Aite PARTNER. ADVISOR. CATALYST.

Biometrics: The Time Has Come

A custom report excerpt, prepared for:

NU Data Security
A Mastercard Company

TABLE OF CONTENTS

LIST OF FIGURES

IMPACT POINTS

- A wide variety of biometric solutions are in the marketplace today. There is no single solution for every use case. To help organizations make sense of this, Aite Group reviewed RFI responses from 25 different vendors in the biometrics space and had numerous conversations with financial institution leaders to understand priorities.
- Consumers are more comfortable with biometrics than in the past, thanks to innovations from hardware providers such as Apple, Google, and Samsung integrating fingerprint readers and front-facing cameras.
- "Continuous authentication" is closer to becoming a reality by leveraging both physical and behavioral biometrics. This could help reduce account-takeover fraud.
- Financial institutions need to balance usability and security as well as privacy and disclosure to effectively implement biometrics.
- Financial institutions also need to consider model risk management and vendor management when selecting solutions. In many cases, these can be handled proactively through existing processes.
- Organizations need to think carefully about identity proofing and binding when rolling out biometrics to ensure the correct biometric is bound to the correct identity and the correct device.

INTRODUCTION

Just 10 years ago, biometrics were the realm of sci-fi and action movies, and they were certainly not a part of the average person’s daily life. This has all begun to change with the introduction of consumer-oriented biometrics, driven primarily through smartphone adoption. Whereas in the past biometrics required expensive specialized equipment, today many sensors are built into everyday smartphones that support biometric authentication.

Through the advancements in mobile phone technology, consumers are more exposed to biometrics and more accepting of them. This is driven by convenience as much as security; just touching a thumb or looking at a camera is easier and quicker than typing in a code. Consumers have come to embrace this technology and largely accept that their biometrics are unlikely to be stolen or compromised—or at least conclude the risk is worth it for the improved convenience.

The explosion of smartphones and associated sensors has led to biometrics innovations that were pipe dreams a few years ago. Biometrics firms are moving past just fingerprints and facial recognition and are looking into voice, heart rhythms, iris and eye vein scanning, and many more. An opportunity exists to leverage biometric authentication methods in a variety of contexts and to achieve virtually continuous user authentication throughout an interaction.

This report looks broadly at a variety of biometrics capabilities that are being deployed across the globe and a number of vendors supporting biometric authentication.

METHODOLOGY

Aite Group requested information from a variety of vendors and received responses from 25 vendors from March to August 2016. This included both physical and behavioral biometrics providers. Aite Group also interviewed over 10 executives from large financial institutions and payments service providers to understand strategic priorities for financial institutions.

WHAT ARE BIOMETRICS?

The use of biometrics dates back to the second millennium B.C., when fingerprinted seals were used to authenticate documents in ancient Babylon. Beginning in the late 1800s, fingerprints were first utilized to identify criminals.[1] Fingerprints have been a staple of law enforcement investigations for decades, and signatures have been used for centuries as a common, but imperfect, way to authenticate documents.

In modern times, various types of biometric authentication have been featured in action movies and implemented in the real world. While the technology to take advantage of biometric authentication has been available for many years, there are four primary reasons biometrics didn't catch on sooner:

- Earlier versions of fingerprint, facial, and voice biometrics technology had too many false rejects, leaving users frustrated.
- Biometrics have had a "creepy" factor, enhanced by Hollywood depictions of dismembered hands and gouged eyeballs.
- In many cases, specialized and expensive biometrics equipment was required.
- Finally, most users do not understand how biometrics work and may believe a graphic image of their face, eye, fingerprint, or voice recording is actually stored and could be easily misused.

In the last five years, many things have changed. Apple's Touch ID, Google's face unlock, fingerprint-reader support in Android, and face unlock on Microsoft's Surface have brought biometrics into the consumer mainstream in a way past efforts could not. Today, more and more consumers have become accustomed to using a fingerprint or face to unlock their phones and tablets, and the technology has evolved to dramatically reduce false rejects and virtually eliminate false acceptances.[2]

A well-publicized success example comes from USAA's efforts to roll out biometrics to customers.[3] Adoption rates were very high, with over 1 million registered users in less than two years.

