Market Guide for Identity Proofing and Affirmation

Published 11 September 2020 - ID G00719390 - 33 min read

By Akif Khan, Jonathan Care

Obtaining confidence in a customer’s identity is the foundation of remote interactions for most organizations. Security and risk management leaders must balance assurance needs with friction in the customer journey, while orchestrating multiple tools and becoming aware of accuracy and bias.

Overview

Key Findings

- The identity-proofing market encompasses a broad range of capabilities in two tool categories. Identity-proofing tools provide confidence in the genuine presence of the identity owner, and identity affirmation tools have a greater variety of capabilities. The affirmation tools add confidence, but cannot, by themselves, provide identity proofing, because they do not prove that the individual claiming the identity is authentic.

- In most organizations, digital transformation has been accelerated by the COVID-19 pandemic, leading to a renewed focus on the digital onboarding process as a critical requirement for doing business.

- Identity-proofing processes are likely to involve multiple capabilities, resulting in a burden to organizations with respect to vendor integration and workflow management.

- An increased awareness of bias in machine-learning-based systems reveals that the facial recognition algorithms used in an important class of identity-proofing products have demonstrated demographic bias in their performance.

Recommendations

Security and risk management leaders responsible for identity and access management and fraud detection should:

- Select capabilities based on use-case needs by mapping out the customer journey and evaluating where identity proofing and affirmation tools can add value, particularly in conjunction with authentication and fraud detection tools.

- Build a business case for investing in improving the identity-proofing aspects of remote onboarding processes by leveraging the increased focus on digital transformation triggered by the COVID-19 pandemic.

- Create scalable and flexible identity proofing and affirmation processes by implementing a solution with strong orchestration capabilities to abstract away the complexity of managing multiple vendors and integrations.

- Demand evidence of impartiality with respect to the identity proofing of different demographic groups by asking vendors to provide data from independent testing of their face recognition algorithms.

Strategic Planning Assumptions

By 2022, 80% of organizations will be using document-centric identity proofing as part of their onboarding workflows, which is an increase from approximately 30% today.

By 2022, more than 95% of RFPs for document-centric identity proofing will contain clear requirements regarding minimizing demographic bias, an increase from fewer than 15% today.

By 2023, 75% of organizations will be using a single vendor with strong identity orchestration capabilities and connections to many other third parties for identity proofing and affirmation, which is an increase from fewer than 15% today.

Market Definition

Seeking high confidence in the identity of customers continues to remain an imperative across a number of use cases in many industries.

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

- *The real-world identity exists.*

- *The individual claiming the identity is, in fact, the true owner of that identity and is genuinely present during the process.*

Identity proofing traditionally focuses on use cases in which an organization is interacting with someone for the first time. Examples include account opening, registration, application or enrollment.

Identity affirmation, on the other hand, is the combination of activities that provide *supporting evidence* for an identity claim to establish trust in an interaction, such that confidence is increased during the identity-proofing process that fraud isn’t taking place.

Thus, it follows that identity affirmation alone is not sufficient to provide a tolerable level of confidence in a customer’s identity. It is deployed as part of the identity-proofing process in the form of supporting capabilities.

In the context of this research, identity proofing is discussed for use cases in remote interactions, such as web, mobile app and contact center, which includes interactive voice response (IVR) systems, as well as live voice calls.

This Market Guide focuses on a human-centric view of identity proofing. It does not cover nonhuman entities, such as bots or Internet of Things (IoT) devices, which could be considered holding identities for which appropriate identity-proofing processes may be required, depending on the use case.

Market Description

Because nearly every component of modern life embraces digital channels, the need to obtain confidence in the identities of customers, citizens, partners and employees through remote interactions continues to grow.

A broad range of capabilities supports this effort. Determining which technology to implement depends on the channel of interaction and the degree of confidence required in the identity. In addition, user experience (UX) considerations have become a critical factor. More often than not, a combination of techniques is deployed to satisfy requirements.

Capabilities within the identity-proofing market can be broadly segmented into six categories.

Document-Centric, Real-World Identity Proofing

This category of identity proofing enables organizations to obtain an acceptable level of confidence in a customer’s identity. It is accomplished via remote digital channels, whereby an image or video snippet of a passport, driver’s license or other identity document is captured via webcam or, more typically, mobile phone camera. It is assessed for signs of tampering or counterfeiting, then the photo on the document is compared with a “selfie” (still photo or short video) taken by the individual submitting the document.

Because this involves testing for genuine presence (also commonly referred to as “liveness detection,” more formally as presentation attack detection), document-centric approaches meet the Gartner definition for identity proofing when deployed correctly. Specifically, the submission of the image of the identity document and the selfie should be a tightly integrated process in the identity-proofing software. The identity assurance achieved with this capability used in isolation is relatively strong, relying on both “something *only* you have” and “something *only* you are.”

Data-Centric, Real-World Identity Affirmation

This category of identity affirmation has been the mainstream approach to proving an identity for many years. It involves checking the identity data (e.g., name, address, phone, date of birth) entered by a user against sources, such as electoral records, credit bureau data and census information. Vendors in this space add value through their access to multiple data sources, and their ability to correlate across them. This correlation increases the confidence in an identity assertion. Data-centric approaches alone *do not* meet the Gartner definition of identity proofing, because there is no test that the individual claiming the identity is, in fact, the authentic possessor of that identity. The identity assurance achieved with this capability used in isolation is relatively low, relying only on “something *you-but-not-only-you* know.”

