2017 IDENTITY PROOFING PLATFORM SCORECARD

OCTOBER 2017

Licensed by:

experian.

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

ABOUT JAVELIN: JAVELIN, 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: online and mobile banking; fraud, risk, and marketing departments; mobile banking vendors; identity proofing technology vendors; identity proofing platform vendors.

AUTHOR: Al Pascual, Senior Vice President, Research Director
Kyle Marchini, Senior Analyst, Fraud & Security

CONTRIBUTORS: Sarah Miller, Research Manager, Custom Research
Sean Sposito, Analyst, Fraud & Security

EDITOR: Chuck Ervin

PUBLICATION DATE: October 2017

FOREWORD

This report was originally produced for Javelin Advisory Service clients and has been licensed for distribution by Experian. The comprehensive analysis of identity proofing trends and providers was independently produced by Javelin Strategy & Research, a division of Greenwich Associates. Javelin maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

One of the foundational fraud challenges that an institution faces — identity proofing — must be tailored to the risks inherent in the channel, market, product type, scenario, and threat environment. In the complex financial ecosystem of 2017, a bifurcated model of identity verification and authentication fails to meet the needs of accountholders or financial institutions. Accordingly, a much more holistic approach is needed to take into account a richer array of context around the identity and behavior of the consumer. In this report, Javelin examines how FIs can best manage identity proofing across different key use cases and provides a guide for selecting the most effective identity proofing platform based on functionality, innovation, and the ability to tailor the product to the needs of the business.

PRIMARY QUESTIONS

- How can financial institutions effectively manage identity throughout the entire customer lifecycle?
- What factors should financial institutions take into account when designing their identity proofing process?
- How are fraudsters adapting their tactics to circumvent current anti-fraud measures?
- What identity proofing vendors offer the widest array of capabilities suited to addressing current and emerging fraud threats?

EXECUTIVE SUMMARY

Neither consumers nor FIs are served well by the traditional approach to identity proofing. A reliance on traditional identity verification approaches — mandated as part of a Customer Identification Program (CIP) in financial services — are no longer sufficient or appropriate for digital channels. In 2017, consumers are applying for new financial accounts in the same digital channels where some institutions still rely on correlating a name, address, Social Security number, and date of birth to form the bulk of their identity verification process.

Mobile phones, the keystone of identity verification and authentication, are under siege. FIs have flocked to the mobile phone as a way to verify an identity through the use of services such as one-time passwords, but this method is very much under pressure by fraudsters. The number of mobile phone account-takeover victims doubled between 2015 and 2016. This kind of data provided during a new account application can be falsified by fraudsters, by opening a mobile account in the victim's name — a scheme that also doubled in number between 2015 and 2016.

The growing role of biometrics in account security means that FIs will increasingly need to know who is enrolling. As biometrics become progressively more important to authentication, financial institutions must be able to assess the level of risk associated with enrolling a new authenticator. Just because a user is logged into a session does not mean that their goal in enrolling a new biometric should be trusted. This will become especially important as out-of-band mobile biometrics becomes more important as either login or step-up authentication for online banking, and as biometrics enabled by laptops and desktops begins to play a significant role in online banking.

Trusting a new device is fraught with risks on both sides of the equation. Once an account has been established, the array of devices and services that consumers have at their disposal complicates account life-cycle management for financial institutions. Any time a new device presents itself — either for online or mobile banking — financial institutions need to assess the risk of allowing that unfamiliar device access to the account against the risk of wrongly blocking a legitimate accountholder.

Even if an approach to identity proofing is effectively tailored to specific use cases today, there are no guarantees tomorrow. Regardless of the tools in place, no identity proofing scheme is foolproof, both in the sense that highly motivated fraudsters will always find gaps in the system and that legitimate individuals do not always behave in predictable ways. And situations will change as new channels are brought into the fold, such as augmented or virtual reality, or virtual assistants such as Alexa.

Experian's CrossCore is the best overall identity proofing platform. With a strong showing in all three categories, but especially in the valuable functional category, Experian took this year's award for the best overall identity proofing platform in a field of 23 providers.

Despite breaches, verifying personally identifiable information (PII) is the most common capability. Even in the wake of large-scale data breaches, PII validation remains a crucial part of the identity proofing process for financial institutions, especially where no previous relationship to the prospective customer exists and FIs must meet know-your-customer (KYC) requirements. Accordingly, data validation is the most widely offered feature among the identity proofing products covered in the scorecard, with 77% of products offering data validation capabilities.

The diverse utility of document scanning drives support by half the market. Document scanning — offered by half of ID proofing

platforms — provides an alternate means of validating PII and streamlining the customer experience. Presence of a valid identification document that passes scrutiny significantly reduces the risk of an applicant with valid PII being a fraudster who has obtained that information through a breach or social engineering. And these solutions can be used to prefill information so as to lower the burden on customers to do the same.

Assessing device input behavior can create insights into digital channel fraud, but provider adoption lags. Specifically looking for unique patterns of interaction with input devices, e.g. keyboard, mouse, or touchscreen, behaviometrics can assess everything from suspicious velocity — attempting multiple applications within minutes — to aberrant navigation patterns within an online banking portal, yet the capability is only supported by 41% of ID proofing platforms.

RECOMMENDATIONS

Start by aligning the approach to identity proofing with the business. Get ahead of fraud threats by aligning potential future changes in the business, such as an expected rise of new technologies, products, channels, or services, with an underlying platform that can adapt with the business. FIs that are apt to be technology leaders or fast followers should seek out extensible platforms that have proven to adapt with the times.

Optimize the identity proofing workflow. Practical considerations, from costs to customer experience, dictate that not everything should be run at once, but rather this process should involve a specific workflow. Not only does this enable thoroughly reasoned decision logic for each scenario, it minimizes unnecessary calls to costly services on applications or other activities that can either be immediately blocked because of a high risk of fraud or streamlined if there is a strong indication that a consumer is legitimate.

Any platform designed to act as a central identity proofing hub needs to have the basics in order to be truly effective. A comprehensive identity proofing platform should allow an FI to integrate with other tools to initiate calls to and consume inputs. It should also allow the creation of custom rules and workflows for different products and channels that use a sufficiently wide scoring band, allowing for granular customization.

Forget knowledge-based authentication. Customers surely will forget the answers, and fraudsters will not. Knowledge-based authentication (KBA) has many acknowledged weaknesses, including the friction imposed on legitimate accountholders and the risk of fraudsters being able to discover the answers to challenge questions, either with social engineering or public information about the victim. Accordingly, use of KBA should be restricted to circumstances where no other tools can feasibly provide sufficient information about an applicant or accountholder.

Verify the phone. Drawing on information sources outside financial services, like mobile network operators, can help on a number of levels. By confirming that the phone number provided belongs to an applicant and that the number is in control of the applicant, financial institutions can offset the impact of fraudsters providing false information that either matches a phone under their control or one they have taken control of.

Work behind the scenes from the start, and work together. Device and behavioral analyses can passively assess risk from the beginning of a session. This can help weed out automated applicants and minimize fraudsters' ability to use botnets to accelerate the application process. Drawing on device fingerprinting, providers that can provide a broad view into devices' reputations across an array of institutions can further help to clarify whether a particular device being used to initiate the application is associated with positive or negative behavior.

Take matters into your own hands with better visualization. As analytic tools grow in sophistication, on-demand visualization offers FIs an opportunity to gain a better vantage point on fraud trends. These tools can help analysts investigate clusters of suspicious cases that might be linked by common elements that might otherwise be difficult to see.

TOWARD A NEW MODEL OF IDENTITY PROOFING

Conventionally, identity verification and authentication were clearly bifurcated. Identity verification — resolving an applicant's identity to a single real-world individual — occurred prior to an account being opened and largely consisted of validating personal information provided by the applicant, usually against a credit report and a small set of other public records. Once the account was opened, it was largely assumed that the identity was valid so emphasis shifted to authentication: ensuring that an individual trying to access an account was the same person who opened it.

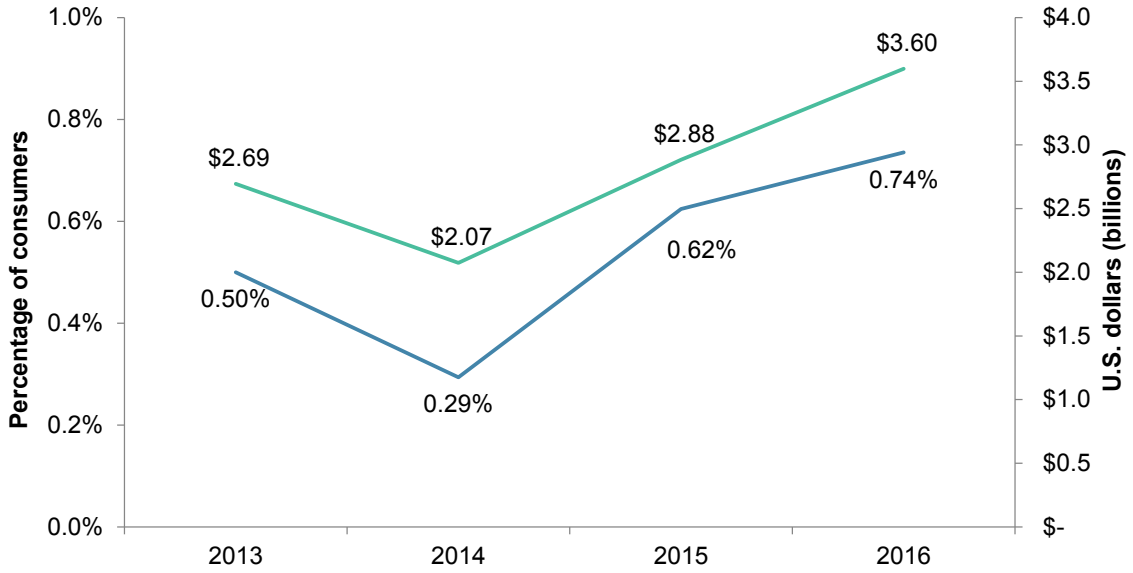
In the complex financial ecosystem of 2017, a bifurcated model of identity verification and authentication fails to meet the needs of accountholders or financial institutions. Accordingly, a much more holistic approach is needed to take into account a richer array of context around the identity and behavior of the consumer.

