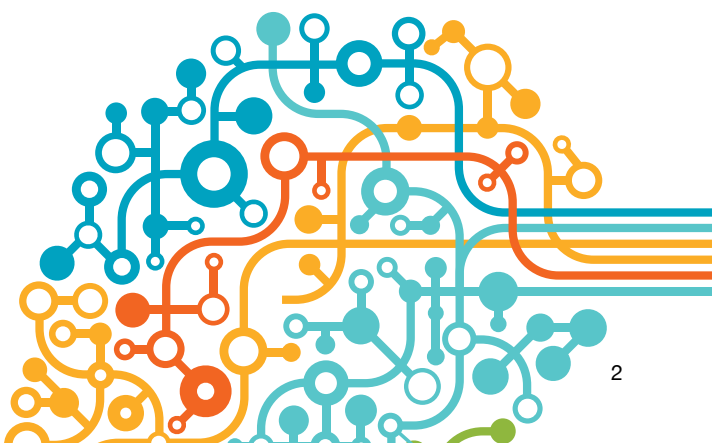
In today's world, personal passwords are relatively easy to crack. Fraudsters are continuously finding new ways to track online passwords and hack into computers. If your Facebook account is hacked, for example, it's not a crisis, you'll simply be asked to change your password settings; but what if fraudsters get a hold of your online bank account log-in, and are able to make transactions from your account?

Scenarios such as this require a new approach to authentication that doesn't rely solely on passwords, specific devices or location, but rather on user behavior.

BioCatch offers a disruptive authentication solution for web and mobile based on cognitive biometrics. Gartner's Market Guide for Online Fraud Detection predicted that by 2017, passive biometric analysis will become a standard feature of at least 30% of one-stop fraud detection solutions — up from less than 1% today.[1]

BioCatch leverages proprietary technology that inserts "invisible challenges" into the user's session. Users unknowingly respond to these subtle challenges developing individual patterns that create unique user profiles. This allows BioCatch to produce a frictionless authentication signature that is dramatically more accurate and sustainable than existing solutions on the market today. Additionally, this continuous authentication allows confirmation of the user at any time throughout the session.

The result - a frictionless and transparent authentication tool.



1 Gartner Market Guide for Online Fraud Detection Report, June 2, 2014

2

HOW IT WORKS

Background

BioCatch collects over 400 cognitive biometric parameters for each user of a bank or eCommerce site, and uses machine-learning algorithms to generate a unique individual profile. Out of these 400 parameters, a few dozen are both consistent and distinct for each user. When a session starts, the system begins to collect information and uses semi-random pro- active challenges in order to generate a user's identity.

On PCs, mouse dynamics, keyboard dynamics, typing patterns, etc. are all used to determine parameters, while on mobile devices the technology relies on collecting biometric data from the touch interface and accelerometer (ex. how you hold the device, how strong is your tap, how wide is the surface area when you press a button, etc.).

BioCatch can also introduce subtle cognitive biometric challenges into the session that users subconsciously respond to without sensing any change in their experience.
The result is a frictionless and continuous authentication that is highly accurate because it doesn't depend on what the user knows or information he/she has, but rather on who the **User is.** Additionally, BioCatch does not require proactive collection or special HW/SW, and has zero impact on usability.

Cognitive Biometric Measurements (Mobile)

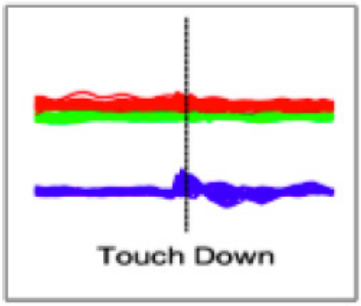
Gartner, in its Market Guide for Online Fraud Prevention 2014, explains passive biometric analysis as, "analysis done 'behind the scenes' and is transparent or unknown to the user (unless an organization chooses to tell the user it is occurring). There is no user enrollment necessary. Over time, the system is trained on a user's biometric "signature" so that it can compare the signature to a fraudster's on a blacklist, or to ongoing user behavior to determine whether the legitimate user is being impersonated. The use of passive voice recognition and passive gesture dynamics — that is, behavioral techniques in which user movements on a device are tracked and measured — have already proved to be very useful in the OFD market."[2]
The following are examples of cognitive biometric measurements that BioCatch utilizes for mobile: Accelerometer Data, Touch Interface and Mouse Interface

Accelerometer Data

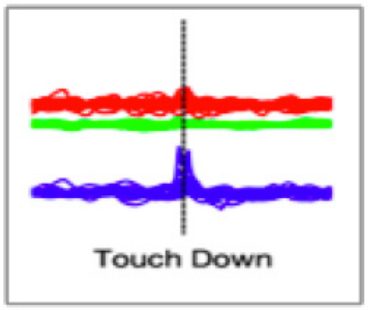
Everyone holds their device in a slightly different way, and making sense of the accelerometer data requires intensive research into cognitive and motoric functions within the specific context of a banking application.