Device-Focused Identity Affirmation

Information about the software (OS, browser, plug-ins, etc.) and hardware specific to a given device (desktop, laptop, tablet, mobile phone, etc.) can be combined to create a unique device identifier (often called a device fingerprint). This information is typically gathered via JavaScript in a browser environment, or a software development kit (SDK) in a mobile app environment. This “attribute-based” approach to creating a device identifier has supplemented the original approach in the field of relying on cookies to “tag” a device, then identifying it in subsequent interactions. There is no standardized way to create a device identifier, with each vendor having its own proprietary algorithms for doing so.

This is an affirmation capability, which enables the assessment of risk in an identity-proofing use case (e.g., has this same device been recorded presenting different identities?), as well as corroborating identity in subsequent interactions as a passive means of authentication (e.g., is this the same device that has been previously associated with this user?). In addition to the device identifier itself, assessment of software-related attributes (such as time-zone settings and browser language) can potentially be leveraged for fraud detection as risk or trust signals during the identity-proofing process.

Digital-Attribute-Focused Identity Affirmation

Digital attributes, such as email addresses, IP addresses or social media profiles, can be leveraged for identity affirmation purposes. The correlation of these digital attributes with real-world identities can yield trust or risk signals during the identity-proofing process. In particular, the email address has proved to be a particularly persistent identity attribute. One may change devices, replace credit card numbers, move houses or switch employers every few years, but personal email addresses often remain unchanged. As a result, being presented with an email address that has never been seen “in the wild” before is typically interpreted as a risk signal.

IP addresses cannot reliably be tied to an individual. However, obtaining geolocation data about IP addresses is a useful way to leverage them for identity affirmation purposes. Such geolocation data is typically compared with the home address provided by a customer, or to device attributes, such as browser language or time zone. Leveraging social media profiles for identity affirmation is still largely the domain of manual investigation.

Behavior-Analytics-Focused Identity Affirmation

Passive analysis of behaviors, such as typing cadence, mouse movements and swipe patterns, can be used to build a profile of a customer during a first-time interaction, such as application or registration. Such a profile can be compared against statistical norms for good and bad behavior across the broader customer population for that organization. As such, behavior analytics is a useful identity affirmation technique that augments the core identity-proofing process by detecting signs of fraud. For example, most applicants for a financial services product, such as a credit card or a loan, would be unfamiliar and careful with the online form. An applicant acting with an unusually high degree of familiarity with an application form can suggest a fraudster who may have made multiple applications already, using different identities.

Information about these behaviors is typically gathered via JavaScript in a browser environment, or an SDK in a mobile app environment. As with the creation of device identifiers, there is no standardized approach to building such behavior analytics profiles. Each vendor in this space has its own proprietary algorithms for doing so. An additional capability offered by vendors in this field is the ability to determine whether an interaction is being carried out by a bot, rather than a human. Malicious bots can be used by bad actors to automate the account application process at scale using stolen or synthetic identities. Spotting such behavior is crucial to the integrity of the identity-proofing process.

Behavior analytics is distinctly different from behavioral biometric modes based on interactions with the digital user interface (UI). The latter is an authentication technique focused on the recognition of a returning user who has already completed the identity-proofing process, and has been issued credentials.

Phone-Number-Focused Identity Affirmation

Phone numbers are useful identity attributes that are leveraged in real-world identity affirmation, as well as for correlation and link analysis with many digital identity attributes, such as email addresses and device identifiers. Identification of the phone number being used to place a call into a contact center is possible via automatic number identification (ANI) or caller ID services offered by the telecommunication networks.

A phone call consists of a signaling stream and an audio stream. A range of vendors focus on the signaling stream to assess the telemetry of the call to detect signs of a phone number being spoofed. Some vendors can link the phone number to data from the carriers and telecom infrastructure providers to reveal the identity data of the registered owner of the phone number.

Furthermore, risk signals can be obtained from carrier data, such as the age of a SIM card, which can be used to assess the risk of a SIM swap as a possible precursor to a fraudulent identity presentation.

The audio stream can be used to authenticate a customer's voice. However, this is not applicable in first-time interaction use cases, such as application or account creation where identity proofing is taking place.

Market Direction

The identity-proofing market is being shaped by a combination of three forces:

