# 2018 MOBILE BIOMETRICS PLATFORM SCORECARD

NOVEMBER 2018

Licensed by:

OneSpan

JAVELIN

# TABLE OF CONTENTS

# TABLE OF FIGURES

**ABOUT JAVELIN:** Javelin Strategy & Research, a Greenwich Associates LLC company, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and technology providers.

**AUDIENCE:** Financial institutions, credit card issuers, authentication technology providers, mobile banking platform providers, and government regulatory agencies.

**AUTHORS:** Kyle Marchini, Senior Analyst, Fraud Management
Al Pascual, Senior Vice President, Research Director, and Head of Fraud & Security

**CONTRIBUTORS:** Crystal Mendoza, Production Manager
Tyler Brown, Analyst, Digital Banking

**EDITOR:** Mark Stevenson

**PUBLICATION DATE:** November 2018

## OVERVIEW

Five years ago Apple unveiled TouchID, and biometrics quickly took consumer authentication by storm. Today, consumers expect their financial institutions to support fingerprint scanning, but an apparently ever-expanding array of biometric modalities are appearing on consumer devices, ranging from iris scanning to palm geometry. Effectively meeting consumers' demands while protecting them from fraud means not only integrating multiple biometric modalities, but also supporting them with robust risk assessment and ancillary authentication capabilities to secure critical moments like enrollment. This report evaluates twelve of the leading mobile biometric authentication platform providers to assess the capabilities they offer in authenticating customers and the flexibility they provide in adapting to the practical needs of businesses.

## PRIMARY QUESTIONS

- Which mobile biometrics platform vendors offer the widest array of features for addressing current and emerging fraud threats?
- How are the availability of biometric modalities affecting consumer expectations for their experiences at their financial institutions?
- What factors should financial institutions consider and prioritize when selecting a biometrics platform provider?
- What measures do financial institutions need to implement to secure biometric authentication?

# EXECUTIVE SUMMARY

## KEY FINDINGS

**OneSpan takes Best in Class among a competitive group of mobile biometric platform providers.** With a strong performance across all three categories, OneSpan offers a platform that not only provides a robust array of biometric authentication capabilities but also supports those authentication capabilities with risk assessment tools and supplemental authentication and identity verification methods. All this is placed within a flexible platform that can be tailored to the business needs of clients.

**Daon, HYPR, OneSpan, and Transmit Security lead in the "Functional" category.** With broad support for a range of biometric modalities, these platforms provide a one-stop shop for biometric authentication. In addition to upfront authentication, these platforms all provide additional risk assessment and supplemental authentication capabilities to provide robust platforms for securing users' accounts.

**Nuance, OneSpan, Nexsign (Samsung SDS), and Transmit Security distinguished themselves as leaders in the "Innovative" category.** This category rewards platform providers that offer cutting-edge features, whether those are emerging biometric modalities or more advanced analytic tools that operate behind the scenes.

**OneSpan, Transmit Security, and Nuance Communications distinguished themselves as leaders within the "Tailored" category.** This category evaluates how effectively the platform providers are able to configure their product to meet the business needs of their clients. And with exceptionally flexible platforms, these three vendors offer a variety of configurable implementation options, supported by professional services arrangements to help adapt the authentication platform to the needs of clients and end users.

**Demand for biometrics outstrips adoption at financial services.** While support for fingerprint biometric authentication is essentially ubiquitous at the largest financial institutions in the U.S., support for facial recognition is largely limited to Face ID integrations.

**Biometric hardware is growing more sophisticated.** Apple's Face ID marked a major step forward for facial recognition hardware. Rather than relying solely on the forward-facing camera, the iPhone X uses an infrared camera to develop a three-dimensional model of the user's face, making it more resistant to spoofing with pictures or video. Outside the U.S., fingerprint sensors embedded behind the smartphone touchscreen are beginning to make their debut, raising the possibility of fully passive fingerprint authentication from a touch anywhere on the screen.

**New biometric modalities are on the horizon.** In addition to the core biometric modalities of fingerprint, face, and voice, vendors are experimenting with newer modalities, such as eye and palm. Iris scanning still requires specialized hardware found on only a few consumer devices, but palm scanning uses just the smartphone or tablet's integrated cameras, enabling it to immediately function for most users and compete in the same space as facial recognition.

**Consumers demand authentication choice.** For more than a third of users, the three authentication options they most strongly want their financial institutions to support are all biometric modalities. While one would expect this to be concentrated in younger, tech-savvy users, consumers who want biometric choice tend to be older, with around 40% being over age 55. Since offering multiple biometric modalities enables users to choose the authentication method that is best suited to the moment, it can appeal to users who are sensitive to the quality of their digital interactions.

**Fraud intelligence sharing has a valuable but limited place in biometric authentication.** Sharing data on identified cases of fraud across institutions can help piece together networks of malicious actors and fraudulent accounts. However, this works well only for biometric modalities that already use server-side authentication, such as voice biometrics in the call center.

**WebAuthn/FIDO2 brings authentication parity to the browser.** While biometrics have made massive strides in user adoption on mobile devices, online banking through laptop and desktop browsers still has a long way to go when it comes to support for strong authentication. The reliance on authenticators with well-known vulnerabilities such as SMS one-time passwords is unsettling when juxtaposed against the reality that the most risky banking activities — large transfers, new account opening, etc. — all continue to be done predominantly through the browser. Fortunately, the release of the WebAuthn/FIDO2 standard goes a long way toward closing that gap. This standard provides a consistent API for use across most major browsers for reliant parties to request strong authentication using methods such as on-device biometrics or hardware cryptographic keys (e.g., YubiKey) and is supported by a growing use of biometrics on laptops and desktops through services such as Windows Hello and integrated Touch ID sensors on high-end Mac devices.

## RECOMMENDATIONS

**Expand support for biometric modalities.** Moving beyond fingerprint and Face ID to support other modalities such as face on non-iOS devices, eye, and voice gives users the ability to choose the authentication method that is easiest for them in a given circumstance or that they feel to be the most secure. This also provides the option for multimodal biometric authentication for step-up (e.g., simultaneously authenticating with voice and facial recognition), which provides much stronger assurance than a single modality.

**Use local template storage when possible.** Storing biometric templates locally on the device reduces risk associated with data compromise, either in transit or through malicious actors' targeting a centralized store of biometric data. When coupled with authentication standards, such as those developed by the FIDO Alliance, local biometric authentication is nearly impossible to phish or misuse intercepted data.

**Controlling risk around enrollment is crucial to providing confidence around ongoing authentication attempts.** If a malicious individual is able to successfully enroll his own characteristics into a biometric authenticator, then even the most sophisticated authentication method will still allow him to pass through security challenges. Consequently, many

providers offer additional risk assessment tools built into their platform, such as device fingerprinting and geolocation. Other tools, such as document scanning, offer natural supplements to biometric authentication, which enables a degree of comparison between the user's captured biometric input and the image on an identification document.

**Look for authentication providers that enable independent adjustment of sensitivity.** One of the unique aspects of biometrics compared with other authentication methods is that the sensitivity of the authenticator can be fine-tuned to match the level of assurance needed and how concerned the authenticating organization is about false-positive declines.

**Move beyond biometrics on mobile.** With the release of FIDO2/WebAuthn, three of the four major browsers (Edge, Chrome, and Firefox) have the capability to support native biometric authentication on laptops, along with other FIDO authenticators. This is a major step forward in bringing biometric authentication to a wider array of devices than just smartphones and tablets.

