OneSpan
Be bold. Be secure.

BEHAVIORAL BIOMETRICS: FRICTIONLESS SECURITY IN THE FIGHT AGAINST FRAUD

WHITE PAPER

CONTENTS

Executive Summary

Behavioral biometrics is one of the most disruptive technologies in biometric authentication. It analyzes the way an individual interacts with their device – the angle at which they hold their phone, finger pressure on the keypad, swipe patterns, keystroke dynamics, and more. Analyzing movement patterns rather than a static biological trait such as a fingerprint allows for persistent but completely transparent authentication throughout the banking session.

Due to its non-intrusive nature, financial institutions (FIs) are turning to behavioral biometrics to reduce friction in their authentication flows and strengthen fraud detection. Behavioral biometrics provides a powerful layer of security against both account takeover fraud (known users) and application fraud (unknown users). While the ability to build and leverage a behavioral profile for an existing customer may seem a more obvious use case, behavioral biometrics is increasingly being used to analyze the behavior of new applicants as they navigate an app and enter data. Comparing against the typical behavior of a representative peer group can flag indicators of fraudulent activity. According to Julie Conroy, research director at Aite Group, "The way that somebody enters their data will be very different if it is their data that they are familiar with, versus a fraudster who just bought that data off the Dark Web."

While highly effective, behavioral biometrics is just one option to authenticate users and is by no means a silver bullet. In fact, the best way to leverage behavioral biometrics is to implement it as part of a holistic, layered approach to risk-based authentication. To help customer experience leaders and fraud executives better understand the role of behavioral biometrics, this paper provides an introduction to the technology and explains:

- Use cases in fraud prevention
- How behavioral biometrics improves the mobile authentication experience
- Why a continuous and transparent approach to authentication is more effective than one-time authentication at the beginning of the banking session

The Difference Between Behavioral Biometrics and Behavioral Analysis

Behavioral biometrics technology captures data points that provide insights into how the user interacts with their device (swiping, typing patterns, etc.). Based on this data, it generates a score assessing how well the data matches the user's historical behavior or the behavior of a representative peer group.

When applied to fraud prevention, behavioral analytics considers a much broader context. Apart from data obtained from behavioral biometrics technology, behavioral analysis also takes into account the way the user interacts with the account – what time they usually log in, whether they add new payees at unusual times, what they have done in the past, whether their cross-channel behavior is consistent, etc. All of this data is evaluated to generate a persistent behavioral profile, which is used to assess the risk of fraud. This way, behavioral analysis can even detect unknown fraud scenarios since it relies on the user's typical behavior.

Behavioral analysis, accompanied by other data points like IP or device ID, is one of the pillars of a modern fraud detection solution.

Introduction

In the early stages of digital banking, the types of financial transactions offered online were limited, in large part due to perceived risk. As more customers shifted to online banking, however, they began looking for the ability to transfer funds, obtain loans, and make payments. This inevitably opened new attack vectors for cybercriminals and raised concerns about how to best verify a customer's identity online.

Similarly, the rise of mobile banking created opportunities for growth, but introduced risk. Today, mobile users want to open new accounts and do many of their financial transactions through their banking app. However, consumers generally lack the awareness or capacity to protect their devices from malware. As a result, fraudsters are targeting the mobile channel more aggressively, and financial losses are on the rise. The most recent reports indicate that mobile malware attacks nearly doubled over the past year[1] and mobile phone account takeovers increased 79%.[2]

The Challenges of Authenticating Mobile Customers

Today, the authentication question has changed from "How can financial institutions ensure they are dealing with a legitimate applicant or customer?" to "How can FIs ensure they are dealing with a legitimate applicant or customer – without negatively affecting the user experience?"