TACKLING ACCOUNT OPENING

One of the foundational fraud challenges an institution faces, identity proofing during the account opening process, must be tailored to the risks inherent in the channel, market, product type, and threat environment. Relying on traditional identity verification approaches — mandated as part of CIP in financial services — are no longer sufficient or appropriate for use in digital channels. In 2017, consumers are applying for new financial accounts in the same digital channels where some institutions still rely on correlating a name, address, Social Security number, and date of birth to form the bulk of their identity verification process. Fortunately, a raft of new technologies and approaches exist that can better ascertain identity and prevent new-account fraud, which has increasing the past two years (Figure 1).

New-Account Fraud Is on the Rise

Figure 1: Losses and Incidence Rebound From 2014 Lows



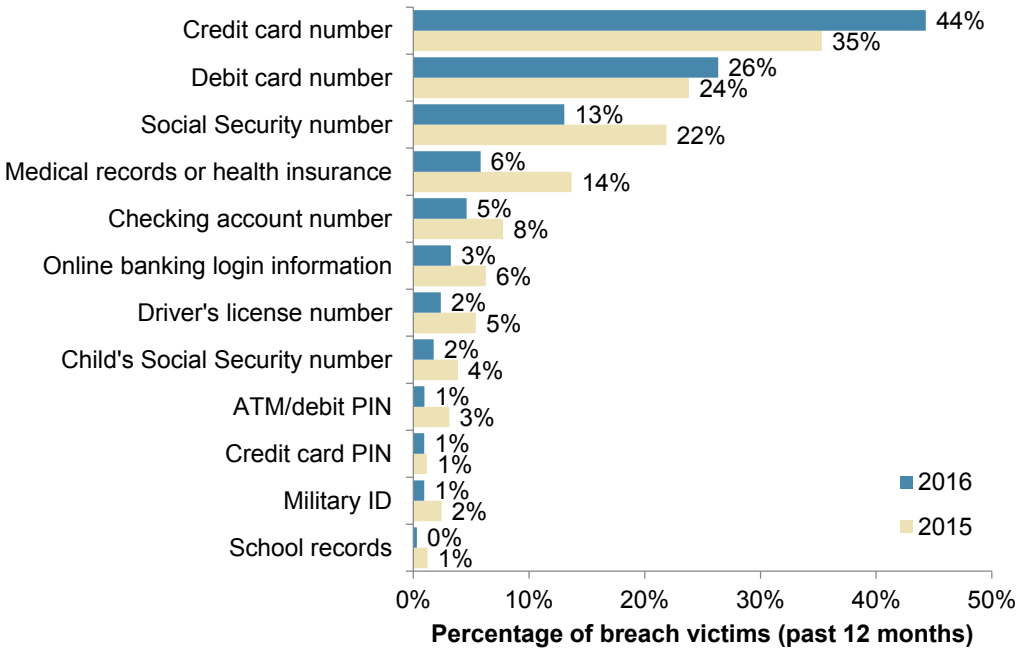
Source: Javelin Strategy & Research, 2017

During account opening, many tools that were conventionally in the realm of authentication bring additional insight into the authenticity of the individual. Device fingerprinting can help identify anomalous characteristics (e.g., use of a virtual machine or a mismatch in location) or identify botnets used to mask fraudulent behavior and to apply for new accounts en masse. Similarly, behaviometrics can assess whether an applicant is a human or an automated tool, though its efficacy for the former to determine *which* human is applying is limited by its exposure to the applicant or fraudster in a previous session.

Conventional tools like PII validation will retain a mandated role in vetting applicants, but the verification of core elements of individual identity are becoming less predictive when determining fraud risk. Years of data breaches affecting sensitive PII — with SSNs being among the most popular targets — have effectively fed criminal efforts to commit new-account fraud (Figure 2). Further still, this data has allowed synthetic identities — those compiled of cobbled-together details, purchased from the Internet's underground — to be used to repeatedly dupe issuers and lenders .

Compromise of Persistent Identifiers Creates Long-Term Challenges for FIs

Figure 2: Type of Data Breached Among Notified Victims, 2015–2016



Source: Javelin Strategy & Research, 2017

Where validating data has true predictive value is in integrating an ever-widening array of data sources. Drawing on information sources outside financial services, like mobile network operators, can help on several levels. First, by verifying a broader range of data — specifically confirming that a certain phone number belongs to the applicant and that the number is in control of the applicant — financial institutions can offset the impact of fraudsters providing false information that matches a phone under their control. The latter is a critical consideration because the number of mobile phone account-takeover victims nearly doubled between 2015 and 2016. And while this kind of data can be falsified by fraudsters by opening a mobile account in the victim's name — a scheme that also almost doubled in number between 2015 and 2016 — it adds significant complexity and cost to deter them (Figure 3).

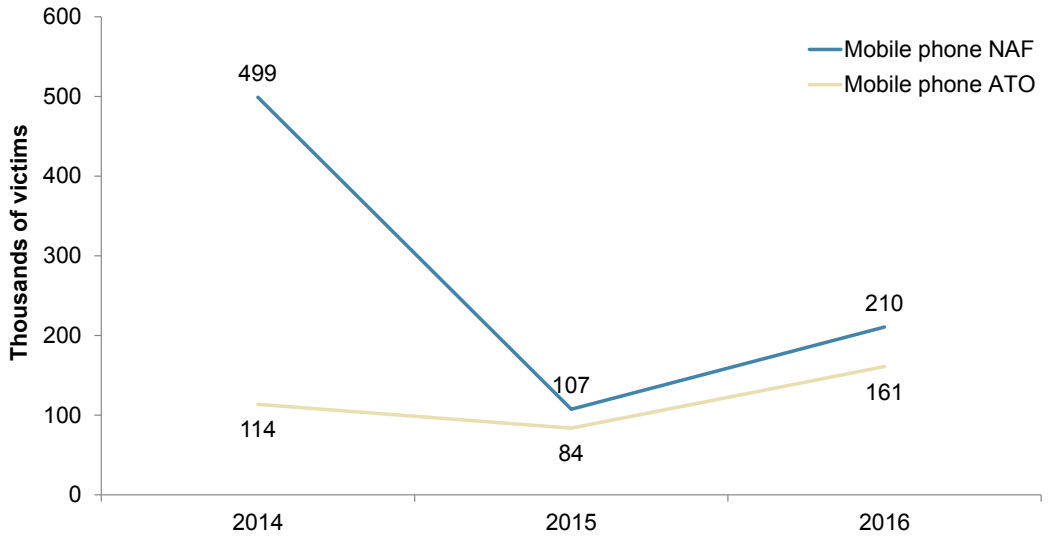
Similarly, drawing on shared intelligence from a consortium of institutions either within financial services or other industries can enrich internal analytics by providing a richer context for an individual in question. This consortium data can include context around more traditional information, such as the application histories associated with different PII data points, or it could provide digitally oriented insights, such as whether a device has a history of fraud at different institutions.

Ongoing monitoring is crucial for managing challenging fraud types like synthetic identity and bust-out schemes. These schemes will often cultivate accounts with near-perfect behavior to raise credit limits at several accounts at multiple institutions, and if these identities are not caught at account opening, it can be challenging to halt them prior to the fraudster acting to monetize the scheme. Consortium intelligence can help give intelligence about bust-out schemes in progress by notifying financial institutions that an account network is unraveling.

To accommodate the volume and velocity of digital financial life, much of this process must be automated. The rise of digital account opening necessitates that financial institutions complete the initial identity proofing process within minutes, if not seconds.

Mobile ATO and NAF Victims Doubled in 2016

Figure 3: Number of Mobile Account-Takeover and New-Account Fraud victims, 2014–2016



Source: Javelin Strategy & Research, 2017

ENROLLING NEW DEVICES AND BIOMETRICS

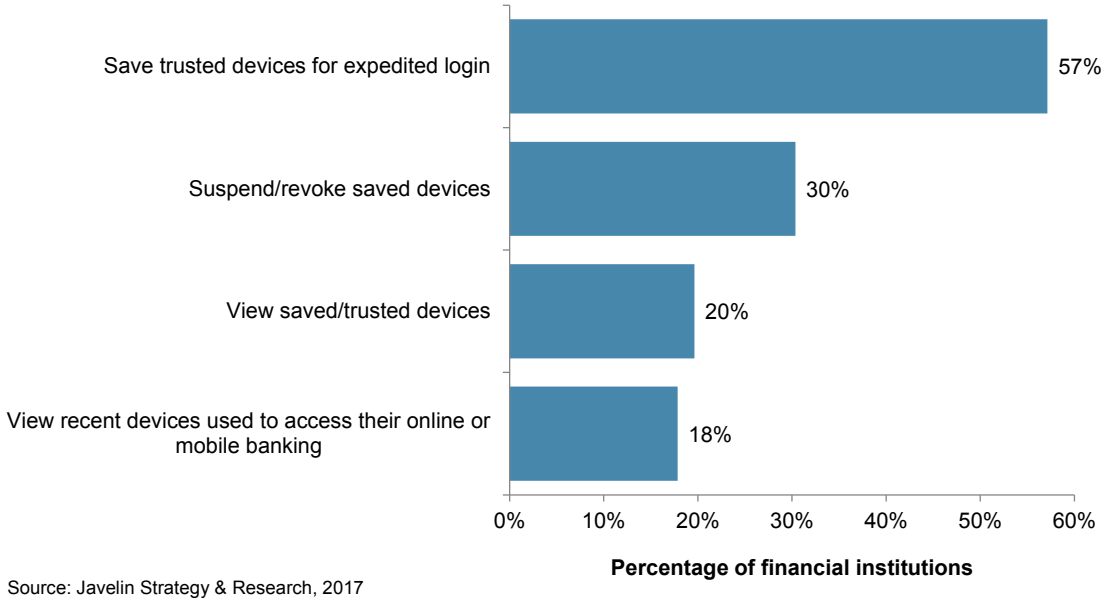
Once an account has been established, the array of devices and services that consumers have at their disposal complicate account life-cycle management for financial institutions. With the rise of digital account opening, many consumers will access their account through the same laptop or desktop computer they used to create it. In fact, more than half of top retail FIs allow users to enroll trusted devices to streamline the login process (Figure 4). However, these same accountholders will need to associate a mobile device with their account to initiate mobile banking. Anytime an accountholder acquires a new device — either for online or mobile banking — financial institutions need to assess the risk of allowing an unfamiliar device to access the account against the risk of wrongly blocking a legitimate accountholder.