# BIOMETRICS CONTINUE TO GAIN STEAM

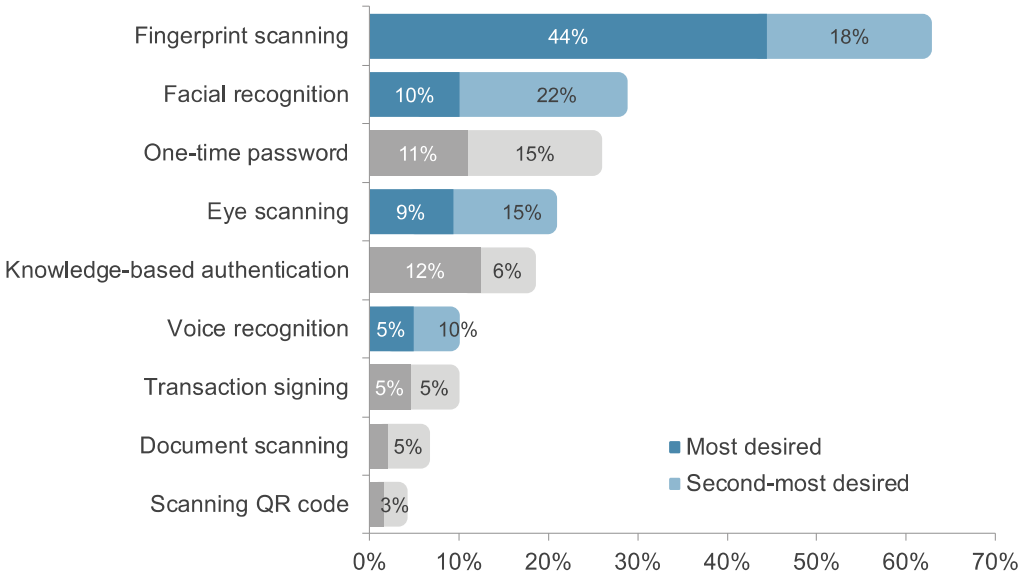
Led by Touch ID, biometrics integrated in mobile devices has familiarized consumers with the action of authenticating with their physical characteristics. With seamless integration into mobile operating systems and applications, support for biometric authentication has become commonplace among consumers.

Consequently, it should be no surprise that three of the top four most desired authentication features for online and mobile banking are biometric modalities. Fingerprint scanning has become an uncontested favorite for consumer authentication, with 62% of consumers selecting it as either their most preferred or second-most preferred authentication method for logging into their financial accounts. What is perhaps more surprising is that facial recognition and eye scanning both also come in the top four, with 32% and 24% of consumers desiring these authentication methods (Figure 1).

Given the current proliferation of mobile biometric technologies, it's easy to forget that Touch ID, the first consumer biometric method to make a mainstream splash, was released just five years ago, in 2013. While fingerprint authentication is still consumers' preferred biometric modality, other modalities are proliferating as consumer devices come equipped with an increasing array of sensors. Fingerprint, face, and voice biometrics are already familiar to many consumers, but that doesn't mean there isn't room for innovation in each of these modalities.

**Biometrics Top Most Desired Authentication at FIs**

Figure 1: Most Desired Authentication Methods for Online or Mobile Banking




Source: Javelin Strategy & Research, 2018

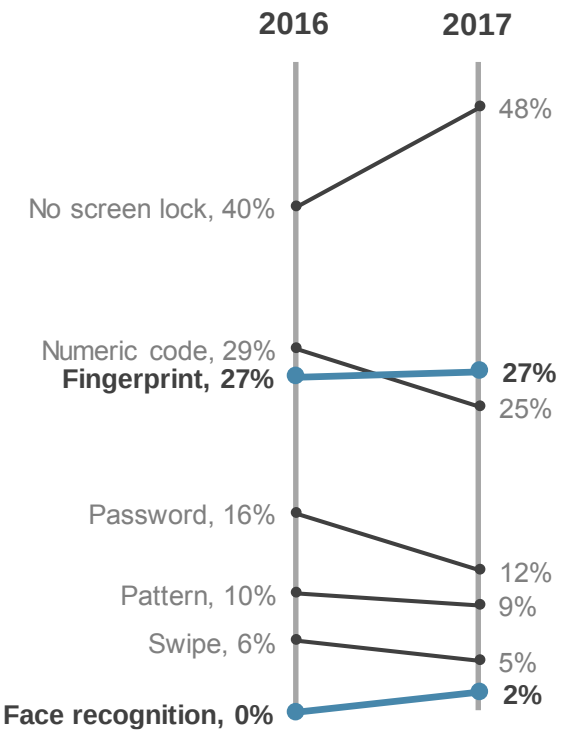
The major change that is impending with fingerprint scanning is the ability to ditch visible sensors embedded in the home button or rear of the phone and conceal the fingerprint reader behind the touchscreen — expanding available screen space and providing a cleaner look that is popular with premium phones such as the iPhone X. No U.S. devices currently support this capability, but it is available on some devices outside the U.S. market such as the Vivo NEX[1] and OnePlus 6T[2], and the upcoming Samsung Galaxy S10 is rumored to use the same technology. Embedding fingerprint readers behind the device touchscreen is one step closer to fully passive fingerprint biometrics that is able to authenticate individuals who are interacting with the screen without requiring a specific authentication gesture.

Face ID similarly represents a major step forward for facial recognition, in terms of both the accuracy of the identification and the user experience. Rather than simply relying on the image captured from a forward-facing camera, the Face ID sensors built into the iPhone X project a grid of around 30,000 infrared dots onto the user's face that are invisible to the naked eye and then use a dedicated infrared camera to create a three-dimensional model of the user's face. This makes Face ID notably more precise and resilient to spoofing than solely camera -based approaches.

Just as important for the user experience, the hardware integrated into the iPhone X does not require a particularly precise angle for authentication, which enables Face ID to operate passively, without requiring users to align their image with the facial recognition frame. This minimizes visual disruption to users' activities while they authenticate and may placate some users who are put off by having to stare at their own image while scanning their face. This development is crucial in ensuring facial recognition's future as another standard biometric modality, potentially even supplanting fingerprint if this kind of hardware becomes widely available.

**Fingerprint Rises to Most Prevalent Screen Lock Method**

Figure 2: Screen Lock Methods on Consumers' Primary Smartphone




Source: Javelin Strategy & Research, 2018

Eye scanning exists in a few different forms. Eye vein scanning is compatible with most forward-facing smartphone cameras but has seen limited adoption among consumers or enterprises. Iris scanning offers somewhat more assurance than eye vein scanning but requires more specialized hardware. To capture the detail necessary for iris scanning, the device must be equipped with a diode that emits a burst of near-infrared light that is invisible to the individual authenticating but provides additional color contrast for the camera.

This makes iris scanning somewhat less sensitive to environmental conditions than facial recognition, though the user experience is very similar.

Despite the limited availability of eye scanning in either form, this biometric modality enjoys a surprising degree of support from consumers, with 24% of banked consumers identifying it as one of the top two authentication methods they would like their financial institution to offer (Figure 1).

Palm geometry is the latest biometric method to make its debut. Using her smartphone's camera, the user captures an image of her hand, which is then compared against a template based on the hand's geometry. Since this modality relies on the availability of an integrated camera on the user's smartphone, it is immediately compatible with nearly every smartphone on the market. However, it is not clear just how much of an advantage this modality offers over other biometric modalities. Since it requires the user to make a more significant gesture to authenticate herself, palm biometrics is unlikely to unseat fingerprint scanning.

The most plausible space for palm biometrics is as a replacement for facial recognition on devices that do not support fingerprint readers. The gestures required to authenticate with each method are comparable, but palm scanning may appeal to users who feel self-conscious about taking a selfie to authenticate.