In light of the onslaught of data breaches, a password-based approach is no longer an option. Multi-factor authentication (MFA) is a must. FIs can implement secure and user-friendly workflows using a wide array of MFA methods, available as both hardware and software solutions. As FIs further optimize the authentication experience, we see more institutions applying a multi-layered, context-aware approach. This best practice approach leverages MFA as part of intelligent, risk-based workflows, backed by risk analysis that is invisible to the user.

At the same time, FIs face ever-increasing customer expectations with respect to convenience. However, securing mobile devices has its own unique challenges, including:

1. **Risk Associated with Friction:** Users expect a high level of convenience from their banking app. Unnecessary friction in the authentication experience may motivate users to switch financial service providers, considering how frequently the average user logs in to mobile banking.[3]

2. **RIsk Associated with Portable Devices:** Mobile devices are stolen in a matter of seconds; SIM porting and SIM swapping[4] are popular fraud techniques in certain regions. Both result in criminals taking over the phone number the victim used to enroll in mobile banking. How then can a bank determine if a sudden login attempt from a foreign country, in the middle of the night, is in fact coming from the actual account owner?

3. **Risk of Malware:** The status of the mobile device and the context in which it operates can change at any time. Every visit to a new website and every new app download from third-party stores – and, in some cases, from the official stores – carries the risk of inadvertently installing malware. Consumers may not be aware of (or even able to install) the necessary protection measures on their devices. Consumers also connect to unprotected Wi-Fi hotspots, which can be controlled by fraudsters. Such poor device hygiene increases the risk of a mobile phone or tablet being infected with malware or having its mobile data intercepted and altered.

The Need for Transparent and Continuous Customer Authentication

While multi-factor authentication is an essential part of a modern authentication approach, FIs should not impose any additional steps on the user. To better assess the context in which a user is accessing an app or performing a transaction, FIs are turning to technologies that work in the background and remain invisible to the user. Technologies such as risk-based adaptive authentication capture multiple data points and analyze them without affecting user convenience, to determine whether it is, in fact, the legitimate user who is executing the transaction.

In addition, instead of relying only on information from the moment of authentication, best practice is to collect and analyze data in a continuous manner. Just because the FI has positively verified the user's identity at the beginning of a banking session does not mean this cannot change throughout the course of the session. Without continuous assessment, FIs should not assume that the individual who logged in to the application is the same individual requesting a large monetary transaction 10 minutes later. Continuous risk evaluation is essential to delivering optimal mobile banking experience – thus the growing interest in behavioral biometrics.

Behavioral Biometrics in Brief

Biometric authentication uses an individual's unique characteristics to confirm their identity. According to Gartner, "To be useful for authentication (via verification, identification or screening), a biometric trait must be unique, persistent and measurable. Furthermore, it must be possible to capture a sample (image, recording, etc.) of that trait and to extract identifying data (a feature set) in a way that preserves that uniqueness."[5]

Several modalities based on static biological traits, like fingerprint and face identification, are already common in banking authentication flows. These are active forms of biometrics, meaning they require a specific action from the user (e.g., fingerprint scan).

Unlike biometrics based on static biological traits, behavioral biometrics analyzes the user's actions. It measures the way the user interacts with their device to continuously verify their identity. This includes the user's data input, capturing movement within a site or app, and their interaction with the device, such as finger pressure, swipe patterns, and keystroke dynamics.

Behind the scenes, behavioral biometrics then analyzes the user's interactions with the device in comparison to a previously developed user profile or "behavioral fingerprint". In the case of an unknown user (e.g. applying for a new bank account), behavioral biometrics can also compare the user's behavior to what is typical for a wider population.

This analysis results in a score evaluating the probability that the person performing the actions is the legitimate user. The greater the similarity score, the less the organization has to worry about the user's identity and intent. Conversely, a lack of similarity between a user's behaviors in comparison to their profile justifies the application of additional layers of authentication. In essence, the user's behaviors facilitate a risk-based approach that applies authentication commensurate with risk.