Although most consumers are becoming more comfortable with biometrics in daily activities, some people are still suspicious due to common misconceptions about how physical biometrics actually work. Many people believe an actual graphic representation or recording of their fingerprint, face, or voice is captured—and they worry about those things being stolen or replicated. This perception couldn't be further from reality. Biometric authentication relies on a

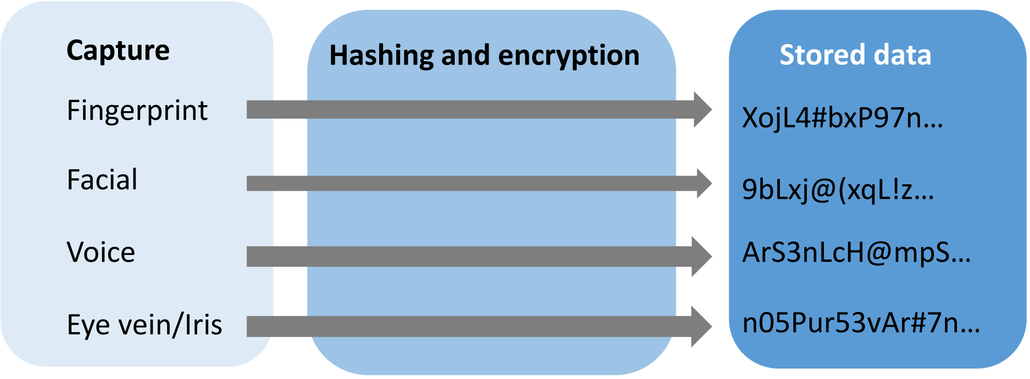
[1] US Marshals Service for Students accessed August 25, 2016, https://www.usmarshals.gov/usmsforkids/fingerprint_history.htm.

[2] See Aite Group's report *Combating Fraud: Consumer Preferences*, January 2017.

[3] "USAA Reaches 1 Million Mobile Biometrics Users," PRWEB, October 2015, accessed September 7, 2016, https://globenewswire.com/news-release/2015/10/15/776613/10152676/en/USAA-Reaches-1-Million-Mobile-Biometrics-Users.html.

mathematical representation of these physical attributes, which would be very challenging to re-create to allow unauthorized access (Figure 1). Yet this misperception is very widespread and still creates a barrier for many consumers in enhancing their security and convenience.

Figure 1: How Biometrics Are Stored



Physical biometrics can not be reverse-engineered based on the hashed/encrypted data that is actually stored on a server

Source: Aite Group

The concern isn't entirely unfounded, but for different reasons. One of the strengths is also a weakness—biometrics are irrevocable. You can't change your fingerprint or face like a password. For example, there are a few proof-of-concept cases in which fingerprints were lifted and re-created to spoof biometrics. In the future, there will certainly be more attempts to bypass biometric authentication, but so far the benefits of biometrics outweigh these edge-case risks, as these attacks are not scalable.

In reality, most people are using something similar to biometrics authentication all the time. When posting photos to popular online sites that match faces in photos to contacts' photos for your convenience, it is hard to tell biometric algorithms are even being used. Because these uses of biometrics are so transparent and "hands free," some consumers and privacy advocates believe we should take a step back and slow down. There is merit in this approach, but we should remember that each of us leaves biometric detritus everywhere we go and in everything we do, from fingerprints to hair samples with DNA to ever-present closed-circuit television (CCTV) and surveillance cameras. When it comes to physical biometrics, there is no avoiding that some biometric identifiers will be left behind in everything we do daily.

Some biometric indicators are completely passive and do not require specific knowledge or action from the user. These behavioral biometrics include keystroke activity and mobile phone use. These approaches offer very low friction to the user and are surprisingly effective. While it seems far out, we each use our mobile devices in pretty unique ways, and mobile devices have an amazing array of sensors: GPS, cameras, accelerometers, gyroscopes, and microphones. Put enough pieces together, and analytics can identify a single user with a high degree of accuracy.

Many contexts require user authentication; thus, there is no single biometrics solution that can solve every use case. Financial institutions will need to evaluate and select biometrics solutions based on a number of parameters, including the following:

- **Usability:** How easy is the solution to use in various contexts and channels?
- **Availability:** How broadly can a solution be deployed across different platforms?
- **Accuracy:** How often does a solution reject real users (false reject rate [FRR]), and how often does a solution falsely accept the wrong user (false acceptance rate [FAR])?
- **Compliance:** How could biometrics improve compliance, and what new compliance or governance concerns may arise, including changes to terms and conditions?