2 Gartner Market Guide for Online Fraud Detection Report, June 2, 2014

Below is an example of two users monitored by BioCatch: The charts represent accelerometer data at the point of pressing a button ('touch down'). Left to the dotted line is before the action, and right is after the event.



User A



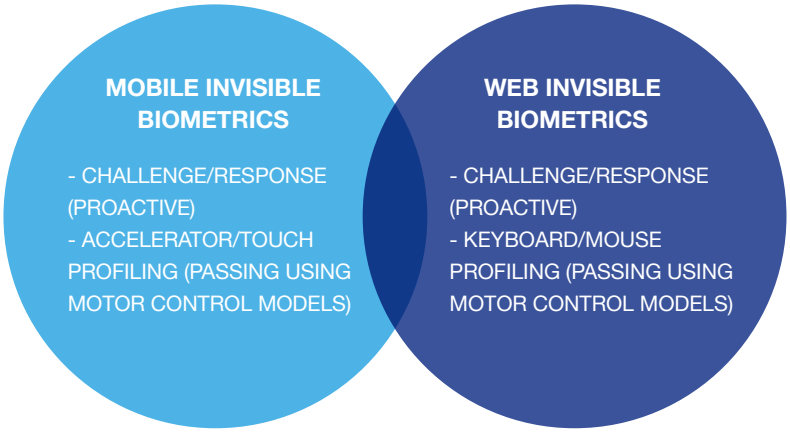
User B

The green and red lines represent left-right and backward-forward movements respectively. It's clear that user B has a somewhat shaky hand (red 'scribbles'). He thumps the device whenever he hits a button. This can be seen by the blue spike at the center (blue represents the vertical movement of the device). The combination of a shaky hand and a strong thump is something very consistent and rather distinct. User A, on the other hand, has a consistent and unique vertical movement pattern right after the event of pressing the button. His hand is quite steady.

Touch Interface and Mouse Interface Analysis using Motor Control Models

BioCatch also passively collects data from the device touch interface (for mobile) and mouse (for PCs), but processes it unconventionally. Whereas other behavioral biometric technologies look for repeating patterns in the way the user interacts with the application, BioCatch takes a different approach. BioCatch uses Motor Control, a cognitive science discipline, to learn how the human mind controls the hand/wrist/finger movement as the user
interacts with the application, and essentially 'reverse engineers' the process in order to find individual traits.

The following sections detail our multi-channel technology, covering Mobile and Web:



Mobile Biometrics: Invisible Cognitive Challenges

At the heart of BioCatch's technology is the patent-pending approach of subtle cognitive-invisible challenges™.

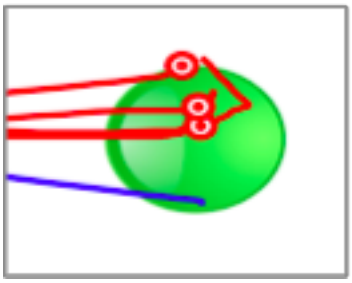
The following examples illustrate how proactive cognitive-invisible challenges™ are used to establish consistent and distinct traits.

Rotation of Movement

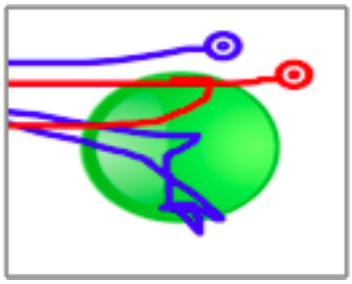
Rotation of movement is an invisible challenge that users compensate for without actually sensing any change in their regular experience. BioCatch's team of researchers test each deviation to determine the threshold below which users stop noticing the deviation.

