Market Guide for Identity Proofing and Corroboration

Published 24 April 2018 - ID G00325713 - 29 min read

By Analysts Tricia Phillips, Jonathan Care, Danny Luong, Ant Allan

The identity of new customers cannot be absolutely verified ("proven"), but high confidence in identity is crucial to protect customers and revenue. Security and risk management leaders must discard flawed legacy methods and embrace analytics that evaluate multiple positive and negative signals.

Overview

Key Findings

- Data breaches have led to rampant compromise of personally identifiable information (PII). As a result, correctly reciting PII is worthless as a stand-alone method of corroborating a person's claimed identity.
- Onerous "identity proofing" methods for new-account opening and as part of step-up or multifactor authentication use cases increase customer abandonment. This creates a competitive liability when customer attrition and market share loss exceed the potential fraud loss.
- Many technologies used in online fraud detection use cases, such as device reputation, can be used in identity proofing and substantiation use cases. In addition, these technologies can be invoked to elevate trust during subsequent interactions.

Recommendations

Security and risk management (SRM) leaders with a responsibility for fraud prevention and secure payment, as well as those responsible for underwriting functions or authentication strategy must:

- Invest in new technologies now to bolster or replace legacy identity proofing tools and processes. Accept that any sense of security that comes from using highly compromised static data as a means of corroborating identity is a dangerous illusion.
- Build a business case for the addition of new approaches for identity proofing use cases that focuses on fraud reduction and credit write-offs, as well as increased revenue from lower false-positive rates, lower abandonment rates, and improved customer experience and loyalty.
- Extend the use of identity proofing and corroboration techniques beyond new-account use cases to login, account maintenance and transactional use cases.

Market Definition

Identity proofing and corroboration is the combination of activities during an interaction that brings an identity claim within organizational risk tolerance, such that:

1. The real-world identity exists
2. The individual claiming the identity is in fact the authentic possessor of that identity

This process must align three aspects of identity — the real-world identity, the digital identity and the person submitting the identity claim.

Market Description

This Market Guide focuses on identity proofing and substantiation use cases in remote (non-face-to-face) interactions (online, mobile web, mobile app, interactive voice response [IVR] or voice-based calls).

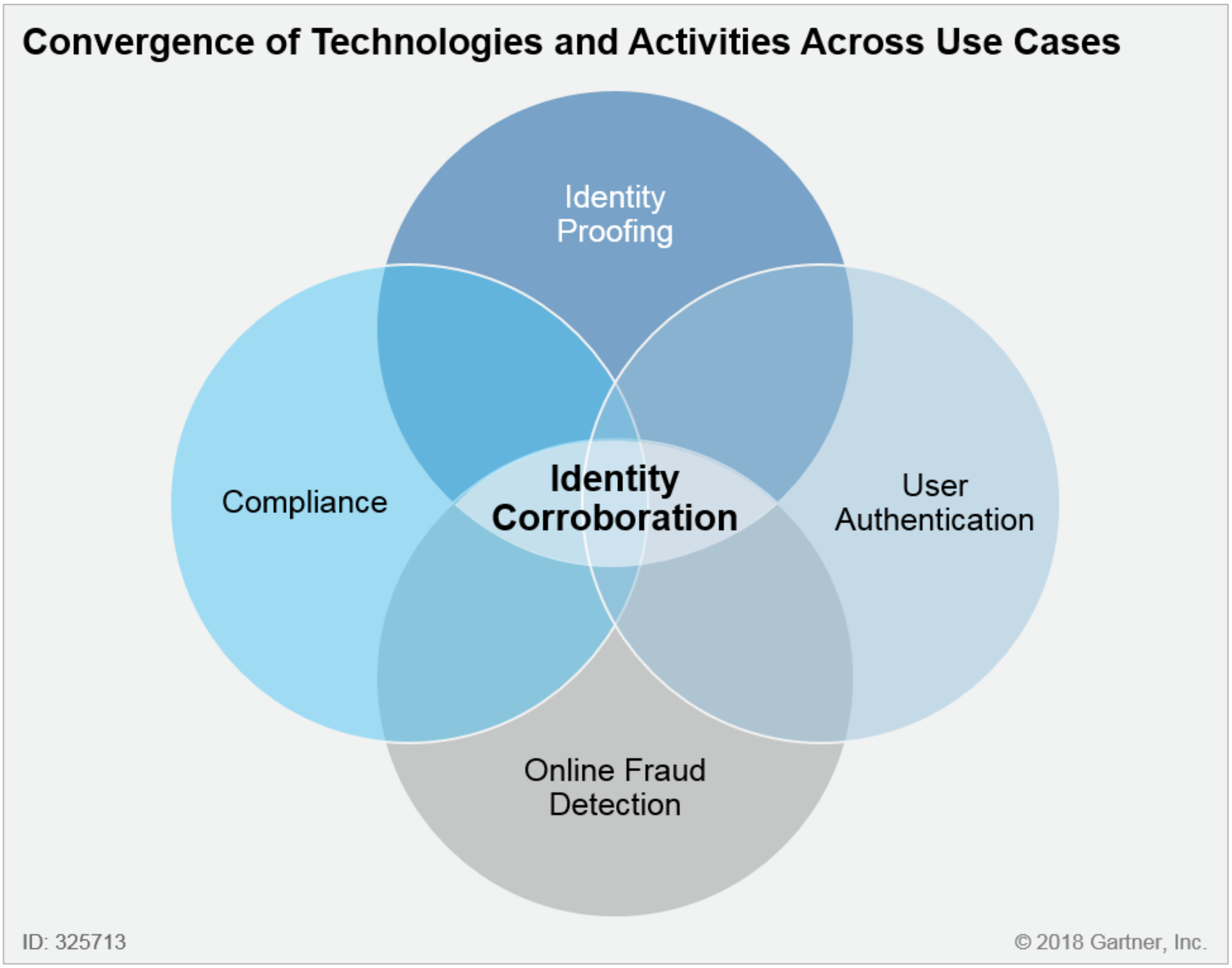
Historically, the verification of static PII served the function of "identity proofing" based on the premise that if a person was able to provide a name, address, date of birth and a government identifier (e.g., Social Security number), he or she must be that person. This premise was never sound, but, for years, served as nearly "good enough." When limited static data verification proved insufficient, knowledge-based verification (KBV) was introduced. This prompted a user to answer questions based on more extensive public records or credit history. Even when this method was new, it was highly problematic as legitimate customers frequently failed these questions, and it introduced a high rate of friction and abandonment.