## THE ROLE OF MOBILE OPERATING SYSTEMS

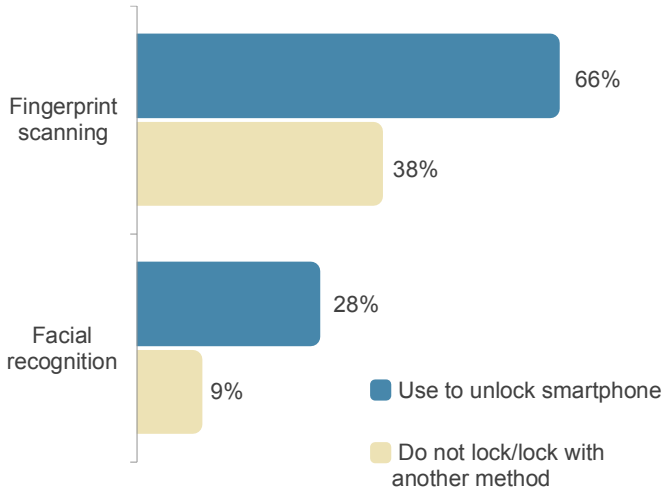
The importance of biometrics in screen locks should not be understated. Users who repeatedly authenticate themselves with the same method become accustomed to the mechanics of that method and tend to have a higher assessment of its security, which translates to the type of authentication methods they would like to see built into the mobile services of other organizations.

Amid a general decline in the use of screen locks on consumer smartphones, the two main integrated biometric modalities were the only authentication methods to increase in usage from 2016 to 2017. With a quarter of smartphone owners using their fingerprints to unlock their smartphone, this modality surpassed numeric PINs as the most prevalent smartphone screen lock method. Unfortunately, in spite of the boost offered by Apple's Face ID and widespread availability on Android devices, facial recognition has still struggled to gain traction, lingering at the bottom of the list.

Consumers who use biometric modalities to unlock their smartphone are significantly more likely to desire their financial institution to offer these same modalities. Consumers who unlock their smartphone with facial recognition are three times as likely to say that facial recognition is the authentication method they would most like their financial institution to offer, 28% compared with 9% of consumers who do not use facial recognition on their smartphone (Figure 3).

**Lock Screen Methods Strongly Influence Authentication Preferences**

Figure 3: Most Desired Authentication Feature, by Method Used to Unlock Smartphone




Source: Javelin Strategy & Research, 2018

## WEBAUTHN, FIDO2, AND BIOMETRICS IN THE BROWSER

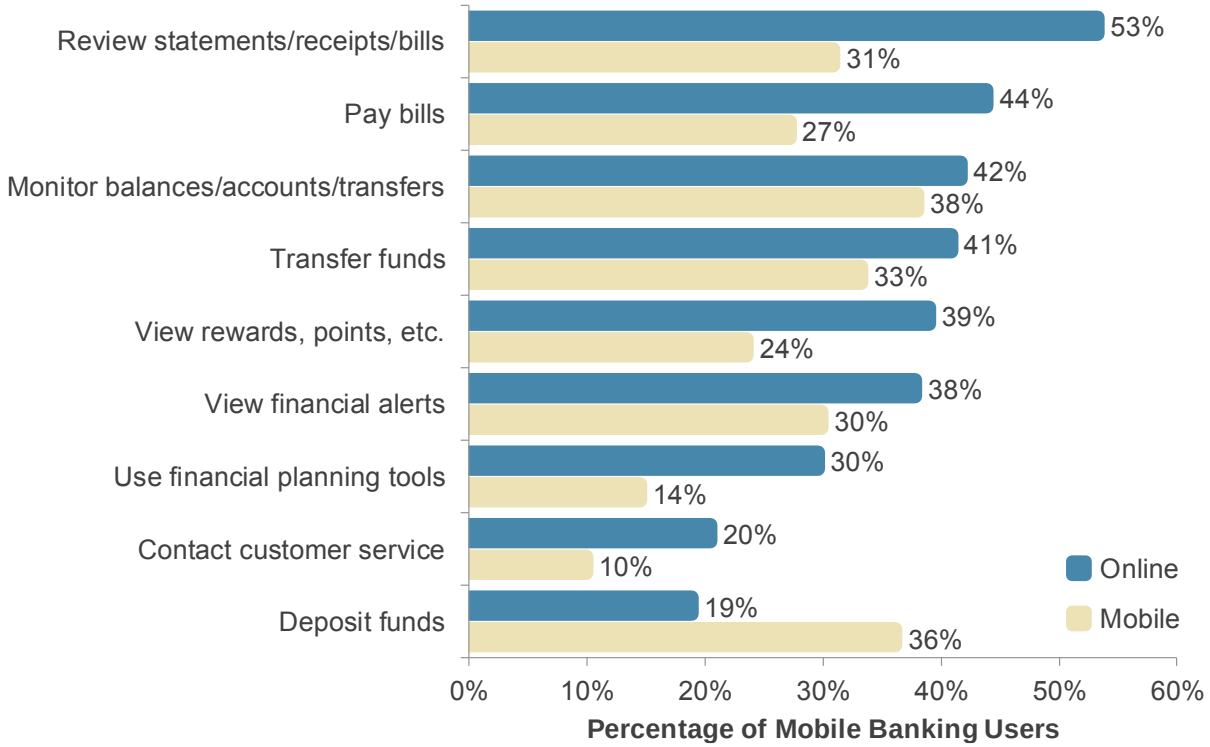
For a long time, there has been a disconnect between the level of risk and authentication assurance between banking channels. Online banking continues to be the preferred channel for many higher-risk banking activities, such as opening new accounts. Even among regular users of mobile banking, 44% report that they prefer online banking for paying bills and 41% prefer online banking for transferring funds (Figure 4). Conversely, mobile banking tends to be used for high-frequency, low-risk activities such as monitoring balances and recent transactions, although services such as P2P payments are increasing the risk associated with mobile banking.

At the same time, high-assurance authentication methods tend to be concentrated on mobile devices, with greater availability of biometric sensors, stronger isolation of apps, and more robust device binding capabilities than are widely available for laptop or desktop computers.

While biometric authentication is principally associated with mobile devices, that will soon be changing. Laptops have long had similar biometric capabilities to smartphones, with fingerprint readers built into many models of prominent brands and forward-facing cameras that could plausibly support facial recognition. However, these were limited by a couple factors:

**Online Banking Remains the Preferred Channel for Higher-Risk Activities**

Figure 4: Preferred Channel for Banking Activities Among Mobile Banking Users (Past 30 Days)




Source: Javelin Strategy & Research, 2018

First, compared with mobile biometrics, which gained near-immediate acceptance in part due to the convenient placement of biometric sensors, fingerprint sensors on laptops tend to more awkward to use, requiring the user to move his hand away from the keyboard or mouse to swipe a finger.

More important from a business perspective, there was no standardized protocol to intermediate enterprises and devices for web authentication requests. Consequently, laptop biometrics were largely limited to supporting on-device keychains that could store credentials (typically usernames and passwords) for use online.