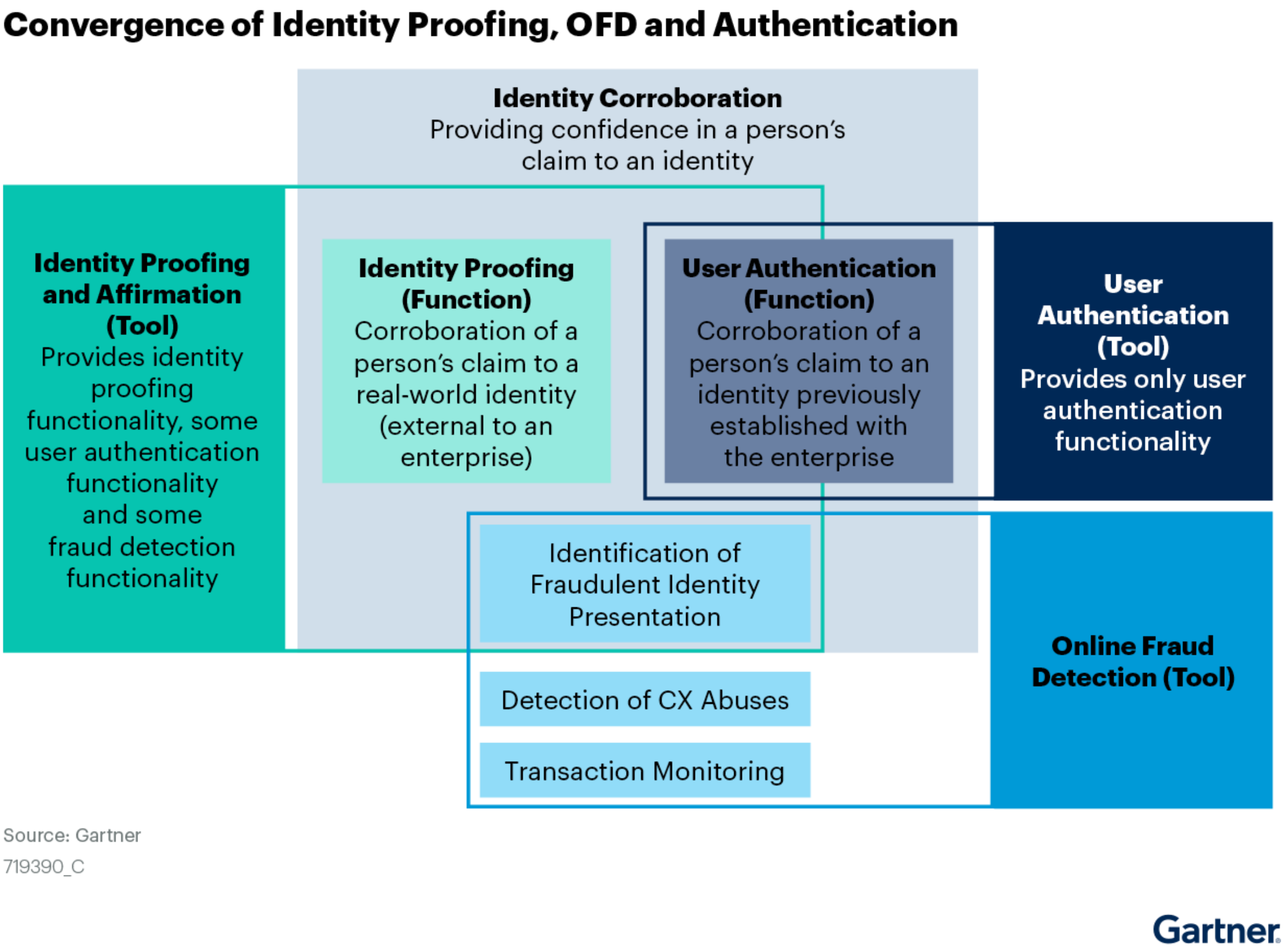
- Convergence with fraud detection and user authentication
- Data breaches of personally identifiable information (PII) rendering checking of static identity data obsolete
- Digital transformation further accelerating due to COVID-19

In addition, although it is not a dominant driver in today's market, the growing use of bring-your-own-identity schemes continues to be an emerging trend.

Convergence With Fraud Detection and Authentication

The lines between the identity-proofing, user authentication and online fraud detection (OFD) use cases are increasingly blurring with regard to the techniques that can be applied to increase trust in an identity claim, and to identify malicious or anomalous activity. An increasing number of vendors offer capabilities that fall into more than one of these three categories (see Figure 1).

Figure 1: Convergence of Identity Proofing, OFD and Authentication


Convergence of Identity Proofing, OFD and Authentication
Identity Corroboration
Providing confidence in a person's claim to an identity
Identity Proofing and Affirmation (Tool)
Provides identity proofing functionality, some user authentication functionality and some fraud detection functionality
Identity Proofing (Function)
Corroboration of a person's claim to a real-world identity (external to an enterprise)
User Authentication (Function)
Corroboration of a person's claim to an identity previously established with the enterprise
User Authentication (Tool)
Provides only user authentication functionality
Identification of Fraudulent Identity Presentation
Detection of CX Abuses
Transaction Monitoring
Online Fraud Detection (Tool)
Gartner

Source: Gartner

719390_C

The link analysis aspects of many OFD tools deliver value when assessing the integrity of combinations of real-world and digital identity attributes presented during the identity-proofing process. For example, an email address or device identifier that can be linked to many different street addresses or phone numbers would raise suspicion. Such links would not be apparent if data-centric, real-world, identity affirmation or document-centric, real-world, identity-proofing processes alone were used. Detecting abuses in the UI, such as automated bots engaging in the identity proofing process as part of an account application, for example, is an area in which OFD tools can add value.

On the authentication front, identity affirmation capabilities, such as those focused on device and digital attributes, can offer additional risk and recognition signals to support the authentication process. An obvious example is the use of the device identifier established during the identity-proofing process during onboarding as a means of passive authentication for subsequent interactions. These signals are increasingly being used as contributing decision factors for additional authentication challenges in use cases for "known" customers. The recognition signals can reduce false positives for fraud, improving customer UX.