Similarly, once a device has been established, many events will require financial institutions to subject the accountholder to additional scrutiny. As the use of biometrics becomes progressively more important to authentication, financial institutions must be able to assess the level of risk associated with enrolling a new authenticator. Just because a user is logged into a session does not mean that their goal to enroll a new biometric should be trusted. This will become especially important as out-of-band mobile biometrics become more important as either login or step-up authentication for online banking, and as biometrics enabled by laptops and desktops begin to play a significant role in online banking.

Regardless of the tools in place, no identity proofing scheme is foolproof. Highly motivated fraudsters will always find gaps in the system, and legitimate individuals do not always behave in neatly predictable ways. Inevitably, legitimate accountholders will need to access their accounts under extraordinary circumstances. Devices malfunction or are lost, and accountholders will need to access their accounts from unusual locations. And situations will change as new channels are brought into the fold, such as augmented or virtual reality, or virtual assistants such as Alexa.

More Than Half of Top FIs Allow Customers to Establish Trusted Devices

Figure 4: Percentage of Top 28 FIs That Offer Device-Management Capabilities



Source: Javelin Strategy & Research, 2017

DESIGNING A ROBUST ID PROOFING WORKFLOW

Practical considerations, from costs to customer experience, dictate that not everything should be run at once, but rather this process should involve a specific workflow. Not only does this enable thoroughly reasoned decision logic for each scenario, it minimizes unnecessary calls to costly services on applications or other activities that can either be immediately blocked due to a high risk of fraud or streamlined if there is a strong indication that the consumer is legitimate. Below are the general steps and potential tools that an FI can use to establish robust robust identity proofing capability.

1. **Before it starts:** A comprehensive identity proofing platform should be in place. The platform should allow an FI to integrate with other tools to initiate calls to and consume inputs from various tools. It should also allow the creation of custom rules and workflows for different products and channels that use a sufficiently wide scoring band, allowing for granular customization.
2. **Start of the session:** Device and behavioral analyses have the advantage of passively assessing risk from the beginning of the session. This can help weed out automated applicants, minimizing fraudsters' ability to use botnets to accelerate the application process. Drawing on device fingerprinting, providers that can provide a broad view into devices' reputations across an array of institutions can further help to clarify whether a particular device being used to initiate the application is associated with positive or negative behavior.
3. **Entering the data:** Tools that can prefill information should obviously be integrated shortly after an individual initiates an application or is required to provide supplemental PII during other scenarios. Document-scanning tools should be integrated early because they can help streamline the process for legitimate applicants by prefilling common data fields. This is especially useful for mobile channels, either app or web, because manually entering information is tedious for consumers in either case.
4. **Assessing the provided data:** The ability to not only verify the data provided but to also gain insight into the history of that data is critical in avoiding fraud. During this stage, FIs can verify that the PII provided matches a single identity and use data from mobile network operators (MNOs) to ascertain the status of the mobile number. FIs can also consider the history of each data point through a consortium relationship to establish whether it was involved with fraud elsewhere. Looking for high-risk behaviors associated with consumer-provided data beyond fraud can supply valuable intelligence about whether a synthetic identity is in use. For example, by establishing whether the identity has an unusual history as a frequent authorized user on several unrelated credit card accounts. This behavior is typical for fraudsters looking to legitimize a newly established synthetic identity.
5. **Day two and manual reviews:** For attempts that are given a passing grade, institutions should continue to monitor for high-risk activities as part of their day-two process. Or if the fraud risk is still unclear, FIs can choose to route the attempt for a manual review. This can include the use of tools that are typically more expensive and require individualized assessment, such as employment verification. This also increases the utility of platforms that support case management.

INTRODUCING JAVELIN'S FIT MODEL

To evaluate products in the inaugural Identity Proofing Platform Scorecard, Javelin developed the Functional, Innovative, Tailored (FIT) model. This 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 identity proofing, this encompasses the capabilities the product offers to resolve a digital identity to a real-life individual and assess the fraud risk associated with an event (e.g., application, transaction, or login).
2. **Innovative:** As fraud continues to evolve with the changing landscape of financial services, any identity proofing product must integrate cutting-edge features in order to retain relevance. This category covers leading features crucial to serving customers and fighting fraudsters 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.

OVERALL

With a strong showing in all three categories, but especially in the particularly valuable Functional category, Experian took this year's award for the best overall Identity proofing platform among a field of 23 providers.

2017 IDENTITY PROOFING PLATFORM

SCORECARD AWARD

BEST IN CLASS

EXPERIAN

FUNCTIONAL

Identity proofing covers circumstances ranging from new account applications to new device enrollment, and in order to successfully discern between fraudsters and legitimate customers, financial institutions must be able to bring a wide range of capabilities to bear as part of their identity proofing workflows.

Equifax, Experian, and LexisNexis Risk Solutions take the top three places as leaders in identity proofing functionality. All three of these companies' products offer channel-agnostic functions, which enable them to support a wide array of use cases. Additionally, each product provides a balance of conventional identity verification and authentication, which enables them to provide value throughout the entire customer account life cycle.

Equifax, Experian, and LexisNexis Lead in Functional Category

Figure 5. Rankings in Functional Category

FUNCTIONAL	
Leaders	Equifax
	Experian
	LexisNexis Risk Solutions
Contenders	FICO (Fair Isaac Corporation)
	GIACT Systems
	IDology
	NuData Security, a Mastercard company
	Socure
	ThreatMetrix
	TransUnion
	Trusona
Followers	AU10TIX
	Early Warning Services
	Gemalto
	ID Analytics
	Jumio
	Mitek
	RSA
	Trulioo
Laggards	BehavioSec
	BioCatch
	DataVisor
	Neustar

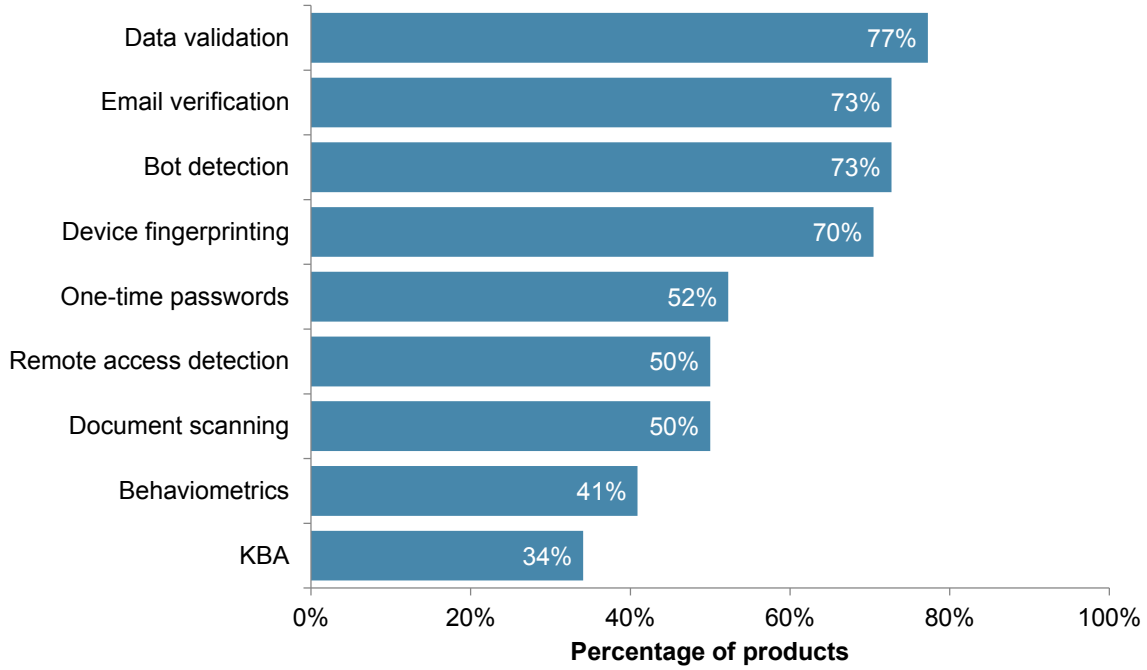
* Vendors in each category are listed alphabetically
Source: Javelin Strategy & Research, 2017

KEY FEATURES

Identity proofing capabilities were analyzed against eight core capabilities: data validation, email verification, bot detection, device fingerprinting, one-time passwords, document scanning, remote access detection, and behaviometrics. Regardless of whether these features come from a single vendor or a combination, financial institutions should have a solution to cover each area.