Organizations that think through the costs and benefits of these solutions have an opportunity to roll out more secure and more customer-friendly experiences, often while reducing costs.

BUSINESS BENEFITS OF BIOMETRICS

Biometrics offer financial institutions two distinct benefits:

- **Improved customer experience:** Especially with mobile interactions, biometric authentication is typically faster and easier than other methods, such as one-time passcodes (OTP). This is especially true for mobile-based interactions.
- **Stronger security:** Stronger authentication improves security and helps to reduce risk. In particular, biometric authentication can make it easier to prevent fraudulent activity early in an interaction, reducing both fraud-loss dollars and operational costs of managing fraud.

There are additional benefits, such as enhanced brand image; reduced call center average handle time; and cost take-out from legacy solutions, customer service, and customer acquisition. All of these benefits add up to a strong case for deploying biometrics that financial institutions around the globe have begun to embrace over the last two years.

While these benefits are impressive and make a good case for deploying biometric authentication, it is important to pay attention to the challenges as well. The following two sections highlight a few of the challenges and concerns financial institutions have faced when evaluating and deploying biometrics.

LEGAL AND COMPLIANCE CONSIDERATIONS

As is often the case, biometrics technology is moving faster than the legal and regulatory systems can keep up. In most countries, there is substantial gray area in terms of biometrics, or worse—an attempt to shoehorn biometrics into existing frameworks that are not necessarily appropriate. The challenges can include the following:

- Required disclosures and terms and conditions in different jurisdictions. In some cases, terms and conditions may need to be updated and distributed to customers. This can be complicated, especially in the U.S., by varying state laws and regulations. Some states, such as Texas and Illinois, have passed laws addressing the use of biometrics information. Many others are considering bills that would likely categorize biometrics data as personally identifiable information (PII) and apply the same standards under existing law.[4] There are similar regulations in the European Union (EU).

- Data handling and privacy must be managed much like other personal data, though questions still remain about how and when biometrics data can be stored, used, and shared.

- Vendor management is very important, as many of these technologies are new to regulators, and they seek affirmation that the vendors are of high quality and transparency. This includes model risk management, which can be a challenge with complex intellectual property.

- Firms should consider legal exposure both on the positive side (e.g., providing better security than peer institutions) and on the negative side (e.g., a failure in biometrics authentication could create legal exposure).

Use of biometrics is still relatively early in terms of mass consumer and business adoption, and it takes some time for legal and compliance frameworks to catch up. This is not to suggest the gray area should prevent firms from evaluating and deploying biometrics technology. More so, it suggests that financial institutions should work with governments and regulators to shape laws and regulations that enable strong user security as well as user privacy and data protection. The U.S. government has begun to provide some resources to better understand biometrics and privacy.[5]

ENROLLMENT AND BINDING

Another challenge financial institutions face is ensuring the physical person enrolling a biometric is accurately resolved to the customer record and the device used. This process can generally be described as “enrollment” and includes identity proofing and verification, identity binding, and device binding.

This process can occur during account origination, or it can be a new process for existing customers. Digital channels, in particular, create unique challenges. For example, in a branch, a physical ID can be produced and proofed rather easily right when the biometric is enrolled. This

[4] Sam Castic, Shea G. Leitch, Aravind Swaminathan, and Antony P. Kim, “Biometrics: A Fingerprint for Privacy Compliance, Part I,” March 2016, accessed September 16, 2016, http://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i/.

[5] “Privacy & Biometrics: Building a Conceptual Foundation,” accessed September 16, 2016, http://biometrics.gov/docs/privacy.pdf.

is not the case in a digital channel, and there is a risk—such as in an account takeover—that a criminal's biometric and device identifiers could be bound to a customer record.

Identity proofing and binding are essentially the weakest links in the chain. Using existing authentication capabilities for enrollment means the biometric is really only as strong as the existing authentication process. While this means using biometrics may improve the customer experience significantly, the security advantages of using biometrics become diluted.