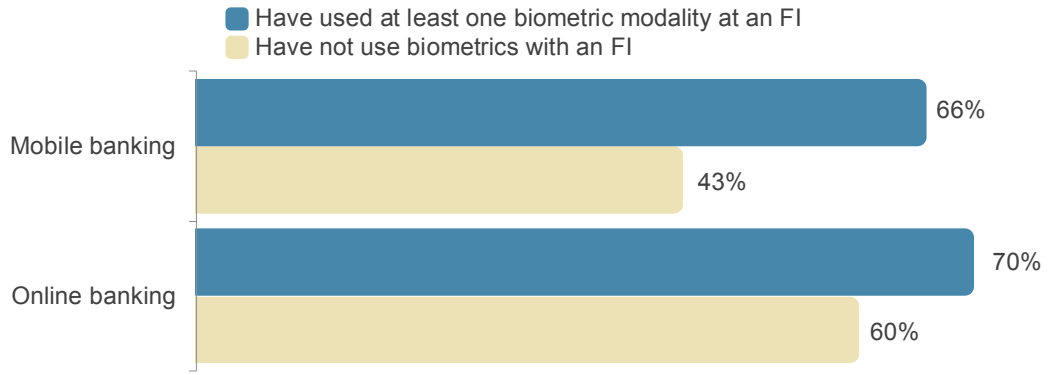
Earlier this year, FIDO and the W3C released FIDO2/WebAuthn, an API for handling cryptographically backed authentication requests within the browser. Using this API, enterprises can leverage strong authenticators, such as on-device biometrics or cryptographic keys on a standalone device such as a YubiKey or stored in an on-device trusted execution environment (TEE).

While the protocol is only months old, early indications are promising. Microsoft, Mozilla, and Google have all committed to supporting the initiative in their browsers, though Apple has remained silent on whether or when it will integrate support into Safari. With biometric authentication featuring prominently in Windows 10 with Windows Hello and Touch ID integrated into the highest-end versions of Apple's MacBook Pro line, users can expect to have biometric authentication used more regularly on their laptops.

Despite the wider availability of strong authentication on mobile, online banking enjoys a strong edge in perceived security among consumers, likely due to greater familiarity. The good news is providing biometric options for authentication can improve account holders' opinions of the security of both channels, with use of biometrics making a particularly great difference in the perceived security of mobile banking. Consumers who have used at least one biometric modality are about 50% more likely to believe mobile banking is secure, compared with those who have not — 66% to 43% (Figure 5).

### Biometrics Improve Perceived Security of Online and Mobile Banking

Figure 5: Perceived Security of Online and Mobile Banking, by Use of Biometrics




Source: Javelin Strategy & Research, 2018

# AUTHENTICATION CHOICE

With heightened consumer desire for biometric authentication, simply supporting Touch ID or other integrated biometric authenticators is not enough. A growing group of consumers is demanding multiple biometric authenticators.

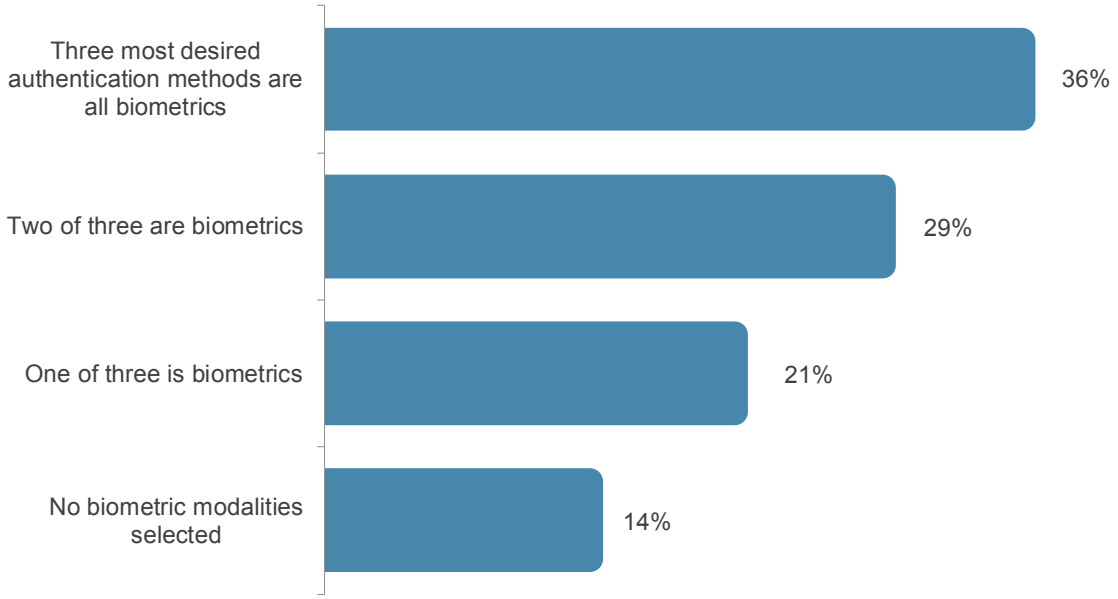
When selecting the three preferred authentication methods they would like to see at their primary financial institution, consumers were strongly drawn toward biometrics. In fact, for 36% of consumers, the three most highly desired authentication methods were all biometric modalities. Only 14% of consumers selected no biometric modalities in their most desired authentication methods (Figure 6).

Contrary to expectations, this group of consumers tends to be somewhat older, with more than two-thirds of consumers older than 65 identifying at least two biometric modalities in their three most desired authentication methods. Ironically, consumers between ages 18 and 24 tend to be the segment least inclined to value multiple biometric modalities, with only 55% doing so (Figure 7).

This apparent anomaly can be fairly easily explained by the increased accessibility that multiple biometric modalities offer. With different biometric methods being suited to different environments and device types, having several different authentication methods available to users

**More than Half of Consumers Want Multiple Biometric Modalities**

Figure 6: Number of Biometric Modalities in Three Most Preferred Authentication Methods

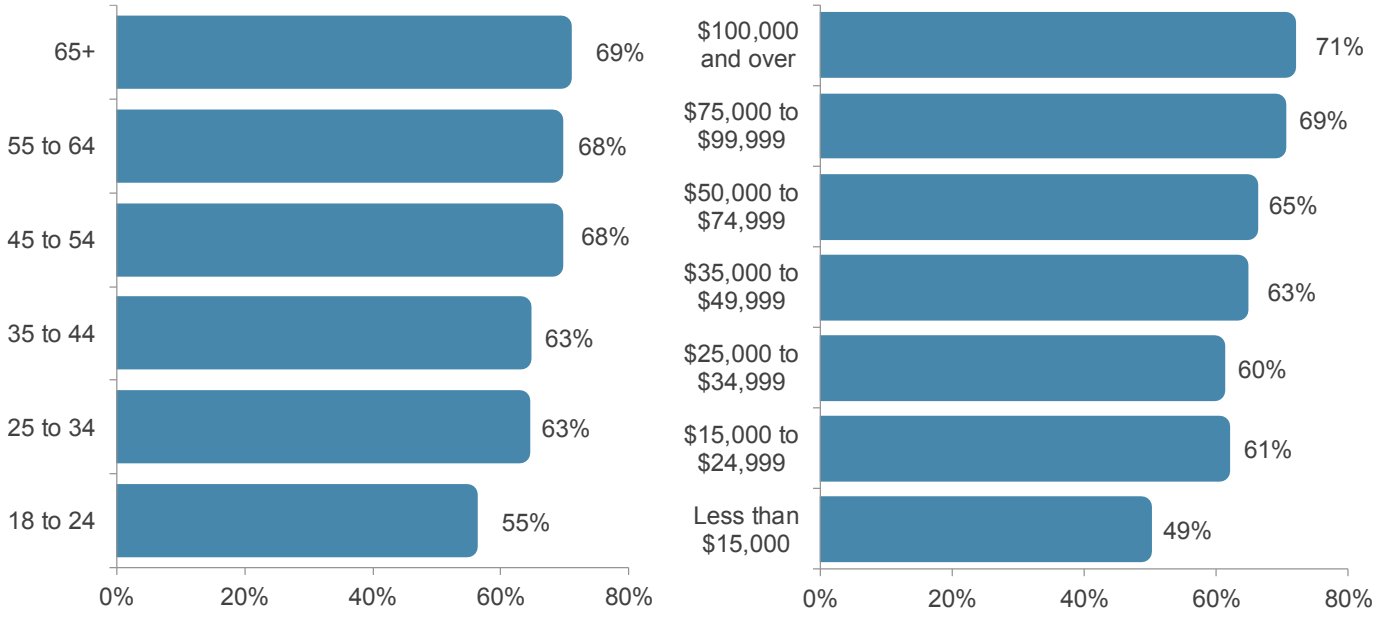



Source: Javelin Strategy & Research, 2018

enables them to select the authentication method that is easiest to use when attempting to access their account given the circumstances. This can also appeal to users who may have a difficult time entering one-time passwords or correctly answering dynamic challenge questions.