Data Validation Remains Central to Identity Proofing

Figure 6. Key Feature Adoption Among Identity Proofing Vendors



Source: Javelin Strategy & Research, 2017

IDENTITY VERIFICATION

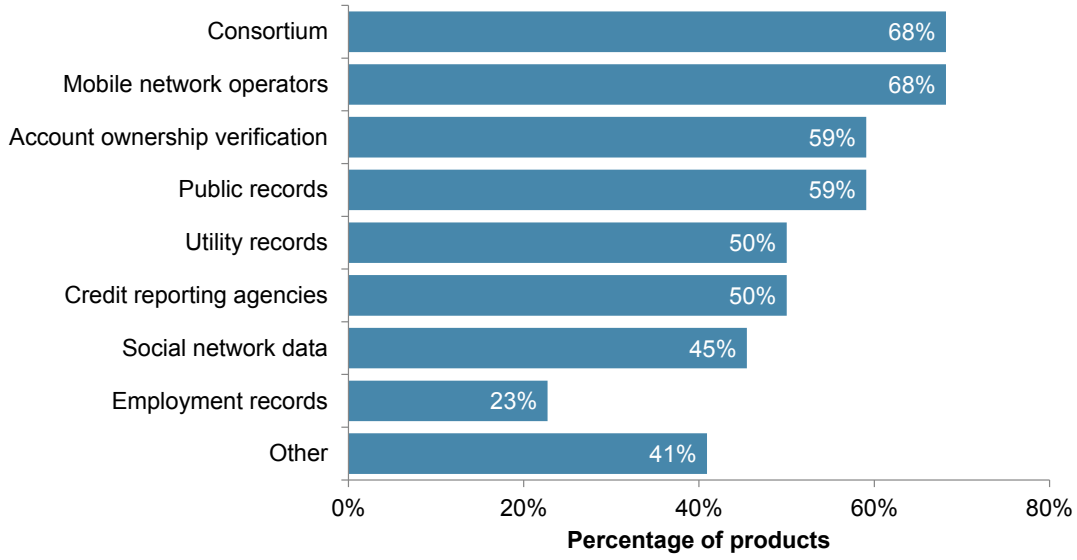
Even in the wake of large-scale data breaches, PII validation remains a crucial part of the identity proofing process for financial institutions, especially where no previous relationship to the prospective customer exists. Accordingly, data validation is the most widely offered feature among the identity proofing products covered in the scorecard, with 77% of products offering data validation (Figure 6).

However, PII validation has a core problem: namely, determining how to make effective decisions about individuals who have minimal history. When a thin- or no-file individual applies for a new account, their history could be indicative of an individual who is simply beginning his or her financial life, or it could be an indication of a fraudulent synthetic identity constructed so as to not hit existing records.

Drawing upon different types of data sources can help provide visibility into thin-file applicants' identities. While a consumer who is opening her first financial accounts will have little or no information on her credit report, it is less likely that she will also have no social media and mobile phone account. Even for individuals with more established histories, using information sources outside of financial services can either provide confirmation of the legitimacy of an identity or identify inconsistencies that trigger additional scrutiny (Figure 7).

Consortium, MNO Data Top Most Prevalent Data Sources

Figure 7. Data Sources Used by Identity Proofing Products



Source: Javelin Strategy & Research, 2017

Document scanning, which is offered by half of ID proofing platforms, provides an alternative means of validating PII (Appendix, Figure 12). The presence of a valid identification document that passes scrutiny significantly reduces the risk of an applicant with valid PII being a fraudster who has obtained that information through a breach or social engineering. However, fraudsters still have a variety of methods of attempting to circumvent document-scanning solutions. Counterfeit or altered documents provide an obvious means of overcoming these challenges, though the cost and logistic difficulty of obtaining forged documents of a sufficiently high quality is likely to deter fraudsters except in the most high-value fraud schemes. Alternately, fraudsters can try to secure images of the victim and legitimate identification documents either through social engineering or malware and create documents on their own, though they may find that their amateur attempts yield little success.[1]

However, all the pieces of an identity will rarely match perfectly to a single individual. Legitimate applicants move, change phone numbers, and have accounts spread across a variety of institutions. Accordingly, it is crucial to have a strong risk engine underpinning any identity verification tool to continually assess the risk associated with information mismatches.

CONTEXTUAL RISK AND INTELLIGENCE

Once it has been determined with sufficient confidence that all the personal information in an application resolves to a single, existing person, it remains to be determined that the person on the other side of the connection is the same as the claimed identity. Device intelligence provides a necessary check against fraudsters making use of compromised information.

Device fingerprinting solutions can assess device-related risk across a variety of metrics. If a device has been seen before, it can be associated with either positive or negative activity. Additionally, noting the number of distinct identities that are associated with the device can help identify criminal networks that are targeting a variety of accounts.

Assessing device risk from a consortium of other institutions can provide a particularly useful defense against automated attacks. With the growth of digital account opening, fraudsters use automated tools to attempt account applications or logins at multiple institutions to increase the odds of success. Knowing that a similar device has been flagged by other financial institutions or merchants can enable entities further down the chain to trigger additional scrutiny for suspected bots.

Behavior monitoring provides an additional safeguard against malicious behavior, automated attacks, and remote access. Behavior monitoring can be grouped into two types: session analytics and behaviometrics

- **Session analytics** observes how the user interacts with the portal: what pages are visited, how long the user stays there, and what kinds of actions are initiated within them. For instance, if a known customer who usually spends time reviewing recent transactions immediately jumps to enrolling a new device and using that device to make an outbound transfer, a security solution monitoring the session should raise red flags.
- **Behaviometrics** draw conclusions based on how the user interacts with the input device, e.g. the smartphone, mouse, or keyboard. Fraudsters have been known to make use of either remote-access tools within malware or misuse of legitimate remote-access software to gain control of a victim's device. A legitimately trusted device accessing the account will not trigger any device fingerprinting flags. However, due to the latency inherent in remotely operating a second device, this kind of attack generates unique patterns of mouse and keyboard activity, which is easily detected by behaviometric tools.

[1] Mobile malware

AUTHENTICATION

Flexibility in authentication provides applicability to a wide variety of use cases. One of the significant challenges in identity proofing is that any additional risk-screening measures that must occur during account opening do not have easy access to trusted devices or communication channels to rely on. This makes it difficult to rely on tools such as one-time codes without additional safeguards in place.

Mobile network data can help verify that the account associated with a mobile device is associated with the same information as the individual attempting to open an account. Additionally verifying that the number is not being forwarded and has a reasonable tenure with the account can help minimize risk.

Knowledge-based authentication (KBA) has many acknowledged weaknesses, including the friction imposed on legitimate accountholders and the risk of fraudsters being able to discover the answers to challenge questions, either with social engineering or public information about the victim. Accordingly, use of KBA should be restricted to circumstances where no other tools can feasibly provide sufficient information about an applicant or accountholder.

Where KBA is used, financial institutions should maintain records on the efficacy of each question used to continually refine the process. Financial institutions should consider the time it takes individuals to answer each question, along with the rates at which legitimate individuals answer each question incorrectly and fraudsters answer each question correctly. Eliminating questions that perform poorly by each metric can help safeguard accounts while minimizing the friction imposed on legitimate accountholders.

INNOVATIVE

To get ahead in the cat-and-mouse game that so often occurs in fraud prevention, introducing cutting-edge features is crucial. Many of the capabilities enshrined in the innovation category will one day be table stakes. Today these innovations are key differentiators between those solutions that are still geared toward the threats of yesterday and those that are poised to overcome tomorrow's major avenues of fraud.

NuData, ThreatMetrix, and TransUnion Lead in Innovation

Figure 8. Rankings in Innovative Category

INNOVATIVE	
Leaders	NuData Security, Mastercard Company
	ThreatMetrix
	TransUnion
Contenders	Early Warning Services
	Equifax
	Experian
	Gemalto
	GIACT Systems
	IDology
	LexisNexis Risk Solutions
	Socure
Followers	AU10TIX
	DataVisor
	FICO
	Jumio
	Mitek
	RSA
	Trulioo
	Trusona
Laggards	BehavioSec
	BioCatch
	ID Analytics
	Neustar

* Vendors in each category are listed alphabetically
Source: Javelin Strategy & Research, 2017

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Integrating artificial intelligence and machine learning into the identity proofing process can help streamline financial institutions' task in several ways. Depending on the sophistication of the AI/ML system, the risk tolerance of the client, and the type of event being analyzed, the proposed rules can either be suggested by the model and implemented by a human analyst — which is supported by 77% of platforms — or automatically implemented, as supported by 55% of platforms (Appendix, Figure 12).

First, by being able to rapidly analyze far more data than any human analyst is capable of, AI rules engines can identify commonalities among identified fraud events. The more established form of artificial intelligence known as supervised machine learning employs models using data where fraud has previously been identified as a reference, and consequently it requires historical "truth data" in order to function.

Unsupervised machine learning is optimal for cases where there is no reference data available to act as a guide. This is clearly suited to tasks such as evaluating events where new threats can cause immediate damage, including high-volume transactions, login attempts, or applications in near-real time. Because of the ability to identify commonalities between suspicious attempts as they occur, unsupervised machine learning models can prove quite powerful if integrated with a rules engine that enables the AI/ML tool to implement new rules independently.

BEHAVIORAL ANALYTICS AND BEHAVIOMETRICS

Behavioral monitoring is a broad term that encompasses tools that monitor for suspicious activity within a session, including session analytics and behaviometrics. The former can be used to discern when the activities taken by a consumer do not match an expected pattern of behavior. The latter can assess everything from suspicious velocity — attempting multiple applications within minutes — to aberrant navigation patterns within an online banking portal. Behaviometrics, which is supported by 41% of ID proofing platforms, specifically looks for unique patterns of interaction with input devices, e.g. keyboard, mouse, or touchscreen (Appendix, Figure 12).

Currently, these tools appear best suited to identifying aberrant behavior: e.g. takeover of a customer's device, scripted credential replay attacks. Certain types of attacks have distinctive behavior patterns that minimize the risk of wrongly flagging a legitimate user who is interacting with his device under unusual circumstances. As these tools are refined, they have the potential to progress more toward distinguishing between two different humans interacting with the same account.

Both of these tools are especially valuable because they enable institutions to continually assess risk during a session without requiring the user to encounter distinct authentication events. Invisible authentication provides two significant advantages: First, it prevents legitimate accountholders engaging in low-risk activity from having to interrupt their session to authenticate themselves needlessly. Second, by not advertising to fraudsters that authentication is occurring, it minimizes their opportunity to adjust their activity to overcome the challenge.

TAILORED

The award category for tailoring covers the flexibility of each solution to adapt to the business needs of clients. Accordingly, each solution was awarded points based on criteria like the types of outputs offered (decision, score, and reason codes), reporting options, access controls for users, and delivery options. This aims to capture how business-friendly each provider is in a variety of metrics.