Some interesting options are available that enable government-issued IDs and cards to be captured on a smartphone and validated, creating a greater degree of confidence in identity proofing. There are also options to validate a device against known "bad" devices and to validate mobile account ownership with the mobile network operator. Much as with other information changes, customers should be contacted separately to confirm the enrollment.

ACTIVE AND PASSIVE AUTHENTICATION

It is important to note that with current technology, there are more modalities for biometrics authentication than ever before. The sensors we carry with us in our phones and wearable technologies create opportunities for both explicit active authentication and ongoing passive authentication.

As an example, today most organizations authenticate users at certain points in their journey, such as at login and possibly again at the time of a transfer or change of account information. These authentication requests are explicit and create stopping points in the customer journey. This is not necessarily bad—it provides the user with a clear signal that his or her security is being protected. At the same time, passive authentication can provide value in convenience and a more streamlined user experience.

An example use case for passive authentication is shared workstations—ensuring that the correct user is logged in and active and that users aren't sharing logins. It becomes possible to identify behaviors associated with a login and to identify different user behavior patterns associated with the same login. This is especially important in highly regulated industries such as healthcare and financial services. Many passive biometrics are behavior-based and impose little friction on the user but can identify unique and distinct patterns of behavior to identify an individual.

ACTIVE VERSUS PASSIVE BIOMETRICS

There is an important distinction between active and passive biometrics. Active biometrics require some interaction with a user, such as taking a photo or placing a finger on a reader. Passive biometrics act in the background and do not typically require specific actions from the user. While active biometrics require specific interaction from the user, creating friction, that friction can provide a greater sense of security to the user. Passive biometrics, also called behavioral biometrics, have the advantage of reducing or eliminating friction and, in many cases, can provide continuous authentication across many different services.

The following are examples:

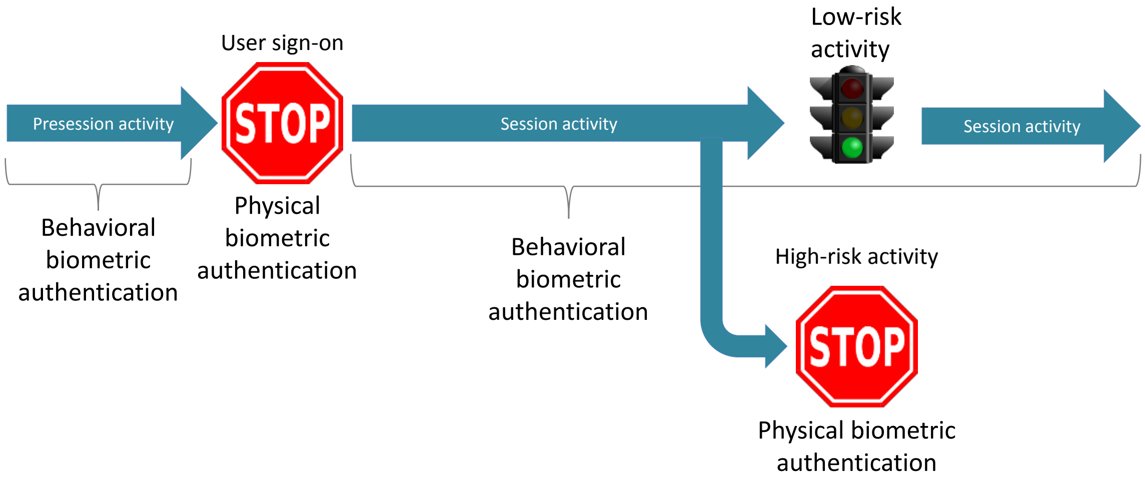
- Facial and eye vein biometrics require the user to be actively involved by snapping a photo and/or blinking their eyes (this provides "liveness" detection, which is difficult to spoof with a photo). This is interactive and is the stopping point in the customer journey.
- Behavioral biometrics, such as mobile device usage patterns and keystroke biometrics, do not require active engagement from the user. Simply comparing usage behaviors while the customer is on his or her journey provides enough information to uniquely identify an individual.

It is important to note that behavioral biometrics do not require active enrollment and bind directly to the device and user. This means there is a small risk that an account-takeover attempt could bind the device and associated behavior with a criminal. Combining both active and passive biometrics offers layers of authentication to mitigate this risk.