The theft of PII enables a criminal to attack static data verification methods and to impersonate people to obtain their credit and public records, thus gathering a robust set of information to circumvent most data verification tools such as KBV. The theft of this data used to occur primarily through theft of paper records or insider attacks. Over the past 10 years, PII breaches have occurred at a much larger scale, with the most significant methods being hacking, malware and social engineering. [1] The stolen data supports account takeover activities as well as new account fraud. (For definitions of types of fraud such as account takeover, synthetic identity fraud and identity theft, see "Improve Your Enterprise Anti-Fraud Program by Implementing a Financial Crime Taxonomy" and "The Growing Problem of Synthetic Identity and First-Party Fraud Masquerades as Credit Losses.")

Despite the level of PII compromise present in most regions, regulatory requirements such as know your customer (KYC) still require verification of static data, and the concept of identity proofing is frequently tied to these activities. Enterprises with a remote business presence (digital or contact center) have had to continually add new approaches and technologies to detect anomalies that may indicate that individuals are not who they say they are, despite the correct recitation of credentials and/or PII. Many of these tools have been classified as online fraud detection tools, and indeed many of them do have relevance in transactional online fraud detection use cases. However, the need to detect and prevent fraudulent and malicious activity at the time of account creation and subsequent access events demands the use of these tools as part of an overall identity proofing and corroboration framework as well.

The lines between online fraud detection, identity proofing, compliance and user authentication use cases are increasingly blurring with regard to the techniques that can be applied to increase trust assurance and better identify malicious or anomalous activity (see Figure 1). This Market Guide focuses on identity proofing and corroboration, which has a traditional application at new-account opening (i.e., traditional identity proofing), but many of the technologies described have efficacy beyond those events to any interaction requiring an assessment of the trust present in the interaction (i.e., broader identity corroboration).

Figure 1. Convergence of Technologies and Activities Across Use Cases



Source: Gartner (April 2018)

Market Direction

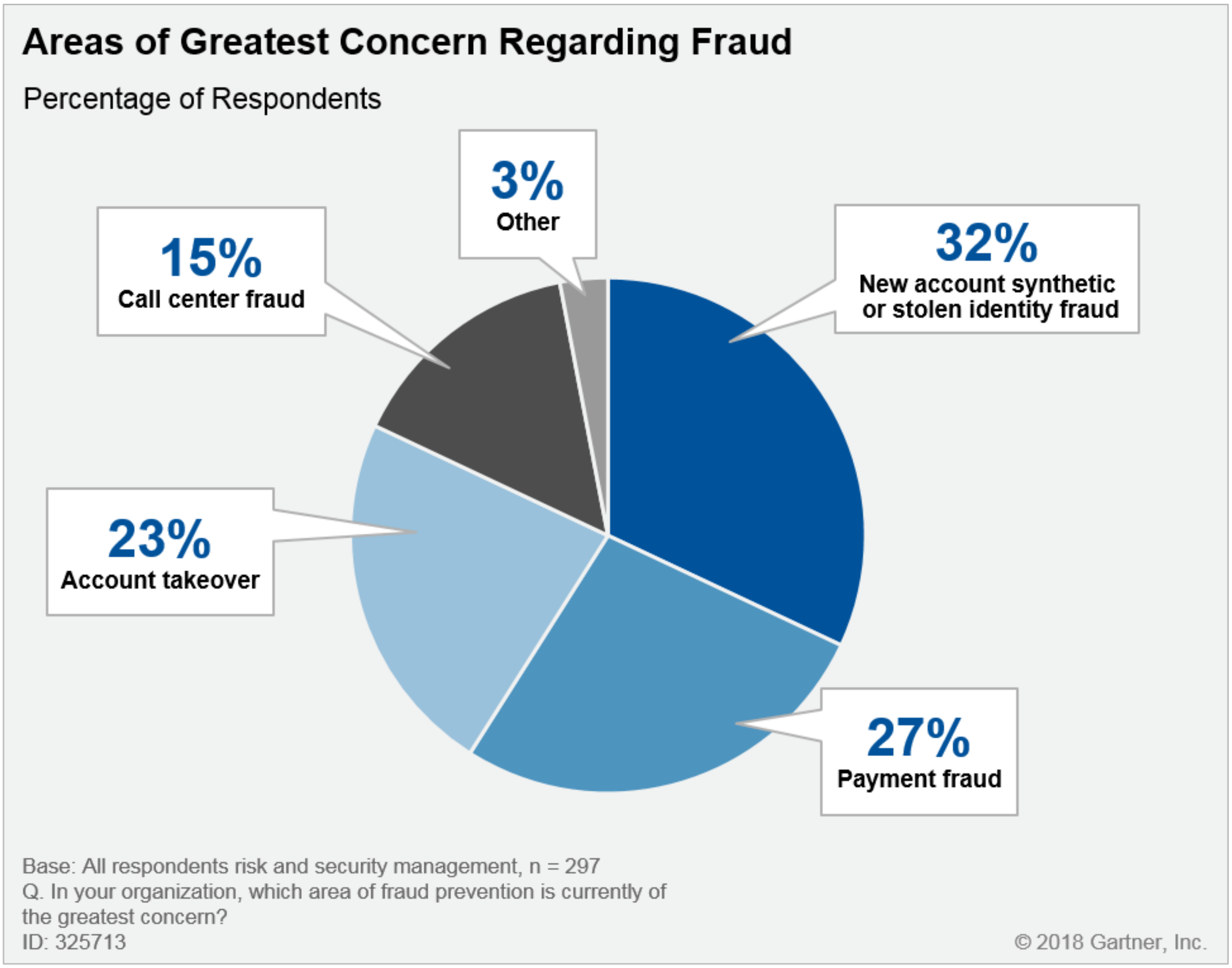
As nearly every component of modern life embraces digital channels, the need to corroborate the identity of customers, users, citizens, partners and employees through remote interactions continues to grow. At the same time, traditional methods of corroborating identity have been nullified due to continued breaches of personal data.