**Consumers Who Want Multiple Biometric Modalities Tend to be Older, Affluent**

Figure 7: Demographic Profiles of Consumers Who Value Multiple Biometric Modalities




Source: Javelin Strategy & Research, 2018

## DIGITAL IDENTITY AND BIOMETRICS

Digital identity platforms provide a single independent authentication service that users can sign up for to authenticate themselves into any of their accounts that support the platform. From the user's experience, this provides a familiar authentication experience across multiple organizations that may or may not support the users' favored authentication method on their own.

FIS and Equifax have launched OnlyID, a digital identity product aimed at financial institutions within the U.S. This product enables participating FIs to offer their users the ability to log in with OnlyID once they have enrolled in the service. By combining the insights of the participating financial institution, with device risk indicators and FIS and Equifax's consumer data, the service is able to form a more robust profile of the user than any single organization is able to.

Integrating with digital identity platforms can be especially valuable for smaller institutions that do not have the budget or technical acumen to offer more sophisticated authentication methods on their own. Allowing users to log in with a digital identity service enables immediate support for all of the authentication methods offered by the service, lowering the bar for access to a variety of biometric modalities.

Right now, OnlyID works only for logins, but other providers are exploring the use of digital identity within account opening. Capital One's DevExchange offers the "Sign Up with Capital One" and "Verify with Capital One" APIs, which provide other organizations with the ability to allow their customers to use Capital One credentials to authorize the sharing of relevant identity data or to verify hashed identity attributes.

Should digital identity schemes gain widespread use among consumers, this use case has the potential to notably simplify the application and identity verification process. Users who are enrolled with the service could have their basic PII essentially autofilled in the application, streamlining the user experience especially for mobile account opening. The organization opening the account can take advantage of the user's history with the digital identity service, gaining insights into device reputation and user behavior that can typically be gleaned only well after the account has been opened.

However, digital identity is not without risks. By virtue of providing access to a wide network of consumer accounts, the digital identity services make valuable targets for fraudsters. A compromised account with a digital identity service can open doors at any participating organization. Additionally, financial institutions have reason to be wary about passing the authentication experience to a secondary branded service. Consumers place a high degree of trust in the security measures put in place by their financial institutions and may not have as much confidence in a third-party service.

## BIOMETRICS IN THE IOT?

The "internet of things" has the potential to revolutionize financial services by dramatically expanding the opportunities for engagement with customers. However, one of the major limiting factors for expanding financial services into the internet of things is the lackluster authentication options currently available.

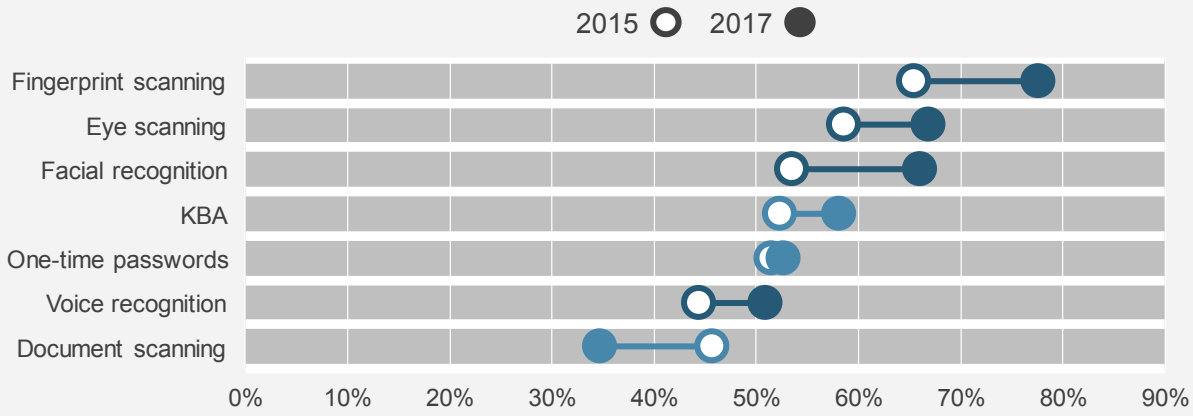
Certain biometric modalities are obvious fits for the internet of things. When a user is interacting with a virtual home assistant, for instance, voice recognition keeps authentication nearly invisible and eliminates the need for verbal passwords or PINs, which are clunky and easily guessed or overheard. However, while assistants have been able to distinguish between the voices of different users to associate them with particular accounts, this has not been extended into the realm of authentication yet.

Unfortunately, that means the strongest authentication methods for the internet of things are still out-of-band — occurring on users' smartphones, rather than on the device where the activity was initiated. Because out-of-band authentication methods necessarily add additional friction in requiring the user to interact with multiple devices, particular care should be taken in the authentication methods selected for these use cases, making biometrics an easy choice.

The growing availability of biometrics appears to be having an impact on consumers' perception of the ease of use of verifying their identity with these methods. While perceived ease of use increased from 2015 for every authentication method covered except for document scanning, biometric modalities clearly outstripped the competition, with fingerprint, eye, and facial biometrics maintaining a significant lead over knowledge-based authentication, which ranked fourth.

**Biometric Modalities Pull Ahead of Other Authentication Methods in Ease of Use**

Figure 8: Ease of Use of Authentication Methods, 2015-17




Source: Javelin Strategy & Research, 2018

# SCORECARD RESULTS

## THE VALUE OF BIOMETRIC PLATFORMS

Many of the providers evaluated within this scorecard can be seen as full authentication platforms with biometrics at the heart, and the scorecard is designed to emphasize the importance of having a full-featured product. Consequently, the criteria emphasize support for multiple biometric modalities across a variety of channels and reward platform providers that back up those biometric authenticators with additional data sources and authentication methods to secure the crucial enrollment step.

The expanding array of banking touchpoints — smartphones, tablets, smart home devices, and more — coupled with consumers' growing desire for choice in their authentication methods increases the value of using a full authentication platform. The alternative, piecing together technologies from multiple vendors in-house, is logistically challenging, costly, and can open organizations up to vulnerability if they do not effectively ingest all the input provided by different authenticators offered by different providers. This is not to say that some organizations cannot build effective in-house platforms using the products of multiple authentication providers but merely that it is a significantly more challenging process with plenty of room for error.

Leveraging multiple authentication methods requires them to be orchestrated effectively, with an analytics engine that can ingest the data provided by each authenticator, assess the risk associated with a particular event, and deploy the most effective and customer-friendly step-up authentication method in the event that additional verification is needed.

Strong supporting infrastructure in the form of integrated case managers, reporting, and analytics is crucial not only for minimizing operational costs associated with managing the platform but also for reducing vulnerability. Today's fraudsters frequently move across channels, perhaps beginning their attack with a password reset through the call center, then moving to online banking to cash out the account. Detecting and stopping these kinds of attacks requires authentication platforms that can have visibility into users' behavior across channels.