CONTINUOUS AUTHENTICATION

A combination of active and passive biometrics offers an authentication environment that can improve both the customer experience and risk mitigation (Figure 2).

Figure 2: Continuous Authentication


User sign-on
Low-risk activity
Presession activity
STOP
Session activity
Session activity
Behavioral biometric authentication
Physical biometric authentication
Behavioral biometric authentication
High-risk activity
STOP
Physical biometric authentication

Source: Aite Group

In this simplified model, authentication is not an event but rather a process throughout the user interaction. There are a few advantages to such a model:

- Behavioral biometrics can start even before login.
- Active authentication challenges can be included to ensure customers "touch and feel" security, while combining multiple methods increases security.
- There is more flexibility in determining authentication risk in different types of interactions.
- Session hijacking can be easier to spot as well as users sharing credentials.
- Many more risk signals can be passed along to enhance transaction risk decision engines.

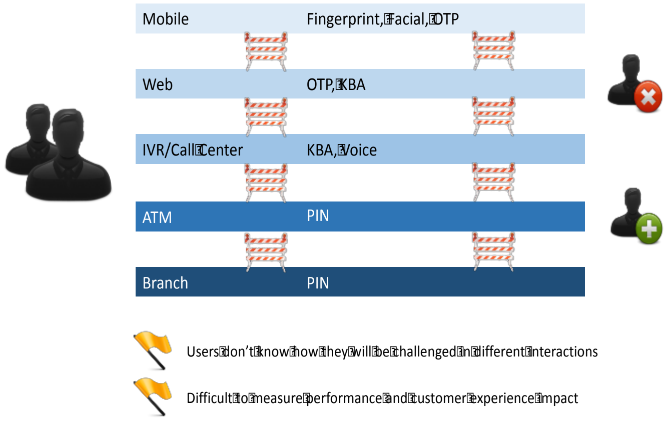
This approach is inherently strategic and requires some thoughtful consideration in terms of vendors, methods, and channels that will be used. There is also an important technology component to coordinate and orchestrate this hybrid authentication approach. To maximize cost savings and minimize technology costs, firms must consider a platform approach. With many disjointed fraud and authentication solutions rolling out to address cybercrime, many organizations have failed to plan early and create a foundation that could support the evolution of cybercrime and incorporate new solutions quickly.

AUTHENTICATION PLATFORMS

It is pretty clear that there are no silver bullets when it comes to authentication. There is no single type of authentication that is effective for all channels, devices, and use cases and no one vendor that can effectively solve every last challenge. Many organizations are faced with silos that lead to a fractured, inconsistent user experiences. These silos also reduce the effectiveness of each individual solution (Figure 3).

Financial institutions need to consider a layer of technology that can integrate various types of authentication and serve them based on risk, channel, and consumer preference. This may be termed middleware, platform, fabric, or any name that connotes the ability to tie disparate application program interfaces (APIs) together.

Figure 3: Common Siloed Approach

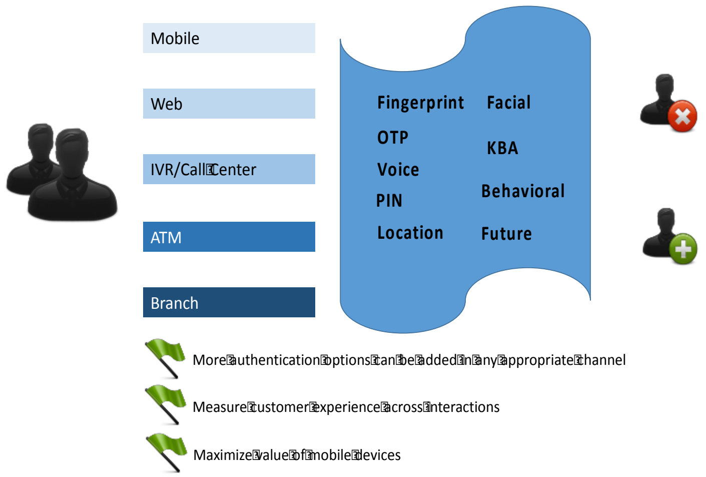

Mobile
Fingerprint, Facial, OTP
Web
OTP, KBA
IVR/Call Center
KBA, Voice
ATM
PIN
Branch
PIN
Users don't know how they will be challenged in different interactions
Difficult to measure performance and customer experience impact

Source: Aite Group 2016

While each individual flow may function reasonably well on its own, there is much to be desired. This becomes very clear when trying to measure authentication effectiveness and customer experience improvements.