Many enterprises who have justified onerous demands on their customers with the prelude "for the security of your account" are finding that the changing demographics of their target customer base prioritize convenience over security. These new target customers — often, but not always, generationally separated from the previous customer base — will not tolerate these demands and will take their business to competitors who offer a lower-friction experience.

This is not to say that financial technology (fintech) or mobile-first businesses always prioritize customer experience over security. The difference is that they invest in the technologies to make security invisible to their customer in as many cases as possible. This investment results in higher conversion and customer engagement as well as higher rates of detection of sophisticated fraudulent and malicious activities.

In a 2017 Gartner Security and Risk Management survey, 23% of respondents said that account takeover was their greatest area of concern related to fraud prevention, while 32% cited identity theft and synthetic identity [2] (see Figure 2).

Figure 2. Area of Greatest Concern Related to Fraud Prevention



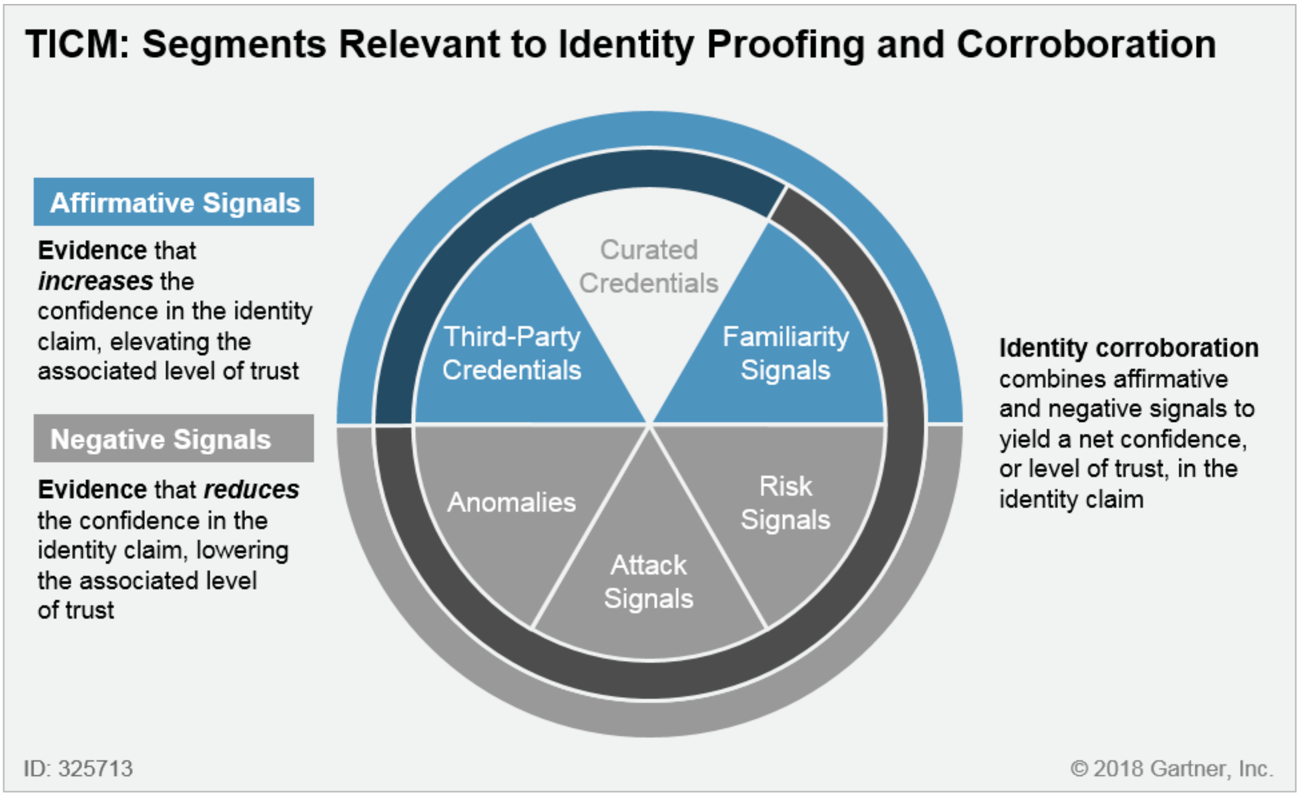
Source: Gartner (April 2018)