Everyone reacts differently to an invisible challenge. In the example below, a fraud director in one of the top 5 UK banks (left) has a small correction to a right-side deviation that would have made him miss his target without correction. The fraud manager did compensate for the deviation, and reported that he didn't sense the challenge or spot anything different in the user experience. That fraud director typically has one small correction at a 60-80 degree (red hook) made during the last 10% of the movement.

But other people respond differently to the same challenge. In the screenshot to the right, a QA manager responds with multiple corrections (blue lines). She begins her correction during the last 20% of the movement.



Fraud Director



QA Manager

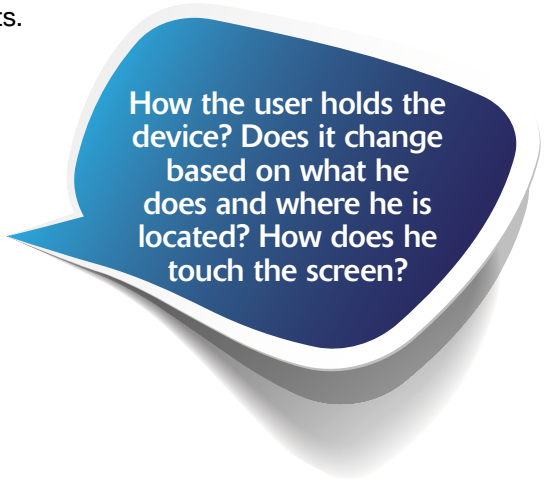
This example demonstrates an iPad touch interface challenge-response by leveraging a drag- and-drop effect. The idea is to leverage existing interactions rather than changing the existing experience. Additional challenges for mobile devices can use interactions such as scrolling up or down (when selecting past transactions, for instance), swipe, pinch & zoom, and typing on the virtual mobile keyboard. While some applications are launched as 'view only' and have a limited spectrum of interactions, additional functionality is expected for applications over time, allowing entry of information, searching and selecting.

As choices become more available to the user, the risk also increases, but BioCatch automatically matches the greater risk because it gains more interactions to leverage.

Spinning Wheel

A common user interaction element in mobile apps is the spinning selection wheel for dates, time, numbers, etc. This is often used when entering information such as a new destination account for money transactions.

BioCatch collects passive measures related to spinning the wheel (speed, stopping strategy, corrections towards the end), but also introduces subtle fluctuations that help us see how the user subconsciously reacts.



Web-based Biometrics

One of the great advantages of using BioCatch is the ability to support multiple channels with the same approach. The following section relates to how the technology works in a web environment where the interaction is via a PC (ex. online banking conducted via a desktop browser).

Invisible Cognitive Challenges™ (PC)

The BioCatch web authentication solution fully supports online banking and any web/cloud utility that is accessed via a browser on PC or tablet.

It does not require any HW/SW on the user device, and integrates easily into the existing environment using a Java Script on the relevant pages, seamlessly feeding into the Fraud and Risk Management systems for immediate use of gathered data.

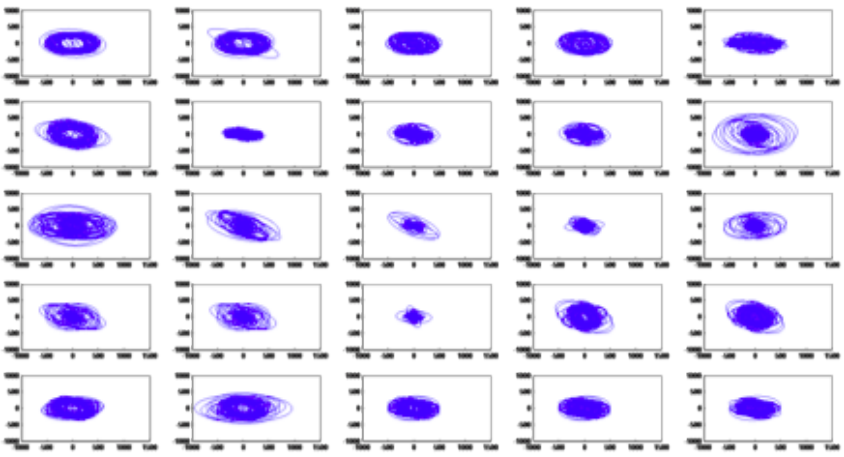
As with mobile applications, BioCatch incorporates invisible challenges for PC as well.

On the PC, our invisible challenges use the **mouse, track pad** and **keyboard interfaces.** There is a growing list of challenges BioCatch is currently researching, and each is analyzed for both contribution to system performance as well as usability (i.e. determine the threshold below which users stop noticing the challenge).