A more integrated approach offers a number of advantages. Multiple types of authentication can be deployed based on risk, cost, and customer preference and can be optimized by channel. It can also help enable a smooth multichannel experience for customers when they need to move from a self-service to an assisted channel (Figure 4).

Figure 4: Common Platform Approach


Mobile
Web
IVR/Call Center
ATM
Branch
Fingerprint
Facial
OTP
KBA
Voice
Behavioral
PIN
Location
Future
More authentication options can be added in any appropriate channel
Measure customer experience across interactions
Maximize value of mobile devices

Source: Aite Group 2016

With this approach, authentication methods can be added, removed, and combined, and business logic for authentication can be consolidated and coordinated, and can evolve over time.

Some vendors provide a combination of authentication options based on a platform that allows a financial institution to incorporate and coordinate a variety of authentication options, including biometrics. Utilizing a platform with consistent integration and communication standards can lower costs and improve time to market when adding new authentication options and managing those in place.

These platform approaches can be especially attractive for larger financial institutions with a wide variety of authentication needs across a number of business units and use cases. This can enable risk-based authentication and/or user-directed preferences for authentication.

Some vendors offer flexible platforms as well as authenticators, others focus on specific biometrics identifiers, and many offer an open architecture to leverage in-house products as well as partner products. When evaluating a platform, a key criterion should be open APIs enabling integration to a variety of current and future options.

TECHNOLOGY STANDARDS

Open standards can help accelerate adoption of technology and encourage interoperability. The Fast Identity Online (FIDO) Alliance[6] is working to promote technology standards for identity verification and authentication. There are some advantages for financial institutions in

[6] FIDO Alliance, accessed August 20, 2016, https://fidoalliance.org.

leveraging FIDO Alliance-compliant vendors. This may allow a more "plug and play" architecture that can support multiple vendors and can easily swap in and out vendors as needed.

Some vendors are members of the FIDO Alliance, some conform to the open standards, and others maintain proprietary APIs. There are strengths and weaknesses to each of these approaches, and while conformance to FIDO Alliance standards is valuable, conformance, or lack thereof, should not be the only factor in vendor evaluation.

In the future, there may be additional standards—some interoperable and some that could possibly even rise to the level of an ISO standard.

KEY BIOMETRICS CONSIDERATIONS

Financial institutions face many different constraints when looking to deploy biometrics. Stakeholders are in many departments, including customer service, call center operations, digital channels operations, fraud management, information technology (IT) security, physical security, legal, and compliance.

In particular, choices made during vendor selection and deployment planning and execution can have serious ongoing impacts, for better or for worse.

VENDOR SELECTION

Vendor selection is always challenging, and even more so when capabilities from different vendors do not map one to one. There is no silver bullet solution; the goal should be to identify the solution(s) that can have the greatest impact in the least amount of time and to find the ways in which multiple solutions can be coordinated and maximized.

- Define the objective, use cases, and priorities. It is not possible to solve all authentications for all stakeholders with just one solution. Look for vendors/partners that support near-term priorities and execute on a long-term strategy.
- In some cases, organizations need to apply a number of vendor management practices during selection. Many of the interesting vendors may not “tick all the boxes” from this perspective, but they should still be considered.
- Often, FAR and FRR can only be calculated accurately inside a lab environment.
- Actual real-world performance can vary based on a wide variety of conditions and use cases. It is important to evaluate a variety of real-world examples to understand performance, such as noisy environments and low-light conditions.
- Many vendors allow institutions to tune the balance between FAR and FRR—on their own and/or with vendor guidance.
- In many cases FAR/FRR should not be the primary driving force in making biometrics (or other authentication) decisions.
- There are vast differences among the vendors that provided FAR/FRR information for this report.
- In most cases, some level of technology integration is required to function within an app, website, call center, or other channel. Each vender will have different models, and some will work better than others for a given FI.