These concerns have only been exacerbated by the continued deluge of reported breaches that revealed names, addresses, government identifiers, driver's license numbers, dates of birth, security questions and answers, mother's maiden names, and more. The number of inquiries related to identity proofing has increased by more than 300% in 2017 versus the same period in 2016, as Gartner clients in banking, finance and insurance, healthcare, government, education, retail, telecom, and service providers attempt to reduce their reliance on highly compromised static PII.

Approaching identity proofing as a continuous and contextual process that provides an increased level of assurance that the identity presented exists and is being legitimately used can aid in the areas of high concern expressed by 70% of clients. Gartner has introduced a Trusted Identity Corroboration Model (TICM; see "Take a New Approach to Establishing and Sustaining Trust in Digital Identities"), which provides a way of understanding the variety of credentials and other soft signals that can contribute to identity corroboration across multiple use cases. In essence, it highlights the range of identity-specific inputs to adaptive, risk-based approaches and the contribution they make: affirmative (or positive) signals (increasing trust) and negative signals (decreasing trust or increasing risk).

Identity proofing and substantiation capabilities are represented in the Trusted Identity Corroboration Model (see Figure 3). They provide the means of gathering and analyzing anomalies, attack signals and risk signals as well as affirmative signals.

Figure 3. Trusted Identity Corroboration Model (TICM)


TICM: Segments Relevant to Identity Proofing and Corroboration
Affirmative Signals
Evidence that *increases* the confidence in the identity claim, elevating the associated level of trust
Negative Signals
Evidence that *reduces* the confidence in the identity claim, lowering the associated level of trust
Curated Credentials
Third-Party Credentials
Familiarity Signals
Anomalies
Risk Signals
Attack Signals
Identity corroboration combines affirmative and negative signals to yield a net confidence, or level of trust, in the identity claim
ID: 325713
© 2018 Gartner, Inc.

Source: Gartner (April 2018)

This model can be applied to identity proofing with the following benefits:

- Maximizes the collection of multiple risk indicators to identify fraudulent and malicious activity during account creation, access and maintenance
- Maximizes the weighting of familiarity signals to ensure that low-risk, good customers can have the best possible customer experience, leading to lower abandonment, reduced operational burden for addressing false positives and higher revenue

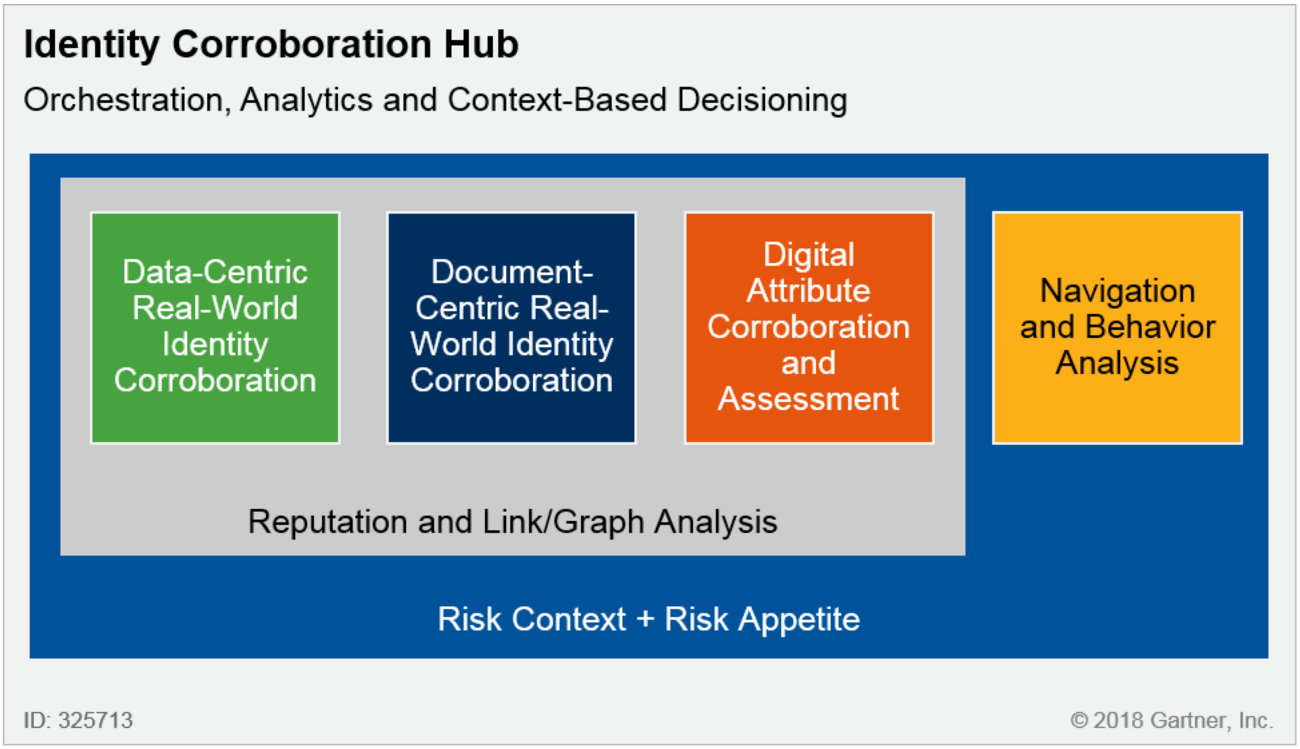
In light of continued, unrelenting breaches of personal data as well as usernames and passwords, enterprises must move to continuous, risk-based assessment of any claimed identity, both at the establishment of a relationship and in every subsequent interaction. The continued reliance on static data, public records or credit bureau data alone to either establish or substantiate trust in an identity is no longer simply unadvisable; it has become negligence. Likewise, a refusal to invest in the gathering and assessment of negative and positive signals puts the burden of security on customers, which is increasingly unacceptable in a world that demands frictionless and secure interactions with businesses and organizations.