DataVisor, FICO, and ThreatMetrix Lead in Tailored Category

Figure 9. Rankings in Tailored Category

TAILORED	
Leaders	DataVisor
	FICO
	ThreatMetrix
Contenders	AU10TIX
	Experian
	Gemalto
	IDology
	RSA
	Socure
	Trulioo
	Trusona
Followers	BehavioSec
	Early Warning Services
	GIACT Systems
	Jumio
	LexisNexis Risk Solutions
	Mitek
	NuData Security
	TransUnion
Laggards	BioCatch
	Equifax
	ID Analytics
	Neustar

* Vendors in each category are listed alphabetically
Source: Javelin Strategy & Research, 2017

FLEXIBILITY IN USE

Broadly speaking, three types of output are relevant to identity proofing solutions: decision, score, and reason codes. Decision is applicable for solutions that provide the final determination of whether the event is associated with an acceptable or unacceptable level of risk. Even with apparently binary circumstances like determining whether an applicant's personal information matches information in selected data sets, some flexibility is necessary to assess risk associated with "fuzzy matching," where a legitimate applicant might transpose two numbers or use a variant spelling.

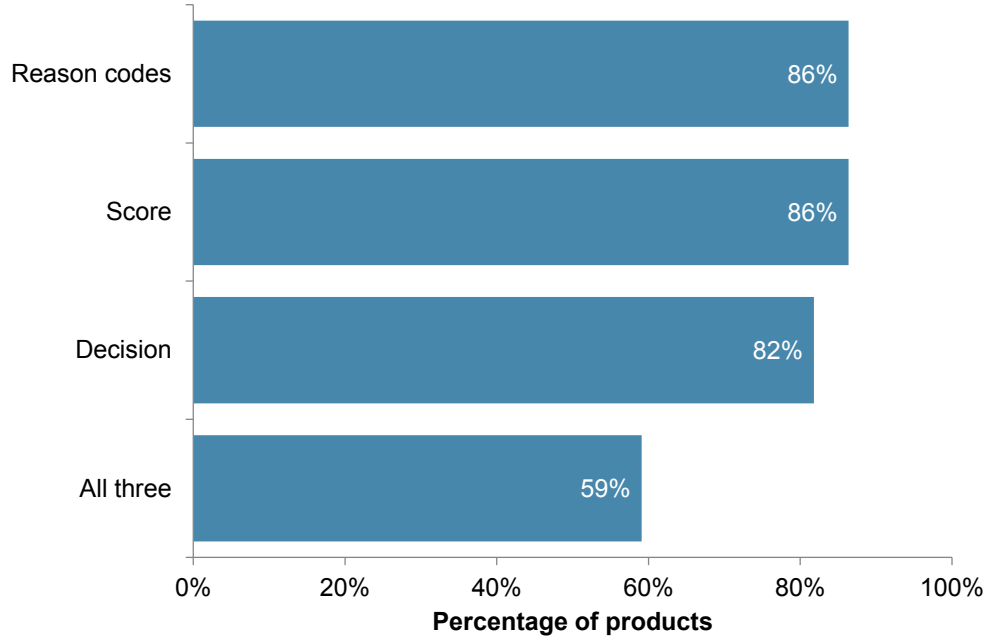
Providing a score as an output can offer somewhat more nuance than an outright pass/fail decision and gives institutions using the solution a greater ability to adjust thresholds for approving, flagging, or rejecting an applicant based on the level of risk. However, on their own, scores and decisions risk excessive opacity.

Reason codes provide necessary insight into the types of fraud schemes currently targeting an institution and, crucially, where to impose tighter restrictions on fraudsters or loosen rules to avoid burdening legitimate applicants. A robust set of reason codes, combined with a flexible rules engine, can give institutions granular control over their identity proofing solutions.

While each type of output is widely adopted among identity proofing products, with each being offered by more than 8 in 10 of the providers covered in the scorecard, just over half of providers offer all three output types (Figure 10).

Half of ID Proofing Vendors Offer a Full Range of Outputs

Figure 10. Reporting Outputs Available



Source: Javelin Strategy & Research, 2017

In addition to accommodating a variety of customer-facing use cases, identity proofing solutions should also support multiple applications in order to provide the broadest value to customers. Ad-hoc processing, offered by 77% of platforms, is crucial to supporting internal fraud analysts conducting manual reviews of flagged events (Appendix, Figure 12).

Supporting this feature requires enabling analysts to manually query the system for additional information around an individual, whether this is for additional context on an identity or for details about whether a device has been associated with access to any other accounts. Obviously, this will not be applicable to certain types of identity proofing tools; behaviometrics, for instance, necessarily cannot have any ad-hoc query capabilities.

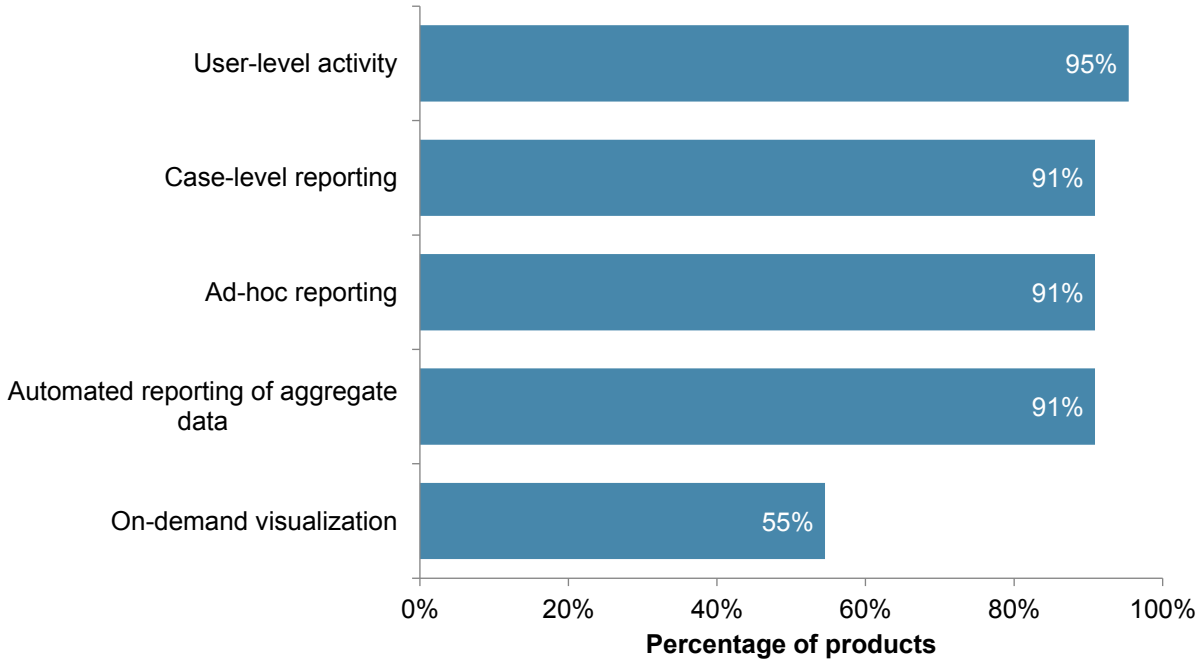
ADMINISTRATION

Many identity proofing tools can provide users with access to tremendously sensitive information about accountholders and applicants, including their PII and account history. This requires reasonable controls to be placed around access to these tools to protect them against unauthorized use and to monitor for misuse by an apparently legitimate user.

The particular level of authentication required to operate an identity proofing tool depends on the sensitivity of the information it is able to access. Data validation tools that can compile the records of an applicants' PII and financial history obviously require additional safeguards, compared to device risk assessment tools, because the former could later be used to perpetrate identity fraud against the applicant should the information fall into the wrong hands.

On-Demand Visualization Represents an Opportunity for Vendors

Figure 11. Integrated Reporting Features



Source: Javelin Strategy & Research, 2017

Integrating the capability to automatically generate periodic reports can help support business functions. Reports for the past month or quarter are likely to be needed for business teams assessing macro-level trends in the types of fraud targeting their institution as well as the efficacy of their solutions. Reporting on user-level activity can provide additional accountability against rogue users who misuse identity proofing solutions to commit insider fraud.

As analytic tools grow in sophistication, vendors have a significant opportunity to distinguish themselves. Although nearly all providers in the scorecard use other types of reporting, only 55% offer on-demand visualization (Figure 11). Visualization tools can be particularly beneficial to analysts investigating clusters of suspicious cases that might be linked by a handful of commonalities. These kinds of cluster analyses are difficult to conceptualize outside of a visual format.

VENDOR PROFILES

For this scorecard, Javelin included 23 vendors that agreed to participate and complete a self-evaluation with details around their products' capabilities in verifying the identity of individuals in a variety of contexts. Javelin independently verified vendor capabilities against publicly available information, where it was available.

For each vendor, Javelin compiled individual profiles that include company information and product descriptions as provided by the vendor, along with details about its category scores and a brief assessment from Javelin.

Vendors Evaluated	
AU10TIX	Jumio
BehavioSec	LexisNexis Risk Solutions
BioCatch	Mitek
DataVisor	Neustar
Early Warning Services	NuData Security, a Mastercard company
Equifax	RSA
Experian	Socure
FICO	ThreatMetrix
Gemalto	TransUnion
GIACT Systems	Trulioo
ID Analytics	Trusona
IDology	

Company: AU10TIX

Product: AU10TIX BOS

URL: www.au10tix.com

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

AUT10TIX's BOS ID brings in customers by scanning not just their documents but by doubling down and identifying their faces, so as to meet the tailored needs of FIs and other client organizations.

Company profile, according to AU10TIX:

"AU10TIX is the forerunner of 2nd generation ID authentication and onboarding technology. AU10TIX technology powers legacy banks and leading financial institutions. AU10TIX is designed to enable faster customer acquisition at higher operating efficiency while enhancing robustness of fraud prevention and KYC compliance. AU10TIX 2nd generation technology offers multi-factor ID authentication, direct record generation and intelligent face-matching. The entire process is 100% automated, and completes in seconds. As full service provider AU10TIX offers augment Selfie-to-I as well as identity verification and screening services. AU10TIX is a subsidiary of ICTS International N.V, one of the world's leading airport security companies for almost 30 years."