The union of identity proofing, user authentication and the overlap with aspects of OFD is identity corroboration, which is relevant in use cases for new and known customers in determining the level of confidence in an identity. This convergence is making the categorization of vendors in markets increasingly challenging. As this trend continues, and functional overlaps increase, the categorization of distinct markets themselves will become more challenging.

Data Breaches Are Rendering the Checking of Static Data Obsolete

The rampant theft of PII via large-scale data breaches continues unabated. [1,2] Such theft enables criminals 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-centric verification tools. The same can be achieved on a smaller, targeted scale through social engineering and malware, or even by looking through a victim’s rubbish or recycling bins.

Nonetheless, data-centric checking of real-world attributes remains the mainstream approach to identity proofing for many organizations. (As stated earlier, Gartner now defines this as an identity affirmation capability, rather than an identity-proofing technique.) Although the deficiencies of this approach are clear to most, its use persists for several reasons. First, depending on geography and jurisdiction, there may still be compliance requirements in regulated industries to check static data sources. Second, in the face of concerns about friction in the customer journey caused by the document-centric, identity-proofing process, many organizations consider checking of static data to be “good enough.” Finally, this good-enough estimation plays into the fact that checking of static data is typically much less expensive than document-centric identity proofing.

In fairness, many vendors that previously focused on data-centric checks have developed their offerings in recent years to address the diminishing returns of relying on static data alone. For example, LexisNexis Risk Solutions augmented its real-world, data-centric product portfolio by acquiring ThreatMetrix in 2018, adding device-focused affirmation. [3] This was further enhanced in 2020 by the acquisition of Emailage, adding digital attribute-focused affirmation. [4] TransUnion took a similar path with the acquisition of iovation in 2018. [5] All of this activity reflects the recognition that the data-centric checking of real-world attributes alone is insufficient to support an identity claim that is within the risk tolerance of many organizations.

This sentiment is reflected in client inquiry calls about identity proofing, as is evidence of the gradual, but ongoing move away from relying on data-centric methods alone. Results from a Gartner poll of 105 respondents via Research Circle, a Gartner-owned online community, 17 February to 28 February 2020, showed that 61% used data-centric methods for identity-proofing needs, and 33% used document-centric methods. Of those using data-centric methods, 10% planned to move to document-centric methods in the following 12 months. This poll was taken before the COVID-19 pandemic caused national lockdowns and increased the focus on digital channels.

Digital Transformation Is Accelerating Further Due to COVID-19

The continuing digital transformation of many industries has served for some time as a driver for organizations to improve online identity-proofing processes. In a regulated industry (e.g., banking), the need to show photo ID as part of the account opening process traditionally meant a visit to one's local bank branch. Many banks have implemented online, document-centric identity proofing to move this process into the digital age and remove the need for a face-to-face interaction.

This was previously seen as a competitive advantage in terms of the customer experience (CX), a way to attract millennials, or any other number of business rationales. The COVID-19 pandemic changed the narrative in this respect — turning online identity proofing into a core requirement for businesses to continue operating, given the enforced absence of face-to-face identity proofing. There is now an acute understanding that circumstances may arise in which the digital channel is not one of many channels, but is, instead, forced to be the *only* channel.

Vendors have responded to the needs and the opportunities of the pandemic. For example, vendors Jumio and Onfido offered free, document-centric identity proofing to qualifying organizations involved in the pandemic relief effort. [6,7] Onfido reported that organizations, such as home care jobs platform Florence, have taken advantage of this offer to bolster their identity-proofing processes.