Another challenge for PC is **mouse disappearance.** In this challenge, the cursor is hidden after the user completes a task until the user starts searching for the mouse.

Users search for the cursor in a different ways. Some use wide search patterns, others use small ones, some are horizontal while others are diagonal, and certain users always search counter-clockwise. Sometimes users move on a certain learning curve and their responses vary according to their location on the curve. There are many parameters which usually consider to be unique, such as the curvature of the movement and the relation between right and left movements. Usually the problem with behavioral biometrics is that the analyzer required to “wait” for a long time until the user provides enough relevant mouse movements in order to accurately authenticate him. One of the main benefits of the Invisible Challenge technology is that it unconsciously “force” the user to make many type of mouse movements in a very short time, allowing BioCatch to get after 500ms the same amount of data which usually others could get only after a few minutes of activity.

The system detects all of that. Users don’t necessarily always search in the same way; but out of the many cognitive-behavioral features BioCatch extracts from the user response, some might be both consistent for that individual and distinct from the general population (when combined with other highly consistent features for that person), allowing better detection and lower false positives.



In this picture: 25 users, each with a slightly different search pattern for a missing cursor.

3

MULTIPLE USERS, MULTIPLE DEVICES

Multiple users on same device (e.g. Husband/Wife Situation and Account sharing in subscription based services)

BioCatch supports multiple users per device by approaching the problem in two ways. First, the system identifies that two users share the same device, then it either builds a separate models for each user or, if suspicious, sends an alert to the account's vendor. Note that detection of multiple users may happen in two cases: during initial training or after the model is built for the main user. Our system handles both options – details can be provided upon request.challenges in order to generate a user's identity.

Single user, multiple devices

In the case of a single user accessing multiple devices, BioCatch supports several scenarios:

- Several devices of the same type (ex. a user with 2 different iPads, or with 2 different iPhones).
- Different device types (ex. a user with an iPhone and an iPad).
- Different platforms (ex. a user with an iPhone and a PC)

Assuming the devices are not identical from an interface perspective, BioCatch uses two methodologies:

1. **Identifying** cognitive parameters that are not device-dependent (or platform-dependent) and are based more on cognitive choices, response times, spatial preferences and other device independent parameters.

2. **Classifying** users into groups of people with similar traits. If there are 10 million active users and the granularity of the system is 1:1000, it means the user will be similar to 10,000 other users and the 'cognitive-behavioral peer group'. The chance that a fraudster will be in this group is extremely small (0.1%) - but monitoring how the peer group behaves can tell a lot. For example, if members of the peer group moved from mouse to track pad, or from iPhone to iPad, and BioCatch experiences a very consistent and predictable change in certain parameters for the group, then BioCatch should expect you to experience a similar change if one moves from a mouse to a track pad. In other words, given the user's model, and the group's device change model, BioCatch can predict how a user will change his behavior as he switches to another platform. This can dramatically lower any friction associated to moving between devices.

4

COMBATTING FRAUD

Invisible challenges take our performance well beyond that of passive controls such as keystroke dynamics, password rhythm analysis or mouse/touch tracking. These passive controls either require a comparatively long training period, or offer a much lower detection rate for a given false positive. It has been academically proven that passive behavioral biometrics is also susceptible to certain replay attacks. BioCatch believes that passive controls alone would not provide a sustainable protection against cybercriminals. However, utilizing an approach synthesizing passive and active (invisible challenges) controls offers a remarkably strong security authentication system.

Good Detection at Low False Positives

The False Positive rate (or False Rejection Rate) is configurable by the system so the customer can choose which FP it wishes to work in. This, in turn will influence the detection rate. For example, in a simulated bank transaction experiment we were able to have FP = 1% with a detection rate of 95.3%.
BioCatch has a roadmap for bringing these good results to an even better performance, by using several techniques such as:

- **Common fraudster traits** (ex. high frequency of cut & paste, moving inside the application using shortcuts, and having typical responses to specific proprietary invisible challenges we're researching).
- **Specific fraudster traits** (using a repository of known fraudsters shared by all of our user base):
  -Research into **user classification** (gender, age, culture).
  -Research into **keyboard layout** (differences between regions).
- **Behavioral Traffic analysis** (how the user behaves inside the web page or mobile app page: for example, does the user normally use ENTER to move to next page, does the user check specific pieces of information in the page before doing an activity, etc. This is similar to web traffic behavioral analysis technologies [how the user navigates in the application, time spent per page, anomalous navigational paths] but on a much more granular level as we collect things from the client side, not the network side).