Product description, according to AU10TIX:

"AU10TIX BOS is the first 2nd generation ID authentication and Onboarding automation platform on the market. BOS enables fully-automated ID document capture, auto-recognition, relevance-screening, content extraction and document authentication as well as multi-modal biometric Selfie-to-ID face matching and additional Electronic Data Verification & Screening (EDVS) services."

Company: BehavioSec

Product: BehavioSec, BehavioSense

URL: https://www.behaviosec.com/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Recent partnerships with Kount and Gemalto prove that BehavioSec's suite of identity proofing tools is winning strong support in the market. Next year, with continuing enhancements to their technology, Javelin expects the company to be even more competitive.

Company profile, according to BehavioSec:

"BehavioSec provides a layer of security that lets customers authenticate themselves through the unique ways they type, swipe and hold their devices. Behavioral biometrics uses continuous machine learning and realtime feedback to create a risk score, separating good users from bad actors by detecting anomalies in behavior. Billions of transactions have been completed using BehavioSec verification every year."

Product description, according to BehavioSec:

"BehavioSec technology helps solve the authentication and verification problem, faced by mobile applications & web logins without impacting the end user experience. The solution brings a new dimension to security by verifying the identity of the end-user through a cost effective risk-based mechanism that does not require any change in user behavior."

Company: BioCatch

Product: BioCatch Solution

URL: https://www.biocatch.com/

SCORECARD PERFORMANCE

FUNCTIONAL	INNOVATIVE	TAILORED
		

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

BioCatch, as a stand-alone solution, has room to grow. But it has proven to be a worthy partner, working with Experian to strengthen its market-leading CrossCore platform with its behavioral biometrics technology.

Company profile, according to BioCatch:

"BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and precious data. Founded in 2011 by experts in neural science research, machine learning and cybersecurity, BioCatch is used by banks and other enterprises to reduce online fraud and protect against cyber threats, without compromising user experience. With an extensive patent portfolio and deployments at major companies worldwide that cover tens of millions of users to date, BioCatch has established itself as an industry leader for behavioral biometrics."

Product description, according to BioCatch:

"BioCatch's behavioral biometrics platform is the bedrock of the entire solution. Focusing on preventing fraud while providing online and mobile users with a frictionless experience, the BioCatch platform develops behavioral biometric profiles of online users to recognize a wide range of human and non-human - malware, remote access Trojans (RATs), robotic activity - cybersecurity threats. The BioCatch Behavioral Biometrics Platform has three main capabilities: Identity Proofing, Authentication, and Threat Prevention."

Company: DataVisor

Product: ID Theft & Synthetic ID Prevention

URL: https://www.datavisor.com

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	
New device enrollment	
New biometric enrollment	
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

DataVisor's ID Theft & Synthetic ID Prevention service runs the gamut within Javelin's FIT model. From laggard to a fast follower, and, yes, even leader in the advisory's tailored category. And its combination of approaches to artificial intelligence distinguish DataVisor's tool among its peers.

Company profile, according to DataVisor:

"DataVisor is a Big Data fraud detection company that protects large online services and financial institutions against coordinated fraud and suspicious activity. Founded in 2013 by Internet security experts, DataVisor's proprietary unsupervised machine learning technology finds new, unknown fraud attack patterns in real-time before they do damage. DataVisor is a proven application of unsupervised machine learning for fraud prevention at high precision and large scale."

Product description, according to DataVisor:

"The DataVisor solution deploys unsupervised machine learning in real-time to prevent synthetic and stolen identities used at account opening, fraudulent card transactions and wire transfers, account takeovers, and more. This approach finds correlations across accounts to prevent coordinated fraud from doing damage. Built on the latest Big Data technologies, DataVisor utilizes unsupervised machine learning, supervised machine learning, and its Global Intelligence Network of 2B+ accounts to provide unparalleled precision and recall. The solution returns fraud scores and reason codes in real-time or batch, which can be consumed programmatically or through an easy-to-use UI."

Company: Early Warning Services

Product: ID Confidence Score, Mobile Identity & Mobile Status

URL: https://earlywarning.com/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	X
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:
Early Warning Services' Identity and Authentication Solutions are among the most utilitarian suites that Javelin evaluated. With a variety of features to apply to a broad array of use cases, from new account opening to remote deposit capture, FIs with diverse needs should seriously consider Early Warning.

Company profile, according to Early Warning Services:
"Creating the Future of Payments™ — Early Warning delivers innovative payment and risk solutions to financial institutions nationwide. For over 25 years, Early Warning has been a leader in technology that helps money move easy, fast and safer. The company provides real-time payments, authentication, and risk mitigation solutions to a network of more than 2,300 financial institutions, government entities, and payments companies."

Product description, according to Early Warning Services:
"Identity and Authentication Solutions includes ID Confidence Score, which uses analytics and resolution technology to predict the likelihood that an individual is presenting their identity. It also blends proprietary and third party data sources with predictive analytics, allowing organizations to better detect manipulated and synthetic identities by confidently distinguishing between verified and suspect identity credentials. Authentication Solutions include Mobile Identity, Mobile Status and Mobile Authentication, which utilize MNO (mobile network operator) insights to authenticate both person and device, ensuring the device is valid on the network, validating the person using the device is authorized and providing visibility of changes to the account."

Company: Equifax

Product: FraudIQ Authenticate

URL: http://www.equifax.com

SCORECARD PERFORMANCE

FUNCTIONAL	INNOVATIVE	TAILORED
		

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Simply put, Equifax's FraudIQ Authenticate tool is extremely functional. It allows for effective identity proofing during new account opening, reauthentication, and device enrollment.

Company profile, according to Equifax:

"Equifax is a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions. The company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."

Product description, according to Equifax:

"FraudIQ®Authenticate is a set of risk-based authentication tools delivered through a flexible platform that you can use to confirm identities and help ensure the security and authenticity of account applications and transactions. Rather than relying on only one type of authentication method, FraudIQ Authenticate allows you to waterfall to the most relevant and effective method for a given transaction, from passive, behind-the-scenes device recognition to more stepped-up methods like knowledge-based authentication and facial matching for riskier transactions."

Company: Experian

Product: CrossCore

URL: www.Experian.com

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Experian's identity proofing platform is a strong performer in every category of Javelin's FIT model. It is functional. It is innovative. And, most important, it is tailored toward the advisory's expectations. The comprehensive nature of CrossCore makes it the market-leading solution for identity proofing.

Company profile, according to Experian:

"Experian has spent the past few years expanding the fraud and ID proofing technologies and services it offers. While the solutions are sector-neutral, the company focuses primarily on financial services, telecommunications, insurance, healthcare, public sector, retail, e-commerce and travel. The offering includes a suite of fraud management products including device intelligence, identity authentication, risk assessment, and, when necessary, knowledge-based authentication."

Product description, according to Experian:

"CrossCore is the first smart plug-and-play platform for fraud and identity services. It combines a flexible, scalable API with powerful workflow and decisioning strategy capabilities. CrossCore enables fraud teams to connect and optimize a portfolio of best-in-class solutions — including Experian and other partners — in concert with existing systems. CrossCore delivers a future-proof way to modify strategies quickly, catch fraud faster, improve compliance and enhance the customer experience."

Company: FICO

Product: Application Fraud Manager

URL: https://www.FICO.com/

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	
New device enrollment	
New biometric enrollment	
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

FICO's Application Fraud Manager leads a field of its peers. The introduction of narrow, unsupervised machine learning technology (or artificial intelligence) in the identity proofing solution makes it a powerful tool for fighting fraud.

Company profile, according to FICO:

"FICO (NYSE: FICO) is a leading analytics software company, helping businesses in 90+ countries make better decisions that drive higher levels of growth, profitability and customer satisfaction. The company's groundbreaking use of Big Data and mathematical algorithms to predict consumer behavior has transformed entire industries."

Product description, according to FICO:

"Prevent first-and third-party application fraud through detection across multiple products and channels. Gain access to world-class analytics that can be deployed quickly to protect new products and enhance existing fraud investments.

FICO® Application Fraud Manager can help businesses in any industry to stop credit fraud where it starts: at the point of application. This FICO solution gives firms in a wide range of industries — banking, insurance, telecommunications, retail, government and more — access to FICO's market-proven, industry-leading analytic technology."

Company: Gemalto

Product: Assurance & Authentication Hub

URL: https://www.gemalto.com

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:
Within Javelin's FIT model, Gemalto's Assurance and Authentication Hubs are strong contenders. While geared primarily toward authentication, the technology, which supports biometric and new device enrollment, is sure to be an identity proofing solution to watch.

Company profile, according to Gemalto:

"Gemalto is a global leader in digital security, with 2016 annual revenues of €3.1 billion and customers in over 180 countries. Gemalto's goal is to bring trust to an increasingly connected world."

Product description, according to Gemalto:

"Gemalto Assurance Hub (GAH) is an open hub that allows banks to assess every single online banking session in real-time. It comes with pre-integrated solutions to analyze a broad range of attributes and signals from the user and the device, such as geo-location, device profiling, IP address, device assessment and behavioral biometrics.

Based on a set off rules defined in the Policy Manager, GAH evaluates the level of assurance banks should monitor for every single transaction performed by their customers and recommends the most appropriate authentication methods. Gemalto Assurance Hub helps financial players make the right choice to minimize fraud: allow the transaction, block the transaction or challenge the customer with a step-up authentication."

Company: GIACT Systems

Product: gIDENTIFY

URL: www.giact.com

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	X
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

GIACT Systems' suite of identity proofing tools is quickly moving into contention with leaders in the industry. This under-the-radar company provides one of the most functional solutions in the market. That is a plus for FIs looking for a fully featured solution outside some of the more well-known brands.

Company profile, according to GIACT:

"GIACT has been helping companies verify valued customers since 2004. As a leader in providing real-time payment risk services, our identification, verification, authentication, and mobile solutions minimize risk and fraud exposure, enabling organizations to focus on providing unmatched, frictionless customer experiences. Since our founding, we've processed billions of transactions for our more than 1,000 customers."