The behind-the-scenes aspect explains why behavioral biometrics is often described as passive. As opposed to active methods of authentication, behavioral authentication does not require any additional actions from the user, which improves the banking experience.

> One of the strengths of behavioral biometrics is that it runs continuously; if a session is taken over by a fraudster, it will be detected. This is superior to a solution that only authenticates a consumer one time at the beginning of a session.
>
> **Shirley Inscoe**
> **Aite Group**

> "Active modes are characterized by discrete enrollment processes and distinct verification steps, which require the user's conscious action and intent. Passive modes are characterized by 'invisible' enrollment and evaluation that take place continuously during normal user interactions, typically without the user knowing the profiling and analysis is taking place."[6]
>
> **Gartner**

Behavioral biometrics helps financial institutions remove friction while addressing strict security requirements, and allows FIs to verify a remote user's identity on a continuous basis, regardless of their device, location, or entered data.

According to Aite Group analyst Shirley Inscoe, "Methods such as behavioral biometrics enable FIs to authenticate their customers in a transparent manner with no negative impact to the consumer. This also improves the customer experience, which is a goal of many FIs in addition to preventing fraud."

Behavioral Biometrics in the Context of the Authentication Process

Two factors contributing to the growth of behavioral biometrics are the increasing number of online and mobile banking transactions, and the ever-increasing frequency and sophistication of fraud.

Behavioral biometrics is a discreet way to verify user actions, while shifting the burden of security away from the user. Customers do not notice this layer since it does not require any action on their part. This means that adding behavioral biometrics to the authentication process will not increase the time the user spends on authentication. (The exception would be a scenario where the similarity score is below the acceptable threshold and this, combined with other factors influencing the risk score, triggers the need for step-up authentication.)

While this technology is highly effective, behavioral biometrics is just one option to authenticate users and is by no means a complete solution on its own. In fact, the best way to implement behavioral biometrics is as part of a holistic, layered approach to risk-based authentication. This risk-based approach depends on the context in which a user is accessing an application or performing a transaction. Behavioral biometrics is one component, but a financial institution should also include push messages, biometric parameters, geolocation, and more, as part of their authentication process.

Increasingly, financial institutions recognize that effective authentication is more than just a one-time event. Behavioral biometrics monitors a user's activity in a transparent way throughout the session. This persistent authentication maintains a passive trust value uniquely associated with the individual. Monitoring, and where appropriate, re-authenticating the user during a session, can help stop cybercriminals who have overcome a bank's initial login security measures or inserted themselves during a session (e.g., Man-in-the-Middle). It also contributes to a better user experience, minimizing unnecessary re-authentication.

Behavioral Biometrics as Part of the Broader Behavioral Analysis

Behavioral biometrics technology produces a similarity score based on captured data points. This score, however, should not be used in an isolated context. As part of the broader behavioral analysis, behavioral biometrics offers an excellent opportunity for FIs to enrich their risk analysis with user-specific data captured throughout the banking session. In this context, behavioral biometrics does not compete with static biometrics or other authentication methods; it supplements them.

Behavioral analysis is a much broader concept that entails the use of both the behavioral biometrics scoring and multiple other data points. It creates a behavioral profile of a user and allows for a thorough risk evaluation. This, in turn, helps the risk analytics engine decide whether a particular user action should be allowed, challenged (by requesting additional authentication measures), or blocked. As such, behavioral analytics plays an important role in a layered, contextual, risk-based approach to security, and contributes to a more accurate picture of users and their activity.

Components of Behavioral Analytics

Behavior and interaction with the device: In this layer, the behavioral analysis provides an overview of the user journey and the analysis of the session. Behavioral biometrics is used to assess the navigation behavior in the application and in the device, such as speed of browsing, accuracy of movement, etc.

Interaction with the account: Behavioral analysis can detect deviations from the user's typical behavior by comparing against historical data related to new payees, transaction amounts, time of the login, address changes, and more.

Cross-channel / cross-device behavior: This layer analyzes user behavior across channels, devices, and products.