Blacklisting Known Bad Actors

When we receive period fraud files, we go back and 'color' the sessions that were reported as fraudulent, extract behavioral-biometric patterns, and add them to a repository of known fraud personas. This is now available to the whole BioCatch customer base. If an intruder will now attack another bank, the system will be able to tell not only is it not the user, but more so, it is a specific fraudster. We won't know their identity, but we will know their traits, and canalso use some of our coming research to classify them (age, gender, culture, motoric traits [left handed / right handed], etc.).

Preventing Replay Attacks

The BioCatch Challenge-Response mechanism does not only improve biometric performance, but can also prevent replay attacks by constantly measuring the liveliness of the system.

Every biometric company can prevent 100% replays by checking for identical data sets that match 100% with previous sessions for the user (BioCatch does it at well), but it gets trickier when the replay attack is salted with some random noise.
If the fraudster replays previous genuine users activity and adds a little bit of noise, a passive biometric system will fail.

However, BioCatch will detect this type of attack by looking for the typical user response for an injected challenge, which we inject in a controlled manner at a pseudo- random time, intensity and direction. If the fraudster uses feed-forward recoding, it will not be able to imitate a genuine response in the right time and place. The figure below explains this procedure schematically.

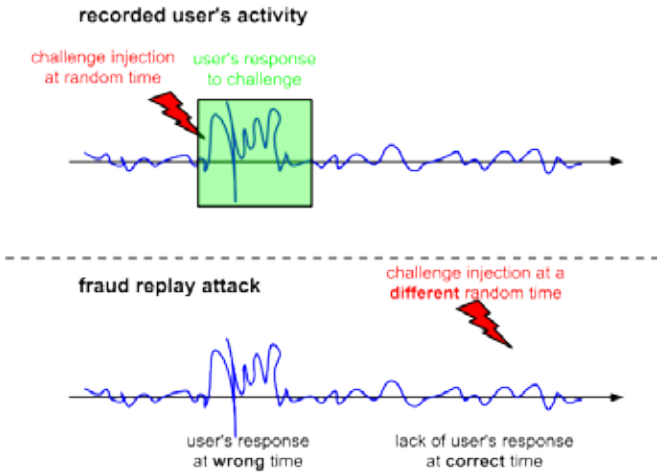


Figure: Schematics of how BioCatch can easily detect replay attack by using active challenge-response mechanism

RAT Catcher

Same-device fraud is a growing concern, and BioCatch developed a unique module for real-time, out-of-the-box detection of same device fraud through remote access attacks. Fraudsters use these RATs in conjunction with regular MITB Trojans to fool device recognition.

RATs, or Remote Administration Tools, are the weapon of choice in state-sponsored attacks and have been successfully deployed against hundreds of global corporations IP geo-location tools protecting online banking and eCommerce. Once installed on a victim's device (PC or mobile), the RAT lets the attacker remotely control it so they can access any application from the actual genuine device.

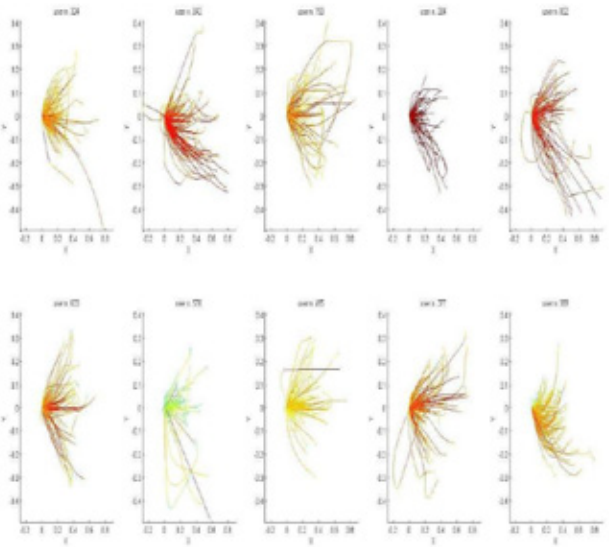
With RAT Catcher, BioCatch can say if the session is remotely controlled, starting from the first session we see for a given user, there is no need to build a profile or wait for a risky activity within the session. It catches Remote Administration Tools using protocols such as VNC/RDP. Please contact us for more information on our RAT Catcher product.