## JAVELIN'S FIT MODEL

To evaluate each biometric platform provider, Javelin uses the Functional, Innovative, Tailored model. This model recognizes that for financial services companies, the decision of which vendor to integrate with depends not just on its capabilities related to solving the business problem of the day but also how well the product is positioned to provide long-term value and how difficult and expensive integrating with the product will be. Accordingly, the FIT model aims to provide a holistic view of the capabilities of vendors' products both within the context of the problem being addressed and in providing flexible integration with customer systems.

1. **Functional:** Criteria within this category capture features related to solving a particular business problem. Within the context of mobile biometric acceptance, this encompasses the capabilities the product offers to support various biometric modalities, assess risk around authentication events, and provide supplemental identity verification features to provide additional security around enrollment and other key moments of the customer life cycle.

2. **Innovative:** As customer expectations and fraud tactics continue to evolve within financial services, authentication platforms must incorporate cutting-edge features to retain relevance. This category covers leading features crucial to fighting fraudsters and serving customers in the world of modern finance.
3. **Tailored:** Long and costly integrations minimize the return on investment from even a very capable product. Accordingly, this category addresses how flexible the solution is in accommodating the business needs of clients.

## 2018 MOBILE BIOMETRICS PLATFORM AWARD

BEST IN CLASS

# OneSpan


### BEST IN CLASS: ONESPAN

OneSpan takes Best in Class among a competitive group of mobile biometric platform providers. With a strong performance across all three categories, OneSpan offers a platform that not only provides a robust array of biometric authentication capabilities but also supports those authentication capabilities with risk assessment tools and supplemental authentication and identity verification methods. All this is placed within a flexible platform that can be tailored to the business needs of clients.

# FUNCTIONAL

As financial services expand into new devices and types of services, biometrics authentication platforms are asked to fit into a wide number of use cases. The functional category covers the breadth of functionality within each platform, including the biometric modalities offered, channels supported, and any supporting technologies and analytics built into the platforms. Daon, HYPR, OneSpan, and Transmit Security lead in the Functional category with broad support for a range of biometric modalities supported by additional risk assessment or supplemental authentication capabilities to provide robust platforms for securing users' accounts.

| FUNCTIONAL | |
|---|---|
| Leaders* | Daon |
| | HYPR |
| | OneSpan |
| | Transmit |
| Contenders | Entrust Datacard |
| | Gemalto |
| | Nok Nok Labs |
| Followers | Nexsign (Samsung SDS) |
| | Nuance Communications |
| | Sensory |
| Laggards | Aware |
| | RSA |

* Vendors in each category are listed alphabetically

* Leaders category expanded due to a tie

## TEMPLATE STORAGE

With any biometric modality, one of the most critical decisions is how to handle the biometric data and templates. Insecure processing and storage risk significant privacy violations, exposing consumers' immutable physical characteristics, which can undermine the effectiveness of future authentication attempts.

In general within the U.S. market, on-device biometric authentication is typically seen as preferable, since it reduces the risk of data's being compromised in transit and it lacks a central store of either templates or raw biometric data, which provides an attractive target for hackers. The repeated attacks on Aadhaar, India's national biometrics database demonstrate just how risky centralized stores of biometric data can be. Earlier this year, administrator credentials for Aadhaar were found being sold on dark web marketplaces for as low as the equivalent of $8.[3] More recently, a malicious patch was discovered, which would disable security features to enable malicious actors to create new identities, potentially with fraudulent biometric data.[4]

Combining on-device storage with authentication standards such as those put forth by the FIDO Alliance dramatically increases the complexity of compromising data, since the attacker must target victims' devices independently and cannot replay any data intercepted in transit to impersonate the victim.

When biometric data is stored on the device, storage within isolated hardware elements such as secure elements (SEs) and trusted execution environments is preferable to storage in device memory, even if the templates are encrypted. While

access to secure hardware devices is often logistically challenging, requiring negotiation with device manufacturers, mobile network operators, and OS providers, TEEs and SEs provide a more robust degree of isolation than most current methods of concealing or isolating sensitive data within ordinary device storage.

However, for some biometric modalities, on-device authentication is not feasible. Most prominently, passive voice biometrics for the call center cannot be done through a mobile app, since that requires the user to have the mobile app installed and initiate the call through the app, at which point some authentication has already been done, largely eliminating the need for passive voice authentication.

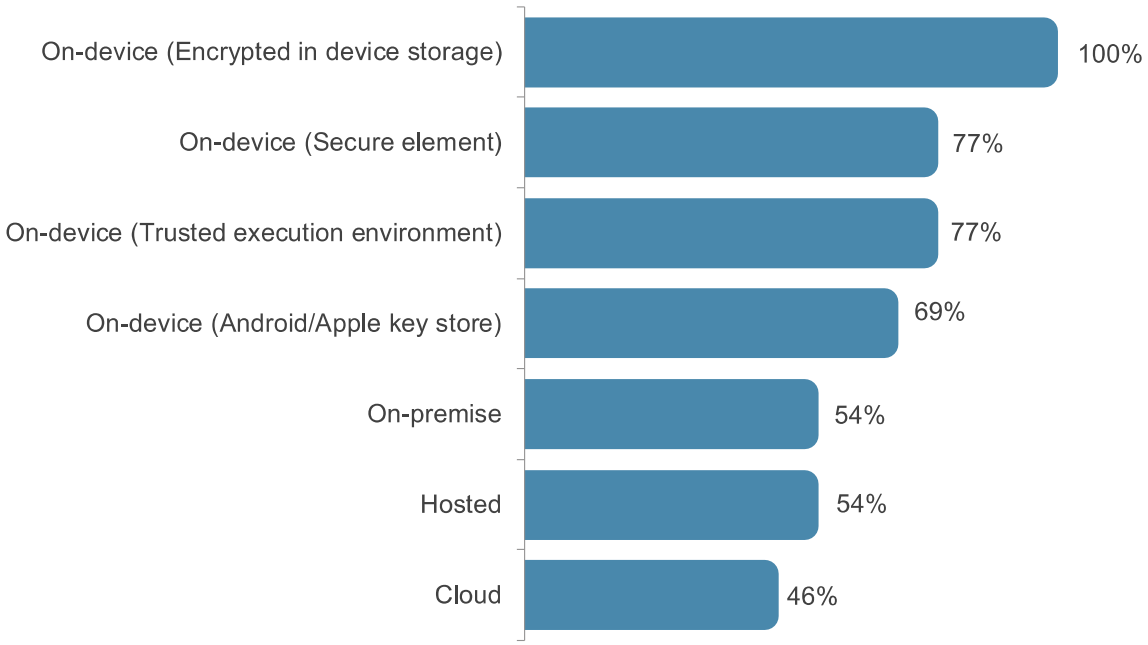
## RISK ASSESSMENT

Despite the increased assurance offered by biometric authentication, these methods are not foolproof means of verifying the identities of users, so financial institutions need to be cognizant of risk associated with biometric enrollment and ongoing authentication.

Enrollment is arguably the most crucial stage of biometric authentication. If a malicious individual is able to successfully enroll her own characteristics into a biometric authenticator, even the most sophisticated authentication method will still allow her to pass through security challenges. Consequently, many providers offer additional risk assessment tools built into their platform, such as device fingerprinting and geolocation. Other tools

**Most Biometric Platform Providers Favor On-Device Template Storage**

Figure 9: Template Storage Options Supported by Mobile Biometric Vendors




Source: Javelin Strategy & Research, 2018

offer natural supplements to biometric authentication, such as document scanning, which enables a degree of comparison between the user's captured biometric input and the image on an identification document.