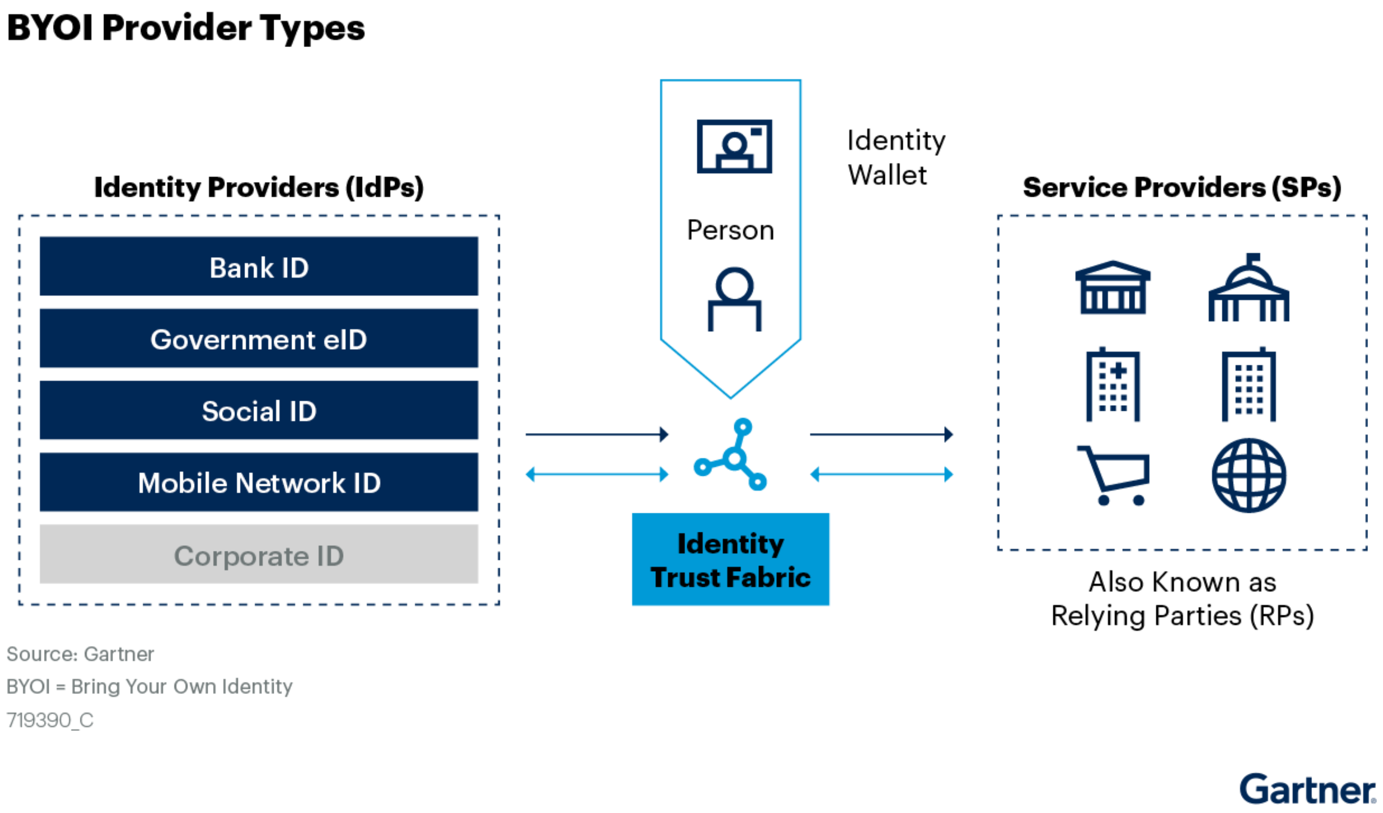
Other than those directly involved in relief efforts, we have seen an increase in inquiries from clients across industries since the onset of the pandemic. Many want to discuss ways to optimize customer onboarding in the digital environment through improved identity-proofing processes. This has resulted in an acceleration in the adoption of new processes to support digital onboarding. For example, Jumio confirmed that financial institutions, such as New York University Federal Credit Union (NYU FCU) and Simba Bank, have adopted their services as a direct result of remote, identity-proofing requirements driven by the pandemic.

Bring Your Own Identity Shows Promise, but Remains Fragmented

In general, consumers remain forced to create individual digital identities for every service they use. This can range from simple login/password credentials to higher-assurance identities based on strong identity proofing (such as a government-issued ID, or a bank ID). This has led to a proliferation of digital identities, most of which do not interoperate and are typically low assurance. This approach clearly will not scale as we move into the future, especially as our digital lives — across our connected homes, mobile devices and connected cars — increasingly rely on digital identity. Digital identity must be simple, secure and, in many cases, portable.

Bring your own identity (BYOI) is the concept of allowing users to select and use a digital identity that is self-managed or managed by a third party and external to the service in which it is used. Examples include social identities (such as Facebook, VK and WeChat) or higher-assurance identities (such as a bank identity or a government eID) or other blockchain-based decentralized identities to access multiple digital services. Service providers can be enabled to trust these external digital identities for the purposes of authentication and access to digital services, as well as for validated identity attribute sharing (see Figure 2).

Figure 2: BYOI Provider Types



Source: Gartner

BYOI = Bring Your Own Identity

719390_C

BYOI solutions in the market today fall into various categories:

- **Social Networks —** BYOI has been well-tested and proved globally with social networks. Services such as Facebook Login give service providers a way for the consumer to create accounts and log in to applications across multiple platforms. [8] Identity assurance levels are relatively low, however, and suitable for only the lightest of customer onboarding use cases. Social media platforms are infamous for large numbers of fake accounts, leading to market distrust of social networks as a source of identity assurance. Social network platforms report that the leading cause of the weakness of identity assurance on their platforms is the cost impact of robust identity proofing on social media lifetime account value.

- **Banks and Financial Institutions —** These have emerged as higher-assurance identity providers. Examples include Capital One in the U.S., BankID in Sweden or the bank-led identity network SecureKey Concierge in Canada. [9,10,11] These banks enable service providers to supply smooth onboarding experiences by leveraging the banks' significant base of verified customer identities.

- **Governments —** These can include a digital identity and, in some cases, a physical credential (e.g., a smart card or eID). These identities offer the strongest level of assurance, because they are often backed by identity proofing from several sources. From a BYOI perspective, these identities are often leveraged for scenarios that require a high level of trust (such as applying online for a mortgage or renewal of citizen services) or for identity proofing (such as employee enrollment).

With the worldwide implementation of International Civil Aviation Organization (ICAO) 9303, machine-readable travel documents (MRTDs), such as passports, smart-chip-enabled MRTDs offer a high degree of protection against forgery. Coupled with easily available MRTD solutions using embedded capabilities in smartphones and other consumer devices, this offers high levels of identity assurance for in-person and remote verification and corroboration.

- **Mobile Network Operators (MNOs) —** The level of trust assurance varies greatly across countries. MNOs in some regions require little identity proofing before issuing a SIM card; those in other regions require a government ID. The GSMA Mobile Connect initiative is one approach from the mobile industry that provides a standardized interface to enable MNOs to become identity providers. This enables service providers to support BYOI. [12,13] The rollout of GSMA Mobile Connect, in part, falls to the regional MNOs and is only available in a few regions globally.