Product Add-Ons

Session Visualizer

This utility allows fraud analysts to visually scan multiple sessions or individual sessions for any distinct or anomalous user interaction patterns. The visualization of user interactions (via mouse/keyboard for PC or touch/accelerometer for mobile) can help the analyst reach valuable insights about genuine or fraud patterns. The tool can compare between a specified user to a random or specific set of additional users in order to see whether the user has similar or distinct traits, and also compare a user session to a random or specific set of previous sessions in order to look for repeating usage patterns or changes over time. The utility can also spot the behind-the-scenes operation of automated scripts as it can show the user never typed information at the time of payment or was occupied by a social engineering screen that was never presented by the bank. There are also non-security uses for the utility (ex. in usability studies, marketing studies etc.).

An example of the visualization is here:



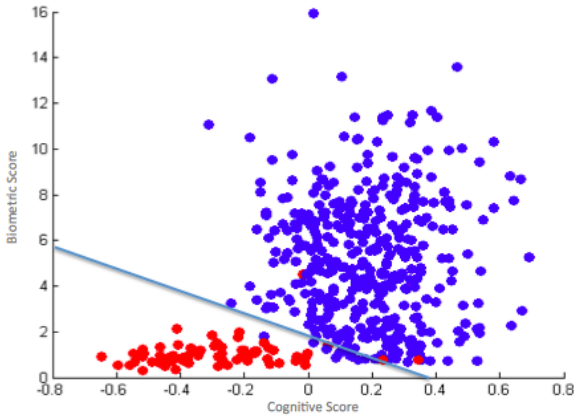
Example: 10 different users across multiple sessions, with only movements to the right isolated, normalized and presented. As seen here, each user has a slightly different speed (green is slow, crimson is very fast). The speed for a given user varies (different colors in a specific user set), sometimes in very particular directions. The overall path shapes are also somewhat different although the tasks are similar. This visualization can help the analysis team come up with new insights about what's going on inside sensitive pages or interactions.
Session Visualizer is currently a prototype. Full development is expected in late 2014.

A Visible Authentication Flavor

Some users prefer a visible authentication method, an easily grasped verification of their account security. At times, visible authentication is required due to the use case (ex. a step-up authentication replacing another control such as OOB text message or KBA question).

Many users have substantiated concerns of identity theft, and an opt-in, visible solution can be marketed as maximal security to this user segment. BioCatch has devised an intuitive, short (<10 seconds) interaction with the user, whereby the user completes a small drag-and-drop puzzle, relaying numerous cognitive and biometric indicators to the system during completion.

Results have been successful: by combining cognitive biometrics (step 1) with behavioral-biometrics (step 2) we can easily differentiate between intruders (shown here in blue) and genuine users (shown here in red).



BioCatch also offers a two-factor layer in which users need to interact with a visible interface that allows them to select digits and form their PIN number (we have several designs - one in which the interface is styled like a combination lock and the user needs to operate and 'unlock' it, and one in which the PIN numbers are scattered and the user drags them to form the PIN).

Users interact with the graphic interface each time they enter the account. Initially, only the PIN is checked, then when sufficient cognitive-behavioral biometric data is collected, the system will start producing biometric scores as a second factor. It will also be possible to offer a self-reset for those who forget their PIN if the biometric score suggests that it is the real user.

SUMMARY

To summarize, BioCatch Invisible Challenges™ technology is the best frictionless and continuous authentication tool for authenticating online users.

With no personal data saved, the Invisible challenges™ are seamlessly integrated into the user's session making his reaction pattern, a single pattern that is unique just to him.

ABOUT BIOCATCH

BioCatch™ is a leading provider of Cognitive Biometrics™ solutions for Mobile and Web applications. Available as a cloud-based solution, BioCatch proactively collects and analyzes more than 400 cognitive parameters to generate a unique user profile. Banks and eCommerce websites and mobile apps use BioCatch to significantly reduce friction associated with risky transactions and protect users against cyber threats, such as Account Takeovers, Man-in-the-Browser (MitB) Malware and Remote Access (RAT) attacks. Additionally, BioCatch provides an enterprise tool that improves the employee authentication experience while protecting access to critical IT assets. The Company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks, eCommerce sites and enterprises across North America, Latin America and Europe. For more information, please visit **www.biocatch.com.**