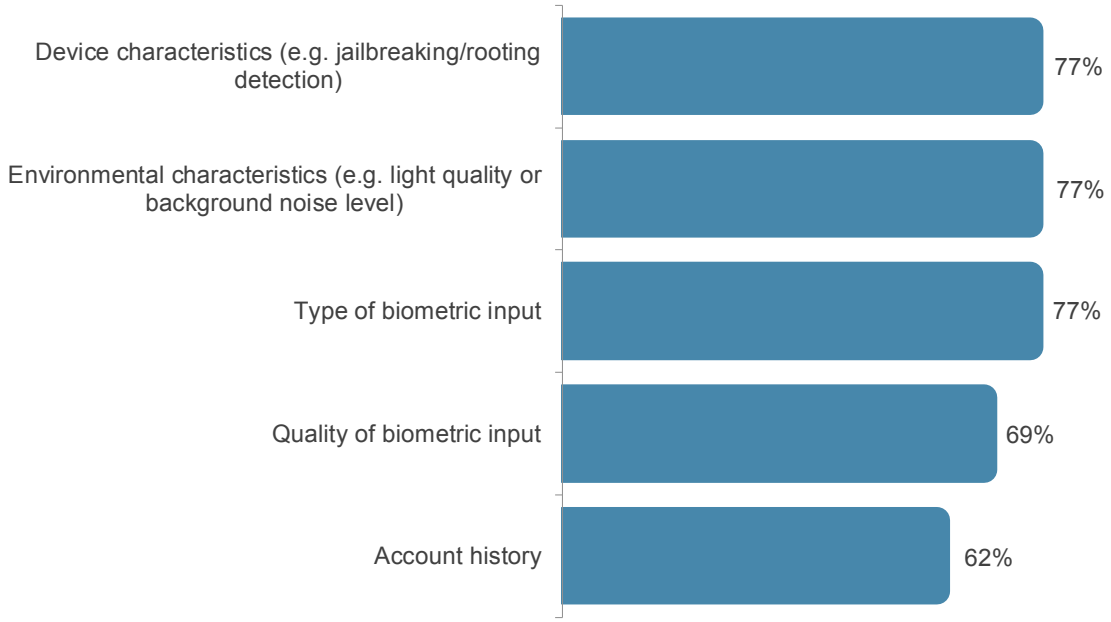
The level of risk around new biometric enrollments is high enough that financial institutions should be wary of significant account activity that occurs soon after a new biometric identifier is enrolled, just as they ought to be wary of high-risk events that occur shortly after a user's password or contact information has been changed. Unfortunately, account history is the risk assessment method that sees the lowest adoption among mobile biometric providers, supported by 62% of the providers evaluated in the scorecard (Figure 10).

Once a secure enrollment has been achieved, providing additional detail around the subsequent authentication attempts can help provide greater assurance. This can include information around risk factors such as environmental characteristics and the users' account history. Not only is this data useful in evaluating whether a particular authentication attempt should be approved, it provides crucial insight into factors that allow malicious actors to overcome biometric authentication or challenges that are impeding legitimate users' attempts to authenticate themselves.

One of the advantages of using a cryptographically backed authentication method, such as those leveraging the FIDO protocols, is that strong device identification is essentially built into the authentication stream. Because the authenticator is bound to the device, financial institutions leveraging this method have strong assurance that the user is authenticating from the same device

**User History is the Least Widely Supported Risk Indicator**

Figure 10: Risk Assessment Information Available




Source: Javelin Strategy & Research, 2018

# INNOVATIVE

Nuance, OneSpan, Nexsign (Samsung SDS), and Transmit Security distinguished themselves as leaders in mobile biometric authentication. This category rewards platform providers that offer cutting-edge features, whether those are emerging biometric modalities or more advanced analytic tools that operate behind the scenes.

| INNOVATIVE | |
|---|---|
| Leaders* | Nexsign (Samsung SDS) |
| | Nuance Communications |
| | OneSpan |
| | Transmit |
| Contenders | Daon |
| | HYPR |
| | RSA |
| Followers | Aware |
| | Gemalto |
| | Sensory |
| Laggards | Entrust Datacard |
| | Nok Nok Labs |

* Vendors in each category are listed alphabetically

* Leaders category expanded due to a tie

## FRAUD INTELLIGENCE SHARING

One particularly challenging area of functionality for biometric providers is in addressing the question of whether and how to share data on fraudulent identities that are detected on their platform. While this kind of consortium intelligence sharing has long been a part of other types of fraud detection solutions, from flagging questionable activity within credit reports or similar documentation to more sophisticated device recognition and reputation products, fewer than half of the mobile biometric solution providers evaluated offer the ability to share data on suspicious activity across companies using the platform.

On the one hand, since fraud rings target multiple institutions, being able to use biometric data to flag an individual as potentially malicious can arguably provide a powerfully persistent means of identifying career criminals in ways that other detection technologies cannot. While the user can change his device and will routinely shift between identities when targeting victims or managing collections of synthetic identities, his physical characteristics will remain unchanged, enabling his network of fraudulent activity to be identified and linked back to the same individual.

At the same time, technological and regulatory limitations make this a challenging proposition. Most biometric authenticators today operate locally, authenticating the user to her device, which then certifies to the server submitting the authentication request that the activity is approved. This ensures that the customer's biometric data is never actually seen by the organization authenticating her. Eliminating the need to transmit biometric data or store it in a central location

reduces the risk of data compromise and limits organizations' exposure to consumer data, making it easier to comply with regulations such as Europe's General Data Protection Regulation (GDPR).

Consequently, shared intelligence on fraudulent individuals is most frequently associated with platforms that employ server-side biometrics, rather than on-device. For certain use cases, use of server-side authentication is nearly unavoidable. For instance, use of passive voice biometrics in the call center cannot be easily done locally on a mobile device and instead is typically done using a voice recognition system housed on the financial institution's servers or with the biometric service provider.

## USE OF AI/MACHINE LEARNING

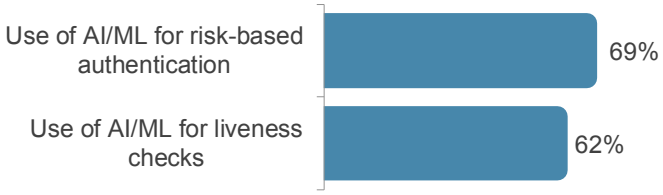
Artificial intelligence and machine learning have been of great interest to the anti-fraud and cybersecurity fields for some time, since they offer the promise of being able to identify and adapt to emerging fraud schemes more flexibly than a policy -based approach and more rapidly than with intervention from human analysts.

Within the area of biometric authentication in particular, these analytic techniques are particularly relevant to the challenges of liveness detection and risk assessment. With most spoofing techniques requiring the attacker to replicate the features of the victim through printing or modeling, liveness detection and risk assessment are obviously connected.

In addition to more effectively detecting spoofing attempts, AI/ML in risk assessment can also assist in reducing false positive declines by updating templates to identify changes in the user's features that may otherwise impede biometric authentication (e.g., growing a beard or getting glasses, both of which can challenge facial recognition). By automatically identifying that the individual is legitimate but has changed in some small way, the authentication platform can reduce the risk of wrongly blocking legitimate users.