Product description, according to GIACT:

"gIDENTIFY uses multiple data sources to confirm consumer and business identities so you can address your underwriting, risk management, and Know Your Customer (KYC) compliance requirements. By using the most current data to evaluate over 100,000 attributes, gIDENTIFY is designed to provide superior accuracy."

Company: ID Analytics

Product: ID Connect Resolution, Comply360

URL: https://idanalytics.com/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	
New biometric enrollment	
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

As an identity proofing tool, ID Analytics is a fast follower among its peers. It still, however, has room to grow. Adding innovative features designed to support biometric enrollment and mobile remote deposit capture would be strong next steps for the relatively recent addition from Symantec's acquisition of LifeLock.

Company profile, according to ID Analytics:

"ID Analytics is a leader in consumer risk management with patented analytics, proven expertise, and near real-time insight into consumer behavior. By combining proprietary data from the ID Network® — one of the nation's largest networks of cross-industry consumer behavioral data — with advanced science, ID Analytics provides in-depth visibility into identity risk and creditworthiness. Every day, many of the largest U.S. companies and critical government agencies rely on ID Analytics to make risk-based decisions that enhance revenue, reduce fraud, drive cost savings, and protect consumers. ID Analytics is a Symantec company."

Product description, according to ID Analytics:

"ID Connect Resolution (IDCR) improves the account enrollment experience, driving higher conversion rates while mitigating fraud. Using only a small subset of input about a customer, ID Connect resolution is able to find the full identity information about that person, verify those elements, and ultimately provide them back to the business to streamline the enrollment process.

Comply360 is a cutting edge compliance suite which screens and verifies submitted identities, returning a letter grade that summarizes the assessment along with individual verification binary indicators for each identity element on the application. The solution also has the capability to return contrary data for identity elements which cannot be verified, notifying organizations of verifiable identity element(s) associated with a submitted identity."

Company: IDology

Product: ExpectID

URL: https://www.idology.com/

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

IDology provides a full-service identity proofing platform. The depth of features in the ExpectID tool makes it a contender in every category in Javelin's FIT model and a worthwhile consideration for organizations looking for a new identity proofing solution.

Company profile, according to IDology:

"IDology is a leading provider of multi-layered identity verification and fraud prevention solutions for organizations operating in a consumer-not-present environment. Founded in 2003, the Atlanta-based company delivers an innovative solutions suite and a fraud prevention platform that empowers organizations to assess overall transaction risk and improves the customer experience."

Product description, according to IDology:

"IDology's ExpectID suite enables businesses and government entities to leverage on demand features that minimize friction for legitimate customers, maintain compliance and decrease instances of fraud by staying ahead of evolving fraud tactics. The ExpectID platform uses an on-demand, flexible, layered approach to identity verification combining activity, identity, location and device attributes. Another key component of the platform is that it helps customers collaborate to prevent more fraud. The IDology Collaborative Fraud Network with industry-wide collaborative velocity and alert tools that have been instrumental in lowering fraud rates for our customers."

Company: Jumio

Product: Netverify

URL: https://www.jumio.com

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Netverify is a fast follower in the field of identity proofing solutions. The promise of new features, along with an increasing number of partnerships, means that the technology may make it increasingly competitive in Javelin's FIT model in years to come.

Company profile, according to Jumio:

"Jumio delivers the next-generation in digital ID verification, enabling businesses to reduce fraud and increase revenue while providing a fast, seamless customer experience. Jumio uses computer vision technology to verify credentials issued by over 200 countries in real-time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, retail, travel and online gaming sectors."

Product description, according to Jumio:

"Netverify combines ID Verification, Identity Verification, and Document Verification for a comprehensive solution to establish the real-world identity of consumers. Leveraging advanced technology including biometric facial recognition and machine learning, Jumio helps businesses meet regulatory compliance including KYC and AML, reduce fraud, and provide a secure experience. Netverify provides an intuitive and satisfying user experience that takes just minutes to complete and seamlessly integrates into websites, iPhone, or Android applications. Jumio is PCI Level 1 compliant and regularly conducts security audits to ensure compliance with security best practices."

Company: LexisNexis Risk Solutions

Product: LexisNexis® Risk Defense Platform

URL: http://lexisnexis.com/risk/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:
LexisNexis® Risk Defense Platform lives up to its name. It fits with Javelin's expectations: providing a deeply functional solution to the increasingly complex problem of identity proofing.

Company profile, according to LexisNexis Risk Solutions:
"LexisNexis Risk Solutions believes in the power of data and advanced analytics for better risk management. With over 40 years of expertise, LexisNexis Risk Solutions is a trusted data analytics provider for organizations seeking actionable insights to manage risks and improve results while upholding the highest standards for security and privacy. Headquartered in metro Atlanta, USA, LexisNexis Risk Solutions serves customers in more than 100 countries and is part of RELX Group, a global provider of information and analytics for professional and business customers across industries."

Product information, according to LexisNexis Risk Solutions:
"The LexisNexis® Risk Defense Platform is a configurable and adaptable policy decisioning engine designed to help your business efficiently manage complex fraud, while ensuring a positive customer experience with onboarding, login, authentication or account management.

The LexisNexis® Risk Defense Platform creates one connection point that links a client's business to a robust set of fraud and identity capabilities and intelligent reporting metrics that help improve the ability to achieve secure authentication and attain the workflow agility to keep a client's fraud deflection strategy ahead of the next big threat, while servicing the good customers with less friction."

Company: Mitek

Product: Mobile Verify

URL: www.miteksystems.com

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	
New biometric enrollment	X
Mobile remote deposit capture	X
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:
Mitek's suite of identity proofing solutions is heavily geared toward verification of physical identity documents, and while performing well in the tailored category, has room to grow in its diversity of features.

Company profile, according to Mitek:
"Mitek is a global leader in mobile capture and identity verification software solutions. Mitek's identity verification solutions allow an enterprise to verify a user's identity during a digital transaction. This enables financial institutions, payments companies and other businesses operating in highly regulated markets to mitigate financial risk and meet regulatory requirements while increasing revenue from digital channels. Mitek also reduces the friction in the users' experience with advanced data prefill and automation of onboarding processes. Mitek's innovative solutions are embedded into the apps of more than 5,800 organizations and used by more than 80 million consumers."

Product description, according to Mitek:
"Digital leaders trust Mobile Verify® because of its proven, customer friendly user experience and market-leading platform built on latest advancements in AI and machine learning. Mobile Verify® enables identity verification by authenticating government issued identity documents in real-time and then tying the person to the document through facial biometric matching of the face on the document to a selfie. Mobile Verify with NFC runs authenticity checks using the data embedded on RFID chips in millions of identity documents. For additional identity assurance, Mobile Verify offers checks against external data sources and the ability to easily capture and submit trailing documents for proof of address, income and more."

Company: Neustar

Product: OneID Fraud Prevention

URL: https://www.neustar.com

SCORECARD PERFORMANCE

FUNCTIONAL	INNOVATIVE	TAILORED
		

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Neustar's OneID Fraud Prevention tool has room to grow. Support for broader use cases, such as new biometric enrollment, and more innovative features would have made it more competitive in this year's field of identity protection solutions. That said, partnerships with Pandora and Tru Optik, and a solid set of base features, mean that the product will continue to be in contention for years to come.

Company profile, according to Neustar:

"Neustar is in the business of knowing with certainty who is at the end of every online interaction, and is trusted by the world's great brands to make critical decisions some 20 billion times a day. Neustar's goal is to authoritatively tell a client exactly who they are connecting with, allowing for critical real-time decisioning."

Product description, according to Neustar:

"The Neustar Fraud Prevention solution helps protect clients from multiple attack vectors by integrating online and offline fractional identifiers to verify consumer identities and the devices they use in every transaction. Neustar utilizes a layered approach to fraud prevention and strongly believes the power to link multiple online and offline identity attributes, landline, mobile phone, IP addresses and device fingerprinting attributes can help prevent sophisticated fraud attacks."

Company: NuData Security, a Mastercard Company

Product: NuDetect

URL: https:// nudatasecurity.com/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	X
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

NuData Security is a strong leader in the field of identity proofing. Geared more toward authentication than identity verification, the NuDetect tool is one of the most innovative solutions in the market.

Company profile, according to NuData Security:

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

Product description, according to NuData Security:

"NuDetect identifies the high-risk accounts that are most likely to lead to brand damage from fraudulent activity — the moment an account is created and throughout the lifetime of the account. NuDetect is also designed to verify if a user is the genuine user or it flags them as an imposter, machine, malware or other high-risk entity. Organizations who verify customer behavior can make informed decisions to reduce authentication requirements for a seamless customer experience while stopping fraud.

NuDetect's behavioral analytics software understands how real users behave in order to help decision makers identify high-risk behaviors and remove good customers from the review queue. NuDetect is on track to analyze 200 billion online interactions in 2017."

Company: RSA

Product: Adaptive Authentication

URL: https://www.rsa.com

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

RSA's business-friendly Adaptive Authentication addresses one of the biggest issues facing FIs — authentication — but an absence of key identity-verification capabilities largely restricts the use of Adaptive Authentication to post-approval, identity proofing scenarios.

Company profile, according to RSA:

"RSA delivers transformational business-driven security solutions helping over 30,000 customers comprehensively and rapidly link security incidents with business context to respond effectively and protect what matters most. With award-winning solutions for rapid detection and response, identity and access assurance, consumer fraud protection, and business risk management, RSA customers can thrive in an uncertain, high-risk world."

Product description, according to RSA:

"RSA Adaptive Authentication is a leading consumer-focused, comprehensive risk-based authentication and fraud detection platform. Powered by RSA's risk-based authentication technology, it's designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators. A risk score is assigned to each activity, and users are challenged only when an activity is identified as high-risk or an organizational policy is violated. Through a combination of granular risk scoring, policy and case management, RSA Adaptive Authentication enables organizations to strike the right balance between security and convenience across digital channels."