In addition to solutions in the categories above, vendors such as ID.me are gaining traction in the U.S. with a federally certified, identity-proofing solution that offers a portable digital identity. This can be used across many government sites and an increasing number of commercial sites. With tens of millions of users signed up, driven mainly through interactions with government sites pertaining to veterans affairs or social security, it offers a glimpse of a BYOI model that is delivering value at scale.

Information on BYOI mechanisms, as well as the evolution of digital identity networks and decentralized and blockchain networks, can be found in "Innovation Insight for Bring Your Own Identity" and "Innovation Insight for Decentralized and Blockchain Identity Services." The market for BYOI remains fragmented — government identities remain jurisdictional, and many MNOs and banks have limited regional reach. Attempts are being made to address this. For example, in Europe, the electronic IDentification, Authentication and Trust Services (eIDAS) regulation helps ensure that citizens can use their own digital government identities to access public services available online in other EU countries. [14]

Finally, even within a region, the differing levels of assurance being offered, the varied customer journeys, and the different demographic user base of each BYOI mechanism mean that service providers may need to integrate many BYOI options. This is likely to be necessary to obtain meaningful coverage of the desired customer base. This "NASCAR problem" of cluttered registration screens remains another barrier to adoption. [15]

Market Analysis

Demographic Bias Is Becoming a Key Focus in Vendor Selection

The increasing focus on document-centric identity proofing in remote use cases is resulting in increased dependence on facial recognition algorithms to govern the identity-proofing process. Facial recognition algorithms are used to compare the selfie of a customer with the photo in their identity document. There has always been awareness of possible bias in this facial recognition process. However, we have observed clients showing far greater interest in this topic during the past six months. This is probably due to the increased political narrative and discussion on different aspects of inequality driven by the Black Lives Matter movement.

Bias with respect to race, age, gender and other characteristics is gaining attention. Clients are growing more keenly aware that demographic bias in the performance of identity-proofing processes could reflect negatively on their brand, in addition to raising possible legal issues. Clients are now far more interested in understanding how vendors measure demographic bias, and whether they are working to address it.

The U.S. National Institute of Standards and Technology (NIST) has carried out extensive and detailed testing on 189 face recognition algorithms, using more than 18 million images of approximately 8 million people. [16,17] The testing was on specific algorithms, rather than on vendor products that may be using these algorithms. NIST measured two types of error that the algorithms could make: false positives and false negatives. A false positive means that the algorithm incorrectly assessed images of two different people as showing the same person. A false negative means the algorithm failed to match two images that showed the same person.

A broad and complex set of demographic bias was found. For example, for one-to-one comparison and matching, the false positive rate for Asian and African-American faces was sometimes 10 to 100 times higher than for Caucasian faces. Another example was that false negative rates tended to be higher with images of women and younger people. It was also interesting to note that algorithms developed in Asia tended to have lower demographic bias on some specific tests.

The reasons for such demographic bias are varied, ranging from potential bias in the design of the algorithms themselves, to the composition of the training data used to feed the algorithms. Image quality was also cited by NIST as a key factor. In conversations with document-centric, identity-proofing vendors, we have found a spectrum of engagement on this topic. Some vendors have demonstrated little awareness of how their algorithms (proprietary or commercially bought) perform in this regard. Others have been able to promptly provide detailed analysis and demonstrable incremental improvements, exhibiting a strong focus on openness, transparency and responsibility. Security and risk management (SRM) leaders should interrogate potential vendors on this aspect of their solutions to ensure that performance aligns with the expectations of both the brand and customers.

Innovation Through Using Alternative Data Sources for Corroboration

Most vendors offering data-centric identity affirmation focus on so-called "'authoritative" data sources, such as credit bureaus, financial data, postal records, electoral rolls and other conventional sources. However, emerging areas of innovation in this space, from newer vendors that are exploring less conventional data sources to support the identity corroboration process, are emerging.

One example is SpyCloud, which uses human intelligence to identify and gather PII and credential data that has been leaked via breaches. Thus far, this has been leveraged to identify when a user logging onto a service is using leaked credentials, highlighting potential risk in the login process. However, such is the breadth and depth of the corpus of data that SpyCloud has gathered that it is proving to be an effective, yet unconventional source for identity affirmation. Different email addresses a customer may have used over many years can be tied via leaked PII and credential data, building a picture of an identity that may grow to include business and personal addresses and phone numbers.

Another example is Identiq, which has built a collaboration network among digital commerce organizations. For example, when presented with a new customer identity, an organization can ask the network whether the name, email address and device identifier of this new customer belong to an identity that other members of the network trust. Other member organizations can then respond based on their own identity-proofing efforts and their own transaction histories with that customer identity. No PII data is shared across the network.

Both examples illustrate that alternatives exist to checking so-called “authoritative” data sources when the requirement is identity affirmation, rather than identity proofing. Depending on the level of assurance needed for the identity-proofing process the affirmation capability is supporting, and the risk tolerance of the organization, such emerging approaches may also be attractive from a cost perspective.