Market Analysis

The expanding categories of tools included in this market can be applied individually or in a fully orchestrated manner any time trust in a digital identity needs to be established or corroborated. It is important to note that the number of tools used increases the need for a central orchestration and analytics function. In addition, the risk of overbuying discrete capabilities without the ability to perform the necessary weighting and normalization of the outputs is significant. Integrating multiple tools without a sense of how each score or assessment will be weighted and integrated into a context-based decision process is likely to lead to high false-positive rates and a poor customer experience.

Typically, the full suite of capabilities is required only by enterprises with the most significant financial or informational data stores, such as government intelligence agencies or enterprise financial service. With the increasing automation of fraud attack and identity impersonation tools, however, more criminal groups are targeting midsize enterprises across multiple industries with an eye toward account takeover as well as new account fraud (see Figure 4).

Figure 4. Identity Corroboration Hub


Identity Corroboration Hub
Orchestration, Analytics and Context-Based Decisioning
Data-Centric Real-World Identity Corroboration
Document-Centric Real-World Identity Corroboration
Digital Attribute Corroboration and Assessment
Navigation and Behavior Analysis
Reputation and Link/Graph Analysis
Risk Context + Risk Appetite
ID: 325713
© 2018 Gartner, Inc.

Source: Gartner (April 2018)

Identity Corroboration Hub

The emergence of the identity corroboration hub addresses the challenge of orchestration, and in some cases, also solves the need for a centralized analytics capability. An identity hub must have:

- Integration to multiple third-party data tools, which should include solutions or data sources related to at least two of the following:
  - Real-world identity corroboration
  - Digital attribute risk assessment
  - Navigation and other behavior analysis
  - Digital or real-world reputation and link/graph analysis

An identity corroboration hub must also have:

- The ability to ingest and normalize incoming data (including custom data), as well as the results of the third-party data call-outs
- A rule or policy engine that enables security and risk management leaders to configure business rules for different types of events (i.e., new-account opening, material change to account, etc.), and that controls when these third-party tools are called, and what action is taken based on the results

Increasingly, it is important that an identity hub expand beyond orchestration and rules into a deeper identity analytics capability. This should provide at least one of the following, but ideally, all three:

- Normalization of the results of all third-party API calls and inclusion of that data into a core identity analytics database
- The ability to score a digital interaction for the likelihood of the following:
  - That the claimed identity is not a real-world identity (i.e., that it is a synthetic identity)
  - That the claimed identity is being used fraudulently (identity theft or account takeover)
- The ability to build an identity graph using linkages and clustering algorithms, among others, to evaluate endpoint, digital identity, physical identity, navigation and other behaviors

Data-Centric, Real-World Identity Corroboration

Real-world identity corroboration has been the mainstay of identity proofing use cases. Static data corroboration and KBV typically rely on public records for real-world activity and on credit bureau data to confirm or deny that the information provided by an individual matches (or not) the information on record. They have been relatively ineffective at detecting both synthetic identity and identity theft. They also have been poorly equipped to corroborate the identity of individuals with an absence of credit history due to the use of alternative financial services, age or recent immigration to the country whose records are being interrogated.

It may be tempting to abandon this method of identity substantiation entirely, and Gartner strongly recommends that all SRM leaders move away from this method as their sole method of corroborating the identity of individuals. However, these techniques meet many of the existing requirements for regulatory schemes such as know your customer.

Dynamic, context-based analytics assessing digital and real-world risk signals are much more difficult to convey to a regulator than an auditable result indicating that the name, address and government identification number provided by an individual matched a credit file. For this reason, the need for this type of static data validation persists. However, the true value of this information increasingly lies in the identity graph and cluster analysis that can be performed using this real-world data combined with digital identity data. Regulators are lagging significantly behind the technology and they must broaden their ability to understand more nuanced identity proofing results. The National Institute of Standards and Technology (NIST) has published guidance on digital identity and identity proofing assurance levels, [3] which should nudge regulators in this direction. In the meantime, for many industries, the boxes must be checked.

Document-Centric, Real-World Identity Corroboration

Gartner has seen a growing interest in remote identity document verification solutions in the past 12 months whereby a passport, driver's license or other form of identification is captured via scanner, webcam or mobile phone camera. It is then assessed for signs of tampering or counterfeit, and then the photo or video of the document is compared to a "selfie" (still photo or short video) taken by the individual submitting the document. There are a few parts of this type of solution that are important to understand:

1. Image quality matters:
   - A document captured through a built-for-purpose document scanner has significantly higher resolution than one captured by someone holding up a document in questionable lighting to a low-resolution web camera. A poor-quality image makes it harder to accurately assess the document for anomalies.