Server-side analytics: In this layer of behavioral analysis, data is fed to the risk engine to enable analysis of links between different collected data elements, users, groups of users, corporations, and events – using a decision engine and machine learning to power real-time analysis.

> We're seeing a lot of benefits of behavioral biometrics for the new account opening use case. The way that somebody enters their data will be very different, if this is their data that they are familiar with, versus a fraudster who just bought that data off the Dark Web.
>
> **Julie Conroy**
> **Aite Group**

Use Cases: Application Fraud

Data breaches are the primary source of stolen personally identifiable information (PII). Some databases may be limited to email addresses or credit card numbers, but so called "fullz" are also available. "Fullz" is a slang term describing a data record containing a wide range of personal and financial information, like date of birth, address, and social security number. With such detailed PII, fraudsters can both impersonate existing individuals and build synthetic identities. No surprise, therefore, that the growing number of data breaches has a direct impact on the number of fraudulent new account applications.

Behavioral biometrics is one of the technologies FIs are beginning to apply to reduce identity fraud in new account openings. For this use case, no previously captured, user-specific behavioral data exists. Instead, in what is known as population profiling, the algorithm compares a user's behavior to what is labeled as typical good behavior for a peer group or a wider population who have already gone through the same flow, to detect anomalies.

In this use case, the behavioral biometrics module performs several continuous checks during the application process. For example, one of the checks defines how fluently the user navigates through the application (e.g., do they use keyboard shortcuts). If the representative peer group didn't do that, it may indicate a fraudster familiar with the account opening process.

Another check will analyze the way personal data is being entered. If a fraudster has a database of stolen identities, it is probable that they have already filled out the same application multiple times – or are using a script to automate the application form completion. In that case, they may complete the process much faster than the general population.

These checks can be tailored to a specific region and use case. For example, if one region's population doesn't generally use the copy-paste feature to enter their ID number, but the applicant does, behavioral biometrics technology can flag this activity as potential fraud (e.g., a criminal using a database with stolen identities) even if copy-pasting personal details is perfectly normal in other regions.

Another consideration is abandonment rates. If the process is tedious and the additional active checks pile up, the risk of the customer becoming frustrated is high. As Gartner puts it, "onerous identity proofing methods for new-account opening and as part of step-up or multifactor authentication use cases increase customer abandonment. This creates a competitive liability when customer attrition and market share loss exceed the potential fraud loss."[7] At OneSpan, we believe behavioral biometrics can help improve user experience in this case, because it only uses passive measures invisible to the user and these don't slow down the application process.

Use Cases: Account Takeover Fraud

As a component of multi-layered behavioral analytics, behavioral biometrics can help FIs protect customers from becoming victims of account takeover (ATO) fraud.

Similar to the new account opening use case, behavioral biometrics compares the current user behavior to that of a peer group. However, because we are now talking about a known user, behavioral biometrics also performs user-specific anomaly detection by comparing current behavior with historical activity. This way, it helps decrease the number of false positives, because the technology can recognize that a specific behavior may be an anomaly for the peer group, but is perfectly normal for a particular individual.

To help prevent ATO fraud, behavioral analytics should be applied as part of a risk-based security approach. This approach helps detect both known and unknown fraud scenarios in real time – protecting customers and transactions, without any negative impact on the user experience.

According to Aite Group analyst Shirley Inscoe, behavioral biometrics provides FIs with an effective tool to improve their approach to customer authentication, while also combatting account takeover attempts. "Behavioral biometrics scores activity and enables financial institutions to take action when scores indicate suspicious activity. Institutions can define various low and high-risk use cases, adjusting required scores for the level of risk involved," she says. "For example, if a customer is moving funds out of the institution, a higher score can be required than if an account balance is being checked."