Orchestration of the Identity Proofing Process Has Become a Critical Requirement

Many organizations will rely on more than one of the identity-proofing capabilities listed in this Market Guide. Orchestrating these different capabilities, most likely provided by different vendors, is an increasing challenge. Previous Market Guides have discussed the concept of the identity corroboration hub. This has evolved to align itself more closely with the concepts of orchestration, as outlined in the “Market Guide for Online Fraud Detection.” A number of vendors offer solutions that provide an orchestration layer to manage the identity-proofing process.

The sophistication of such orchestration or workflow capabilities varies widely. Simply ingesting risk signals all at once from multiple sources to arrive at a consolidated decision does not constitute orchestration. Management of multiple capabilities that are native to a single-vendor solution can result in workflow management, but also does not constitute orchestration. A complete identity-proofing orchestration solution must offer the capability to:

- Define a workflow for the identity-proofing process, typically, but not always, focused on the onboarding use case.
- Manage integrations to multiple vendors across a broad spectrum of identity-proofing and affirmation capabilities.
- Ingest and normalize the results from vendors in the same class of capability to facilitate the ease with which different vendors can be used and interchanged — for example, for comparison or

failover.

- Define policies that govern event handling at each step of the workflow and control the next step of the workflow with respect to the vendors that are called. This will control the UX, because further steps in the workflow may facilitate requesting further information from the customer.

- Manage changes to the workflow in a “no code” manner, typically via a visual drag-and-drop workflow interface.

- Deliver value-added analytics capabilities, such as processing the data returned by all vendors to deliver a simple verdict on whether the identity assertion falls within the defined organizational risk tolerance. This also includes analyzing all returned data in real time to identify risk signals through techniques such as link analysis and velocity checking.

Gartner sees an increasing number of vendors developing their orchestration capabilities. For many, this involves simple first steps on the path toward orchestration, such as adding the ability to ingest data from other vendors for a one-off assessment, but without workflow capabilities. For example, several document-centric, identity-proofing vendors have added integrations to data-centric identity affirmation sources. *Such vendors have realized that, if they don’t become the orchestrators, they will simply be the orchestrated.*

However, a number of more-mature, identity-proofing orchestration solutions are already in the market, including Trulioo, Sphonic and TruNarrative. Demand for solutions offering orchestration of the identity-proofing process is growing from SRM leaders who see such orchestration capabilities as key strategic assets for a number of reasons:

- A single integration that negates the need to manage any other tools directly, reducing implementation cost and complexity.

- Flexibility to change the identity-proofing process and optimize it via A/B testing with minimal impact.

- Redundancy through workflows that include failover vendors in the event of latency or downtime from a primary vendor.

- Scalability in supporting business requirements, such as expanding into new regions that may require the leveraging of new vendors or data sources.

Representative Vendors

Market Introduction

The vendors listed range from well-established providers with a significant presence in the identity proofing market, and vendors that are often cited in client interactions, to smaller, less-often-cited identity proofing vendors, especially those offering fresh approaches to meeting client requirements. (See Note 1 for a discussion of the rationale.) It is challenging to segment the market, because many vendors offer services that cut across the different capabilities described in this guide. However, in an attempt at clarity, we break them down into the following categories:

- **Document-Centric Identity-Proofing Vendors (see Table 1) —** These vendors assess the authenticity of an identification document via a submitted image, and also compare a selfie from the customer with the picture in the document. Detection of genuine presence is a key feature to meet the definition of identity proofing. Many of these vendors have built integrations with data-centric, identity affirmation sources to augment their services.

- **Vendors With Data-Centric Identity Affirmation Foundations and Document-Centric Identity-Proofing and Device-, Digital-Attribute- and Behavior-Analytics-Focused Identity Affirmation Capabilities (see Table 2) —** These vendors traditionally focused on data-centric identity affirmation, typically acquiring and gaining access to a range of data sources and applying their own linking and correlation of these sources to create master identities. In recent years, these vendors have evolved to add (typically by acquisition or partnership) document-centric identity-proofing, device affirmation and behavioral analytics capabilities. The result is a broad offering that spans many capabilities, anchored in vast datasets for real-world identity affirmation.

- **Device- and Behavioral-Analytics-Focused Identity Affirmation Vendors (see Table 3) —** These vendors support the identity-proofing process by providing trust and/or risk signals based on device characteristics and the behavior of the customer. The latter includes identifying signs that the interaction is being performed by a bot. Some vendors focus more strongly on one of these capabilities than the other.

- **Phone Number-Focused Identity Affirmation Vendors (see Table 4) —** These vendors offer such services as the detection of automatic number identification (ANI) spoofing and obtaining identity data about the registered owner of the phone number, in addition to information such as age of SIM or porting.

- **Vendors With Strong Orchestration Capabilities (see Table 5) —** These vendors deliver value by connecting to other vendors and data sources, and acting as the single point of integration for clients with strong workflow capabilities and value-added analytics.