2. Document libraries feed algorithms:
   - In order to programmatically assess an image, there must be sufficient training libraries of both good and bad documents of the same document type in order for the algorithms to detect anomalies with any level of accuracy. It is critical to know the most likely documents used by your customers and verify the coverage level for those documents by a potential vendor.

     The approach of most providers in this space is to assess submitted images using machine learning algorithms and rely on manual review or higher-friction approaches if the legitimacy of document and "selfie" does not meet requirement thresholds. These manual processes can be provided by employees of a vendor, internal employees, or simply result in a fallback to higher-friction approaches, such as asking the person to present identification in person.

3. Liveness testing holds one of the keys:
   - The ability to perform liveness testing on the photo or video selfie used to compare to the submitted document photograph is essential. This is to prevent an attacker using a stolen, legitimate document along with a photo or video clip of the other person as the selfie.

4. Customer experience is paramount:
   - While some providers tout the document verification process as frictionless, it is far from it. While it is true that the friction involved in the process is lower than it would be to go into a branch office, it is not frictionless or even low friction. "Armchair applicants" must rise from their position to locate their government document and must prepare for a photo. Additionally, the device used by the customer will have considerable impact on the results of the image or video capture and the customer experience. For example:
     - Using a scanner for the image capture can be inconvenient, as it does not support the mobile-first experience that is desired by many enterprises and customers.
     - Using a webcam can be frustrating, as there is considerable variation in camera quality and lighting combined with an inability to provide real-time feedback to the user. In some cases, a user may capture the required images and then, after submitting them, receive a request to perform the actions again but with better placement, focus or lighting.
     - Using a camera from mobile web has the same challenges as a webcam with regard to real-time feedback, though the average camera quality tends to be more consistent in most markets.

- Capturing the document and selfie from an embedded SDK in a mobile app is optimal, as the user can be directed in real time to find a better light source, position the document or face in the optimal location for the capture.

Unfortunately, the primary use case for the application of these solutions is at new-account opening, and, with some industry variation, the majority of consumers do not download a mobile app prior to applying for a new service or product. For this reason, some enterprises are using this category of solution as a method of increasing trust assurance after the initial identity assessment and account approval has occurred and a mobile app has been downloaded. For example, preliminary approval of a new bank account or credit card may be provided without document verification if all other signals are positive. Document verification is required only if subsequent activity decreases the level of trust assurance with the customer and additional verification is required. By this point, the risk of abandonment by the customer is lower than at the time of application, and the chances are higher that a mobile app has been downloaded, which can reduce friction in the remote document verification experience.

Managing internal expectations about accuracy, decision time and user experience is critical for the successful use of these solutions. Gartner strongly recommends performing analysis of the devices used most commonly for interactions requiring identity corroboration. In addition, analyze the demographics of customers expected to use these services, specifically, the most likely type of identification documents (state or regionally issued driver's licenses, passports, etc.) held by these customers.

Digital Attribute Risk Corroboration and Assessment

A digital attribute in this case can be an email address, the existence of a social profile, or attributes of any device used by a customer to access services or products. This includes endpoints such as phones, personal computers, tablets, mobile phones, kiosks, etc. While "device fingerprinting" has been widely adopted for assessment of computers, tablets and smartphones, in its most simplistic form, it is vulnerable to remote access Trojans (RATs), and man in the middle (MITM) and man in the browser (MITB) attacks. There is a dramatic increase of personal computing devices used by an individual, and an overreliance on traditional device fingerprinting solutions to determine whether a user is a criminal or good customer. This combination can result in higher-than-desirable customer friction and a false sense of confidence due to high-risk attackers masquerading as average users.

Digital attribute assessment can include the following:

- Collection of multiple data points from the device, such as browser type and language, TCP/IP configuration, OS information, wireless settings, hardware clock and hundreds of other attributes
- The ability to analyze those data points to create a "fingerprint" of the device
- The ability to analyze those data points to determine anomalies or known risk signals
- The ability to collect "truth data" from client organizations (i.e., whether the endpoint is confirmed to have been associated with malicious or fraudulent activity) to provide near-real-time input into machine learning models
- The ability to detect automated attack patterns in the form of bot activity on a web or mobile app interface, or automated IVR attacks in the contact center

Solutions in this space are frequently channel-specific (web and mobile, contact center, or kiosk), and, historically, providers with a focus on detecting fraudulent individual activity have not supported use cases such as advanced bot attack and malware detection. In the past year, Gartner has seen the leading providers in each of these channels expanding their product capabilities to support better detection of negative and positive signals from an end user's device.

In order to keep pace with the market and threat landscape, solutions that cover mobile and web channels are increasingly providing traditional device fingerprinting as well as more advanced device scoring and anomaly detection, bot detection, and malware detection.

In the contact center channel more than in any other channel, there is still an overreliance on the most basic static data for authentication and identity proofing. Solutions to detect a high-risk interaction in this channel have historically been fragmented. Phoneprinting, biometric voice recognition and spoofing detection were previously provided by distinct vendors. The past year has seen significant expansion of capabilities by leading vendors through partnerships and native product development to support both authentication and fraud detection solutions. In the contact center channel, identity proofing, fraud detection and authentication have had more overlap than in any other channel, with KBV commonly considered "authentication" as well as "identity proofing." The ability to collect and analyze risk and familiarity signals in the contact center is critical to identity proofing use cases.