Tips for Including Behavioral Biometrics in Your Authentication Mix

- Implement behavioral biometrics as an additional, invisible layer in the authentication journey.
- Use behavioral biometrics together with a risk analytics engine and a mobile security solution to establish trust with the mobile device and create an additional layer of protection.
- No single authentication method is a silver bullet. Be aware of the possibility of false positives and negatives and design your workflows accordingly.
- Define various low and high-risk use cases, adjusting required scores for the level of risk involved.
- Use behavioral scoring during the whole session to detect anomalies as soon as they appear (e.g., a sudden change in typing pattern).
- Leverage data from behavioral biometrics in a broader fraud analysis context.
- Decide which behavioral actions to measure for your use case.

Benefits of Behavioral Biometrics

Behavioral biometrics is one of the most disruptive technologies in identity management. It offers several benefits for FIs, with no negative impact on user experience.

1 Given that it relies on a user's natural actions, behavioral authentication minimizes the time it takes to authenticate a user. Less friction increases the likelihood that customers will use additional digital channel services as they become available.

2 As part of the risk analysis, behavioral biometrics increases the accuracy of risk scoring, enabling FIs to securely roll out services associated with more risk.

3 Behavioral biometrics has sufficient flexibility to optimize the authentication process. It provides a great user experience for genuine users, while at the same time delivering data that can serve as a trigger to step-up the authentication challenge when necessary. For example, if a user tries to log in from a suspicious location, behavioral biometrics can help authenticate the user, removing the need for step-up authentication challenges.

4 Behavioral biometrics can play an active role in mitigating fraud risk. Its similarity score can be used for fraud analysis, acting as one of the data points to determine the risk score of a transaction. This way, it can also help reduce false positives.

5 Behavioral biometrics is available as an easy-to-implement SDK. The technology builds profiles of new customers automatically and in a way that is invisible for the customer, eliminating the need for additional user actions for enrollment.

Additional reasons to consider behavioral biometrics for user authentication:

- Reduced Administration: When deployed in a digital channel, a smoother authentication process reduces the administrative burden associated with accessing and maintaining the user base.
- Cost Savings: Behavioral biometrics does not require any dedicated biometrics hardware.
- Increased Customer Satisfaction: Due to its non-intrusive nature, banking institutions can leverage behavioral biometrics to reduce friction in their authentication flows.
- No Privacy Concerns: Behavioral data converts a user's behavior to a mathematical representation within their profile, which is meaningless to criminals.

Conclusion

Behavioral biometrics is a powerful part of the broader, contextual analysis in fraud prevention. It offers financial institutions an excellent opportunity to enrich their risk analysis with user-specific data. At the same time, it does not require any specific user actions in order to capture the data. By performing continuous, real-time analysis in the background, it ensures a positive banking experience for legitimate users while detecting and stopping fraudsters.

At OneSpan, we understand the unique challenges financial institutions face in fighting digital fraud and optimizing the mobile customer experience. Contact us to learn more about how to include behavioral biometrics as part of a solution that will enhance your authentication flows, help deter application fraud and account takeover, and simplify the digital banking experience for your users.

1. https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies
2. 2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt, Javelin Strategy & Research, March 2019
3. A study from Aite Group shows U.S. adult consumers under the age of 50 are far more likely to pick up their smartphone to complete a digital banking transaction than a desktop, laptop, or tablet: https://www.aitegroup.com/report/winning-over-digital-banking-customer
4. An article explaining the difference between SIM porting and SIM swapping: https://www.letstalk.com/cellphones/guides/port-out-scams
5. Gartner, Technology Insight for Biometric Authentication, Ant Allan, Tricia Phillips, refreshed: 27 November 2018 | Published: 6 September 2017
6. Gartner, Technology Insight for Biometric Authentication, Ant Allan, Tricia Phillips, refreshed: 27 November 2018 | Published: 6 September 2017
7. Gartner, Market Guide for Identity Proofing and Corroboration, Tricia Phillips, et al, 24 April 2018

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to f raud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com