DEPLOYMENT

During and following vendor selection, organizations must be cognizant of deployment challenges and the customer experience. Key considerations include the following:

- **Identity proofing and binding:** There must be a way to ensure the biometric being enrolled is bound to the true identity. This could be through actual physical in-person proofing and binding, though this creates a poor user experience that would reduce enrollments. There are alternate strategies online and for self-service such as comparing the photo from a driver's license to a selfie on a mobile device.

- **Revoking and re-enrolling biometrics:** In the relatively unlikely event of a compromise, organizations need to think about how to rescind a biometric binding or to add a new biometric identifier. An everyday example, compared to compromised biometrics, is that users could have a simple problem such as a bandaged finger. Offering multiple biometric identifiers can mitigate this potential challenge.

- **Customer communication and marketing:** In some cases, users need a level of education about biometrics, how biometrics help secure their accounts, and how secure biometrics really are. This also presents a marketing opportunity to highlight an institution's commitment to security and drive enrollment.

- **Employee training:** Employees, working at both the branch and the call center, should be familiar with the deployment, ideally as a part of pre-rollout testing, to help answer basic customer questions. This is particularly important for the enrollment process, which is most likely the point when customers will need assistance.

- **Governance and model risk management:** As with other analytics-based processes, model risk management should be considered from the start, not just when regulators ask for it. Well-prepared vendors should be able to share their experience and documentation.

NUDATA SECURITY OVERVIEW

NuData Security	The solution provides a combination of real-time machine-learning-based predictive analytics, passive behavioral monitoring, and non-PII behavioral intelligence across all NuData clients. The functionality offers behavioral profiling of both "good" behavior and malicious behavior, such as bots or malware. The solution provides capabilities for authentication for existing clients and also ensures new enrollments or originations can be protected from scripted or bot attacks.	The solution offers continuous real-time analysis of behavioral biometrics throughout the user session. By continuously monitoring online user behavior, good and bad users can be identified as early as the first visit. An actionable score is created in real time, leveraging a unique combination of machine-learning and predictive analytics, and a non-PII based behavioral pattern network provides intelligence across the customer base.

CONCLUSION

Biometrics are becoming mainstream, driven at least in part by capabilities included in mass-market mobile devices. At the same time, the accuracy and dependability of biometric algorithms have been improving. While improved security is a key consideration, the convenience and improved customer experience using biometrics is often the primary driver when deploying solutions.

- Financial institutions should be actively considering biometrics solutions if they are not already in place. The mobile channel is a good place to start to maximize customer experience and security.
- While mobile device capabilities have good penetration, many financial institutions and vendors are looking to voice biometrics as a solution that fits with many channels and is mature enough to provide a solid customer experience.
- No single biometric solution is appropriate for every channel and every use case. Firms should consider each channel and use case to identify the right biometrics solutions, where those solutions fit in the customer journey, and whether they support the desired customer experience.
- A platform approach to biometrics, and authentication in general, can be valuable for organizations that seek to implement a comprehensive and cohesive authentication capability.
- Institutions should consider the value of standards, such as those set by the FIDO Alliance, to support interoperability between and among authenticators. Embracing standards can also ease the implementation of new solutions that will likely emerge in the future.
- For most financial institutions, improving the customer experience, especially on mobile devices, is the biggest driver for biometrics solutions, with improved security as a welcome added value.
- Firms should keep in mind that there are opportunities for process improvement when implementing biometrics, which could result in significant savings.
- Such changes require training for internal staff and for customers to reach maximum adoption and customer trust. Branch and call center staff especially need to be trained on the enrollment process to guide customers if they face challenges and to get them over the enrollment hurdle.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT NUDATA SECURITY

NuData Security is an award-winning passive biometrics and behavioral analytics company. Our flagship product, NuDetect, helps companies identify users based on their online interactions - behavior that can't be mimicked or replicated by a third party.

NuData believes good users deserve good online experiences and brands deserve protection against abuse. NuDetect analyzes hundreds of device, location, passive biometric and behavioral signals to build an ongoing digital identity. This analysis informs clients of fraud risk and gives them choices about what actions to take even before the transaction.

NuDetect analyzes nearly 80 billion online interactions yearly. NuData is trusted by some of the largest global brands in the world to verify users with their own natural behaviors and offer a great customer experience.