Email address and mobile phone number as digital identity identifiers are increasingly relevant as well. While one may change devices, replace credit card numbers, move houses or employers every few years, personal email addresses and, increasingly, mobile phone numbers have emerged as more persistent identity attributes. Risk assessment of an email address can include:

- How long an email address has been in use (newly created emails are higher risk than older ones)
- What the risk level of the domain is
- Whether there are any real-world identity attributes associated with the email or between the email and the device, historically within digital identity networks

These assessments can provide a level of positive identity assurance through familiarity signals or, in the case of high-risk, negative or absent history, they can provide important negative signals. Likewise, knowing the mobile phone carrier, status and even subscriber's personal data can provide a connection between real-world and digital identities.

Organized criminals continually evolve their methods of masking their identities. The solutions that were highly effective five years ago are insufficient today against the more sophisticated attacks without supplementation from other technologies and solutions. As with most of the capabilities for identity proofing and corroboration, the use of advanced analytics to rapidly identify emerging patterns of behavior by malicious actors is a key differentiator. Digital attribute assessment continues to be one of the first defenses in a digital fraud and identity proofing strategy, but, as with the other categories, it is insufficient to detect all identity fraud on its own.

Navigation and Behavior Analysis

Behavior analysis can allow the observation and analysis of users' activities within a digital property or IVR. This can include analysis of:

- The way users type
- The placement and timing of their mouse movements and clicks
- The way they scroll
- Their swipe pattern on a mobile device
- The way in which they interact with an IVR
- The time they spend viewing a page before taking the next action

Some of these data attributes fall into the category of behavioral biometrics. That term refers to the use of collected behavioral data to generate a behavior profile for an individual user. Initial focus for passive behavioral biometrics was authentication and account takeover prevention use cases, with the idea that behaviors could act as a passive second factor of authentication for a specific user. High false-positive rates relative to expectations and lengthy profiling requirements have reduced the enthusiasm for these technologies as a credential replacement, but they are still effective in many deployments, particularly for continuous user authentication.

More recently, the collection of these interaction behavior data points has been combined with more general navigation behavior and applied to new-account opening or "first interaction" use cases. For these use cases, the algorithms are focused on analyzing peer group behavior signals, rather than corroboration of a specific individual. This is accomplished by providing a baseline of "normal" behaviors for a general population or a peer group against which any interaction can be compared. Field-level analysis can be used to provide a risk signal about whether the person who filled out the form or interacted with an IVR is in fact a human, and what type of human they seem to be (high risk or low risk). This analysis includes which types of data should be copied and pasted versus typed in, the speed at which low-risk users have historically filled out a given form, their time on the page, and more nuanced navigation. Some vendors are collaborating with market-leading financial services organizations to build models for behaviors related to first-party fraud, synthetic identity fraud and third-party fraud to supplement other identity proofing and corroboration use cases (see "The Growing Problem of Synthetic Identity and First-Party Fraud Masquerades as Credit Losses").

This is not a technology that could ever be used as a stand-alone identity proofing solution as it does not corroborate an identity in any traditional way. What it can potentially do is provide the risk indicator that tips the scale toward the identity not being corroborated in an otherwise "clean" identity proofing interaction or one where there are no clear risk or familiarity signals using other tools.

One of the challenges in this area has been in regions highly concerned with privacy, as consumer sentiment, political viewpoint and even local legislation can restrict the deployment of technologies seen as invasive. While behavior analysis is far from personally identifiable information by most reasonable assessments, many people are skeptical of this technology because it seems "creepy" (see "Digital Businesses Need to Understand the Creepy Line From Peoples' Perspective").

Reputation and Link/Graph Analysis

Reputation and link analyses focus on analytics-based relationships and risk of digital attributes, real-world identity attributes, and most successfully, both. These techniques have shown some success in detection of synthetic identity fraud, first-party fraud and sophisticated identity theft, which often go undetected by other tools.

This space is growing quickly due to the rapid adoption of advanced machine learning techniques supporting cluster and link analysis and of anomaly detection and advanced computing capabilities enabling real-time analysis and scoring.

Vendors in this category have:

- A network- or consortium-based dataset including digital and/or real-world identity attributes such as mobile phone number, email address, mailing address, IP address, device IDs or "device fingerprints," augmented by third-party data providers and participating organizations.
- The ability to use machine learning to identify correlations between data attributes, evaluate the strength of those correlations, the reputation of those data attributes and correlations, and to deliver a score or risk indicators for a specific attribute or a claimed identity.

A vendor may use multiple sources of static, real-world identity data, social media account data and mobile phone number data. Using cluster and correlation analytics, it may develop a combined digital and real-world identity cluster. This cluster could include multiple email addresses, phone numbers and mailing addresses that have been used by an individual, as well as the connections that these data attributes may have to other identities. Enterprises using these services may send an API call with name, address, email address, device information, etc. to the vendor. This data is added to the core dataset and a response is returned regarding the analysis of that data from a risk or familiarity standpoint.

For example, a new prospective customer may have little history at a mailing address based on real-world identity data, but the real-world identity information provided does match public or bureau records. Correlations can be viewed as familiarity signals that help corroborate the identity of the person, despite their short tenure at a mailing address. For example, if the email address provided meets the following, then there is a high trust correlation that this identity presenting the mobile phone and email address is the true person, despite little history at an address:

- It has been part of an identity network for years
- It is associated with the same mobile phone number that was provided
- One or both of those matches the name of the claimed identity
- There is an absence of negative information about any of the attributes

If, however, there is little history at the mailing address, and the email address and mobile phone number are not connected to the other identity attributes, it could be an indication that the claimed identity is actually stolen or synthetic. These negative signals based on the analysis and reputation of the real-world and digital identity attributes can serve to tip the scales of trust in one way or another.