Company: Socure

Product: ID+

URL: https://www.socure.com/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	X
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Socure's ID+ suite is an up-and-coming contender among the identity proofing solutions that Javelin evaluated. Strong partnerships with AU10TIX, unique features, and the introduction of new APIs will put the company in a strong position to compete for leadership positions next year.

Company profile, according to Socure:

"Socure is a leader in creating high-assurance digital identity verification technology. Its predictive analytics platform applies artificial intelligence and machine-learning techniques with trusted online/offline data intelligence from email, phone, address, IP, social media and the broader Internet to authenticate identities in real-time."

Product description, according to Socure:

"Socure ID+ is a real-time predictive analytics platform that combines the newest forms of machine learning and artificial intelligence with digital, offline and social identity data to deliver accurate and robust KYC, identity verification and fraud risk prediction solution in the market. From a single RestFul API, Socure delivers email, phone, and address riskScore, NAPE correlation models, overall identity fraud risk prediction, KYC/CIP, AML Watchlist and physical document verification services. Socure's digital-to-physical identity verification platform, with a fully integrated Document Authentication service (powered by Au10tix), extends ID+ digital identity verification capabilities to determine the likelihood that a government issued ID is authentic and associated with the PII provided."

Company: ThreatMetrix
Product: ThreatMetrix Digital Identity Intelligence, ThreatMetrix Dynamic Decision Platform, ThreatMetrix Smart Authentication
URL: www.threatmetrix.com

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	

COMPANY AND PRODUCT INFORMATION

Javelin's take:
The only company that was a leader in multiple categories, ThreatMetrix offers a suite of identity proofing products that is among the fittest of all the identity proofing suites Javelin evaluated.

Company profile, according to ThreatMetrix:
"ThreatMetrix®, the Digital Identity Company®, provides an end-to-end platform for digital identity intelligence and trust decisioning. Our solutions recognize up to 95 percent of returning website visitors. We instantly detect high-risk transactions and dynamically score them, enabling digital businesses to safely grow online revenue and personalize the digital experience for trusted customers.
We believe security doesn't need to come at the expense of profitability. Security and fraud prevention simply needs to be better, not harder for legitimate customers. That's profitability and security without compromise."

Product description, according to ThreatMetrix:
"ThreatMetrix Digital Identity Intelligence performs risk-based scoring of transactions in real time. Our highly unique approach to authentication and fraud prevention uses dynamic behavioral history from across the Digital Identity Network® — creating true digital identities that can't be faked or replicated.

ThreatMetrix® Dynamic Decision Platform® puts digital identity intelligence to work. The market-leading Dynamic Decision Platform provides enhanced authentication, identity verification and fraud decisioning. Integrating Digital Identity Intelligence with behavioral analytics and machine learning capabilities, the platform also incorporates third-party data sources for exception handling. Case management helps to isolate and investigate transactions that require further review.

ThreatMetrix® Smart Authentication™ combines the frictionless experience of market-leading risk-based authentication (RBA) with strong customer authentication (SCA) in a comprehensive solution."

Company: TransUnion

Product: IDVision

URL: https://www. transunion.com/

SCORECARD PERFORMANCE

FUNCTIONAL INNOVATIVE TAILORED

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

All three of the major credit reporting agencies, Experian and Equifax included, have recognized FIs' needs for identity proofing services. But only TransUnion, in Javelin's view, outperforms its closest competitors in innovation. Its IDVision tool isn't only on the lookout for true name fraud, it checks for instances of synthetic fraud, protecting FIs from fabricated-identity crimes.

Company profile, according to TransUnion:

"TransUnion realizes that Information is a powerful thing. The company is dedicated to finding innovative ways information can be used to help individuals make better and smarter decisions. TransUnion helps uncover unique stories, trends and insights behind each data point, using historical information as well as alternative data sources. This allows a variety of markets and businesses to better manage risk and consumers to better manage their credit, personal information and identity. Today, TransUnion has a global presence in more than 30 countries and a leading presence in several international markets across North America, Africa, Latin America and Asia. Through the power of information, TransUnion is working to build stronger economies and families and safer communities worldwide."

Product description, according to TransUnion:

"TransUnion's IDVision suite offers powerful end-to-end fraud and identity solutions that enable clients to say 'YES' with confidence. TransUnion delivers a superior consumer experience while providing greater certainty by delivering the whole picture of customers, their digital behaviors and transactions through a combination of superior data, predictive analytics that anticipate evolving threats, and flexible delivery."

Company: Trusona

Product: Identity Authentication Suite

URL: https://www.trusona.com/

TRUSONA
When you truly need to know

SCORECARD PERFORMANCE

FUNCTIONAL **INNOVATIVE** **TAILORED**

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	X
New biometric enrollment	X
Mobile remote deposit capture	X
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

This year, Trusona's Identity Authentication Suite found itself in strong contention among its peers. In Javelin's view, the unique combination of technologies and its insurance feature make it distinct in the market and one to watch.

Company profile, according to Trusona:

"Trusona is a global leader in Identity Authentication. The Trusona Identity Authentication Suite offers a range of solutions spanning from frictionless, no password login to only insured authentication solution. Trusona is leading the #NoPasswords Revolution where there are no passwords to be created, remembered, stolen, or compromised — ensuring the people are who they say they are and no one else can. Trusona is being utilized across government, health care, finance, and media corporations. The company was founded in 2015 by CEO and cybersecurity expert Ori Eisen and is funded by Kleiner Perkins and Microsoft Ventures."

Product description, according to Trusona:

"The Trusona Identity Authentication Suite offers three levels of Identity Authentication solutions which do not require username or password.

All solutions are initiated by a tap and rely on patented anti-replay technologies that use the unique nature of every authentication to prove the True Persona behind every digital interaction."

Company: Trulioo

Product: GlobalGateway

URL: https://www.trulioo.com

SCORECARD PERFORMANCE

FUNCTIONAL	INNOVATIVE	TAILORED
		

Applicable Use Cases	
New account opening	X
Reauthentication/step-up authentication	X
New device enrollment	
New biometric enrollment	X
Mobile remote deposit capture	
Other	X

COMPANY AND PRODUCT INFORMATION

Javelin's take:

Trulioo's GlobalGateway tool is fast extending its reach worldwide, inking partnerships and deals across the globe. The sheer spread of its technology means that it will continue to grow and adapt to new markets and customer needs, and it is well-suited for organizations with global identity proofing needs.

Company profile, according to Trulioo:

"Headquartered in Vancouver, Trulioo is a Canadian RegTech company tackling one of the most ambitious challenges in identity verification — to build a universal solution for fraud, risk mitigation, and regulatory compliance systems worldwide. Trulioo is a leading global identity verification provider, enabling businesses from all over the world access to 4.5 billion consumers in over 60 countries via 200 data sources, including the ability to authenticate more than 3,500 identity documents from nearly every country in the world - all through a single API."

Product description , according to Trulioo:

"GlobalGateway, Trulioo's online electronic identity verification (eIDV) platform, is used by over 500 businesses worldwide to reduce fraud, mitigate risks, and comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) rules.

Developed for an international market, GlobalGateway was created to help build a layer of trust and safety online and therefore help businesses and organizations around the world to instantly verify identities through a single integration and contract."

APPENDIX

Functional, Innovative, and Tailored (FIT) Capability Table

Figure 12. Percentage of Vendors Offering Certain Features, by Category

FUNCTIONAL	
Channels supported	
Online	100%
Mobile	100%
Phone	77%
In-branch	82%
Channel agnostic	86%
Other	27%
Key feature types	
Data validation	77%
KBA	34%
Document scanning	50%
Bot detection	73%
Device fingerprinting	70%
Email verification	73%
One-time passwords	52%
Remote access detection	50%
Behaviometrics	41%
Other	59%
Regulatory regime	
FCRA	23%
GLBA	41%
Other	9%
Information sources	
Credit reporting agencies	50%
Mobile network operators	68%
Public records	59%
Employment records	23%
Utility records	50%
Social network data	45%
Consortium	68%
Account ownership verification	59%
Other	41%
Feedback cycle	
Clients identify correctly/incorrectly flagged cases	95%
Able to prefill information	
Able to prefill information	50%
INNOVATIVE	
Key feature types	
Remote access detection	50%
Behaviometrics	41%
AI/Machine learning	
Suggested by AI, implemented by human	77%
Suggested by AI, implemented independently	55%
Information sources	
Mobile network operators	68%
Social network data	45%
Consortium	68%
Account ownership verification	59%
Insurance against losses	
Insurance offered	2%
Maximum coverage	5%
Authentication available	
Security key/smartcard	14%
Able to prefill information	
Able to prefill information	50%

TAILORED	
Product output	
Score	86%
Decision	82%
Reason codes	86%
All three	59%
Customizable rules	
By client	82%
Through provider	91%
Professional services	100%
Ad-hoc processing	
Ad-hoc processing	77%
How quickly are decisions rendered	
Batch	59%
Near-real time	95%
Integrated case manager	
Integrated case manager	32%
Types of access controls available	
No authenticated login portal	23%
Single user privilege level	36%
Individual user privileges	77%
Authentication available	
Username/password	91%
SSO	55%
One-time passwords	23%
Security key/smartcard	14%
Other	27%
Integrated reporting	
Automated reporting of aggregate data	91%
Ad-hoc reporting	91%
Case-level reporting	91%
User-level activity	95%
On-demand visualization	55%
Other	9%
Delivery options	
SaaS	82%
Hosted	50%
On-Premise	45%
Cloud	77%
Other	10%
Pricing model	
Per transaction	91%
Per user	36%
Per year	41%
Product testing	
Historical data	82%
Production data (live)	95%
Production data (mirrored)	68%
Integration	
API	100%

Source: Javelin Strategy & Research, 2017

METHODOLOGY

For this scorecard, Javelin included 23 vendors that agreed to participate and complete a self-evaluation with details around their submitted products' capabilities in verifying the identity of individuals both at account opening and throughout the customer relationship. For vendors with multiple products, only those that were submitted and relevant to identity proofing 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 60% of total points, Innovative accounting for 20%, Tailored accounting for 20%.