Table 1: Document-Centric, Identity-Proofing Vendors

Vendor ↓	*Product, Service or Solution Name* ↓

Vendor	Product, Service or Solution Name
Acuant	AssureID and FaceID
AuthenticID	*No specific product name*
Daon	IdentityX
IDEMIA	ID Proofing
IDmission	Identity
Intellicheck	*Multiple applicable products*
Jumio	Identity Verification
Mitek	Mobile Verify
Onfido	*No specific product name*

Source: Gartner (September 2020)

Table 2: Vendors With Data-Centric, Identity Affirmation Foundations and Document-Centric Identity Proofing and Device-, Digital Attribute-, and Behavior-Analytics-Focused Identity Affirmation Capabilities

Vendor	Product, Service or Solution Name

Vendor	*Product, Service or Solution Name*
GBG	*Multiple applicable products*
LexisNexis Risk Solutions	*Multiple applicable products*
TransUnion	IDVision with iovation

Source: Gartner (September 2020)

Table 3: Device- and Behavioral-Analytics-Focused, Identity Affirmation Vendors

Vendor	*Product, Service or Solution Name*
BehavioSec	*No specific product name*
BioCatch	*No specific product name*
buguroo	bugFraud
Callsign	*Multiple applicable products*
IBM	Trusteer
NuData Security, a Mastercard solution	NuDetect
SecuredTouch	*No specific product name*

Source: Gartner (September 2020)

Table 4: Phone-Number-Focused, Identity Affirmation Vendors

Vendor	Product, Service or Solution Name
Neustar	*Multiple applicable products*
Next Caller	VeriCall
Nuance	*No specific product name*
Pindrop	*Multiple applicable products*
Prove (formerly Payfone)	*Multiple applicable products*
Smartnumbers	Protect

Source: Gartner (September 2020)

Table 5: Vendors With Strong Orchestration Capabilities

Vendor	Product, Service or Solution Name
4Stop	*No specific product name*
Experian	CrossCore
Sphonic	Workflow Manager

Trulioo	GlobalGateway
TruNarrative	*No specific product name*

Source: Gartner (September 2020)

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 Recommendations

The need for confidence in the identity of customers during remote interactions remains paramount. Account opening, registration, application or enrollment are all typical cases in which identity proofing is applicable. There is no single, one-size-fits-all approach. Myriad identity-proofing capabilities are available, depending on the use case and the level of confidence in an identity that is tolerable.

SRM leaders should take the following steps.

Understand organizational risk tolerance for identity-proofing use cases:

- Work closely with internal stakeholders to understand the events in the customer journey for which identity proofing is required.
- Map out the identity-proofing capabilities that are applicable to each event.
- Understand the degree of confidence in an identity that is required for each event — in some cases, this will be driven by organizational risk appetite; in others, it will be driven by compliance requirements.

Avoid seeing identity proofing, OFD and user authentication as separate functions:

- Treat identity proofing, OFD and user authentication as activities on the same spectrum of risk mitigation.
- Drive efficiency gains and cost savings by assessing where vendors can be used across identity proofing, OFD and authentication use cases.

Build an identity-proofing strategy on a foundational orchestration layer:

- Leverage a vendor that has built connections to multiple other vendors and data sources and offers flexible workflow capabilities.
- Optimize your identity-proofing process by using this orchestration layer to test and evaluate different workflows, comparing different vendors and data sources to achieve your identity-proofing objectives.
- Support the scalability of your business by using the orchestration solution to connect to vendors and data sources that facilitate expansion into new regions.

Demand accountability from vendors with respect to demographic bias:

- Interrogate vendors that use face recognition algorithms to reveal data and insights into demographic biases in their solutions.
- Accept that demographic bias is common in many solutions, and that it may not be possible to eliminate in a timely manner; however, to drive fair handling for all customers, pressure vendors to improve.
- Communicate openly with all relevant internal stakeholders to ensure that the risks that demographic bias in the identity-proofing process may present to your brand are understood.

Evidence

[1] "The 15 Biggest Data Breaches of the 21st Century," CSO

[2] "World's Biggest Data Breaches & Hacks," Information is Beautiful

[3] "LexisNexis Risk Solutions Announces ThreatMetrix Acquisition Close," LexisNexis Risk Solutions

[4] "LexisNexis Risk Solutions Announces Definitive Agreement to Acquire Emailage," LexisNexis Risk Solutions

[5] "TransUnion Completes Acquisition of iovation," TransUnion

[6] "Go for Good," Jumio Go Product Page

[7] "Identity Verification Support for Essential Services," Onfido

[8] "Facebook Login Overview," Facebook for Developers

[9] "Products — Sign In With Capital One," Capital One

[10] "BankID Homepage," BankID

[11] "SecureKey Concierge Service," SecureKey

[12] "Identity," GSMA

[13] "Mobile Connect Homepage," Mobile Connect

[14] "Trust Services and Electronic Identification (eID)," European Commission

[15] "NASCAR Problem," IndieWeb

[16] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology (NIST)

[17] "Face Recognition Vendor Test (FRVT) — Part 3: Demographic Effects," NIST

Note 1
Representative Vendor Selection

The listed vendors represent what's core in the market, what extends it and what will transform it. They were selected on the basis of one or more of the following:

- Vendors offering capabilities that support identity proofing in ways that are unique, innovative and/or demonstrate forward-looking product strategies.
- Frequent inquiries by Gartner clients about a particular vendor for identity-proofing use cases.
- Vendors that represent particular market segments or geographic regions, thus helping to illustrate the breadth of the market.
- Fair representation from year-to-year, with rotation of vendors that may have previously met the above requirements, but were omitted simply due to space restrictions.

The representative vendors here do not constitute an exhaustive list of all providers with these characteristics; we are limited to enumerating a limited set of vendors. Necessarily, many worthy vendors have been omitted with no implied criticism; neither is inclusion an endorsement.