These capabilities are an important component of the most sophisticated identity hubs; and the ability to ingest, normalize and analyze data from multiple third-party sources — rather than simply creating rule-based actions on the third-party data — is both difficult and valuable.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

There are myriad data types and signals that must be corroborated and analyzed in order to achieve a sufficient level of trust in a modern identity proofing and corroboration use case. Vendors listed in Table 1 have one or more of these capabilities and are representative of the evolution of the requirements of these use cases. This list is not meant to be exhaustive, and the presence or absence of a vendor is not indicative of the performance or abilities of a particular vendor's solution(s).

Additionally, many vendors may be primarily known for their support of more traditional online fraud detection or authentication use cases. Inclusion in this Market Guide indicates active use by vendors' customers of their solution for identity proofing and corroboration use cases.

Table 1: Representative Vendors in Identity Proofing and Corroboration

Representative Vendors ↓	Identity Corroboration Hub ↓	Data-Centric, Real-World Identity Corroboration ↓	Document-Centric, Real-World Identity Corroboration ↓	Digital Attribute Corroboration and Assessment ↓	Navigation and Behavior Analysis ↓	Re an Id Re an Li Ar
Acuant		*	X			
BioCatch				X	X	X
buguroo				X	X	
Emailage				X		X
Experian	X	X	*	X, *	*	X
EZMCOM		*	X	X	X	
Fraud.net				X		X
IBM Trusteer				X	X	X

Representative Vendors ↓	Identity Corroboration Hub ↓	Data-Centric, Real-World Identity Corroboration ↓	Document-Centric, Real-World Identity Corroboration ↓	Digital Attribute Corroboration and Assessment ↓	Navigation and Behavior Analysis ↓	Re an Id Re an Li Ar
ID Analytics		X	X	X		X
IdentityMind	X	X, *	*	X, *	*	X,
IDology	X	X	X	X		X
iovation				X		X
Jumio		*	X			
Kount	X	X, *		X, *	*	X
LexisNexis Risk Solutions*	X	X	X	X	*	X
Mitek			X			
Nuance				X	X	
NuData Security, A Mastercard Company				X	X	X
Pindrop				X	X	
SecuredTouch					X	
ThreatMetrix, A LexisNexis Risk Solutions Company	X	*		X		X
TransUnion	X	X, *		X, *	X	X
TRUSTID				X		
Whitepages Pro		X		X		X

X = Built or acquired native capability* = Provided through integrated partnerX, * = Capabilities for this category are available as a native platform capability and can be supplemented throug integrated partner

Source: Gartner (April 2018)

Market Recommendations

Security and risk management leaders must ensure that they:

- Perform an inventory of your current identity proofing methods, and assess the likelihood that the existing methods can be subverted by criminals. Be realistic about the limitations of data-centric real-world identity corroboration tools.
- Include the cost of poor customer experience when evaluating the business case for new investments for identity proofing use cases. A process that is both fragile and high friction should be a high priority for replacement or augmentation.
- Prioritize the detection of identity-related attacks at all facets of customer interaction, including both online and offline channels such as web portals, mobile apps, call center and other telephony interactions, emails, faxes, and written letters.
- Ensure the identity proofing and substantiation strategy ties into a broader risk management framework encompassing new application assessment, user authentication, fraud detection and prevention, and account management. Leverage tools in place or on the roadmap for use cases in these areas.

- Evaluate the use of an identity hub to enable the orchestration and testing of multiple solutions as the need arises. While many organizations do not require the full suite of capabilities today, sophisticated attacks are moving down market and a plan for rapid incorporation of new technologies as needed is recommended.

Evidence

[1] "2016 Data Breach Investigations Report," (http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf) Verizon; Figure 4 "Number of breaches per threat action category over time."

[2] The annual Gartner 2017 Security and Risk survey was conducted between 24 February 2017 and 22 March 2017. The goal was to better understand how risk management planning, operations, budgeting and buying are performed, especially in the following areas: risk and security management; security technologies, and identity and access management (IAM); business continuity management; security compliance and audit management; and privacy.

The research was conducted online among 712 respondents in five countries: the U.S. (n = 141); Brazil (n = 143); Germany (n = 140); the U.K. (n = 144); and India (n = 144). Qualifying organizations have at least 100 employees and $50 million (or U.S. dollar equivalent) in total annual revenue for fiscal-year 2016. All industry segments qualified with the exception of IT services and software and IT hardware manufacturing. Further, each of the five technology-focused sections of the questionnaire required the respondents to have at least some involvement or familiarity with one of the technology domains we explored.

Interviews were conducted online and in a native language and averaged 19 minutes. The sample universe was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

Disclaimer: "Total" results do not represent "global" findings and are a simple average of results for the targeted countries, industries and company size segments in this survey.

[3] See the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (https://doi.org/10.6028/NIST.SP.800-63-3) document suite, specifically, the sections on Enrollment and Identity Proofing (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf) .

Note 1
Representative Vendor Selection

Representative vendors were selected on the basis of one or both of the following: frequent inquiry by Gartner clients about that vendor for identity proofing use cases and/or vendors who are offering capabilities supporting identity proofing and corroboration in a way that is unique, innovative and/or that demonstrate a forward-looking product strategy.

Note 2
Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.