### AI/Machine Learning Is Integrated by More Than Half of Biometric Platform Providers

Figure 11: Adoption of Artificial Intelligence/Machine Learning Capabilities




Source: Javelin Strategy & Research, 2018

# TAILORED

OneSpan, Transmit Security, and Nuance Communications distinguished themselves as leaders in the "Tailored" category. This category evaluates how effectively platform providers are able to configure their product to meet the business needs of their clients. And with exceptionally flexible platforms, these three vendors offer a variety of configurable implementation options supported by professional services arrangements to help adapt the authentication platform to the needs of clients and end users.

| TAILORED | |
|---|---|
| Leaders | Nuance Communications |
| | OneSpan |
| | Transmit |
| Contenders* | Daon |
| | Entrust Datacard |
| | HYPR |
| | Nok Nok Labs |
| Followers | Aware |
| | Gemalto |
| | Nexsign (Samsung SDS) |
| Laggards | RSA |
| | Sensory |

* Vendors in each category are listed alphabetically

* Contenders category expanded due to a tie

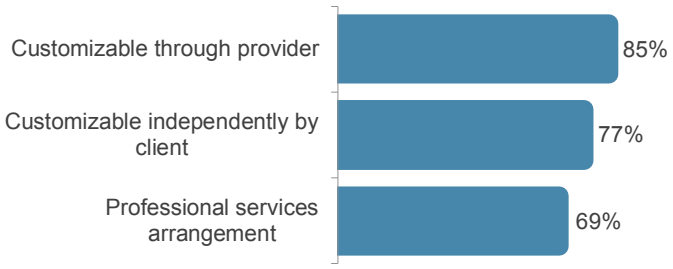
## SENSITIVITY CONFIGURATION

One of the unique aspects of biometrics compared with other authentication methods is that the sensitivity of the authenticator can be fine-tuned to match the level of assurance needed and how concerned the authenticating organization is about false-positive declines.

Being able to refine the sensitivity of biometric modalities in response to reporting on successful and failed login attempts is one of the key advantages of utilizing a biometric algorithm developed by and built into a vendor's authentication platform rather than authenticators baked into the device OS. While authenticators such as Touch ID and Face ID provide the quickest implementation, since they essentially involve tapping into an API within the OS, they also operate as black boxes, with neither the authenticating company nor the vendor providing the authentication platform with ability to adjust how closely the user is matched to the template.

### Fine-Tuning Sensitivity Allows FIs to Balance False Positives With Fraud Risk

Figure 12: Support for Customized Authenticator Sensitivity




Source: Javelin Strategy & Research, 2018

Five of six platforms evaluated within the scorecard (85%) support the capability to configure authenticator sensitivity on behalf of their clients. However, more sophisticated organizations often want to be able to adjust their configurations independently, being able to more quickly increase sensitivity in response to ongoing attacks or reduce sensitivity if they are seeing excessive false positives. This capability is supported by a notably smaller number of providers (69%).

# APPENDIX

## Overall, Goodwill, and Reliability Scores for Evaluated Financial Institutions

Figure 13: Trust Scores by Financial Institution

| | | |
|---|---|---|
| **Supported channels** | | |
| Online (browser) | F | 100% |
| Mobile | F | 100% |
| Phone (IVR) | F | 62% |
| Phone (Agent) | F | 69% |
| In-branch/standalone hardware devices | F | 85% |
| **Supported modalities** | | |
| Fingerprint | F | 85% |
| Face | F | 100% |
| Eye (iris) | I | 31% |
| Palm | I | 31% |
| Voice (active) | F | 69% |
| Voice (passive) | F | 46% |
| Behavior | F | 85% |
| **Template storage options** | | |
| On-device (Trusted execution environment) | F | 77% |
| On-device (Secure element) | F | 77% |
| On-device (Android/Apple key store) | F | 69% |
| On-device (Encrypted in device storage) | F | 100% |
| Hosted | F | 54% |
| On-premise | F | 54% |
| Cloud | F | 46% |
| **Mobile integration options** | | |
| SDK | T | 100% |
| Custom integration | T | 100% |
| Standalone application | T | 62% |
| **Delivery options** | | |
| Software as a service (SaaS) | T | 69% |
| Hosted | T | 92% |
| On-premise | T | 85% |
| Cloud | T | 100% |
| **Information sharing** | | |
| Information sharing available | I | 62% |
| **Pricing model used** | | |
| Per transaction | T | 69% |
| Per user | T | 100% |
| Per year | T | 85% |
| **Identity verification capabilities** | | |
| Data validation (PII matching, etc.) | F | 46% |
| Device fingerprinting/reputation | F | 77% |
| Document scanning | F | 46% |
| Geolocation | F | 62% |

| | | |
|---|---|---|
| **Output types** | | |
| Categorical | T | 69% |
| Decision | T | 85% |
| Reason codes | T | 85% |
| **Sensitivity configurations** | | |
| Customizable independently by client | T | 77% |
| Customizable through provider | T | 85% |
| Professional services | T | 69% |
| **Native analytics/risk assessment** | | |
| Quality of biometric input | F | 69% |
| Type of biometric input | F | 77% |
| Environmental characteristics | F | 77% |
| Device characteristics | F | 77% |
| Account history | F | 62% |
| **AI/ML capabilities** | | |
| Use of AI/ML for liveness checks | I | 62% |
| Use of AI/ML for risk based authentication | I | 69% |
| **Professional services** | | |
| Assistance with integration into mobile app | T | 100% |
| User experience/interface | T | 92% |
| Analytics | T | 100% |
| Optimizing sensitivity | T | 69% |
| **Integrated case manager** | | |
| Integrated case manager | I | 38% |
| **Administrative access controls** | | |
| No authenticated login portal is integrated into our product | T | 15% |
| Single level of access for users | T | 15% |
| Access control tailored to individual users | T | 85% |
| Not applicable | T | 8% |
| **Authenticated administrative portal controls** | | |
| Username/password (unique to the portal) | T | 85% |
| Single-sign on with client credentials | T | 62% |
| One-time password | T | 46% |
| Security key/smartcard | T | 31% |
| **Types of reporting available** | | |
| Automated reporting of aggregate data for regular periods | T | 77% |
| Ad-hoc reporting | T | 69% |
| Case-level reporting | T | 77% |
| Reporting of user-level activity | T | 77% |
| On-demand visualization | T | 69% |

Source: Javelin Strategy & Research, 2018

# METHODOLOGY

Consumer data within the scorecard was collected principally from an online survey of 5,000 U.S. respondents fielded in November 2017. For questions answered by all respondents, the maximum margin of sampling error is 1.39 percentage points at the 95% confidence level. The margin of error is higher for questions answered by smaller segments of respondents.

For the scorecard component of the report, Javelin included 12 vendors that agreed to participate and complete a self-evaluation scorecard with details around their submitted product's capabilities in supporting mobile biometric authentication. For vendors with multiple products, only those that were submitted and relevant to mobile biometric authentication platforms were considered in the scorecard. Javelin independently verified vendor capabilities against publicly available information, where it was available. Rankings are not a reflection of the full breadth of capabilities of any particular vendor.

Each criteria in the scorecard was weighted according to Javelin's assessment of its relevance in addressing current and emerging fraud schemes, as well as its ability to facilitate positive customer experience in digital channels. Overall score was calculated as a composite of the three categories, with Functional accounting for 50% of all total points, Innovative accounting for 30%, and Tailored accounting for 20%.

# ENDNOTES

1. https://www.theverge.com/circuitbreaker/2018/7/19/17589676/vivo-nex-review-camera-fingerprint-sensor-apex, accessed Oct. 12, 2018.
2. https://www.cnet.com/news/oneplus-6t-removing-the-headphone-jack-was-a-tough-decision/, accessed Oct. 23, 2018.
3. https://gizmodo.com/full-access-to-indias-national-biometric-database-repor-1821772876, accessed Oct. 15, 2018.
4. https://gizmodo.com/simple-hack-turns-indias-massive-biometric-database-int-1828972521, accessed Oct. 15, 2018.

| Companies Mentioned | |
|---|---|
| Aware | Nok Nok Labs |
| Capital One | Nuance Communications |
| Daon | OneSpan |
| Entrust Datacard | RSA |
| Equifax | Samsung SDS |
| FIS | Sensory |
| Gemalto | Transmit |
| HYPR | |