DIGITAL IDENTITY TRACKER®

DECEMBER 2021/JANUARY 2022

PYMNTS.com | jumio

Read the previous edition

■ DECEMBER 2021
Digital Identity Tracker®

DIGITAL IDENTITY TRACKER®

PYMNTS.com | jumio

ACKNOWLEDGMENT

Digital Identity Tracker® was produced in collaboration with Jumio, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

EDITOR'S LETTER

The digital identity space has become more complicated as consumers are depending more on digital interactions during the pandemic. Their engagement with digital tools may be on the rise, but their trust in these technologies is wearing thin. Many do not believe that companies that ask for their personal data can adequately protect this information or keep it private, in fact.

This means customers place a premium on finding companies they can trust, and organizations that demonstrate a dedication to ethically handling personal data via cutting-edge digital identity solutions have an opportunity to stand out from the competition. Even companies that have suffered data breaches or security failures can realize significant gains in customer trust and confidence if they respond to these unfortunate incidents with transparency and open communication.

Consumers also value convenience. Too much friction during verification and authentication processes can cause dissatisfaction and abandonment, though a certain amount can reassure users that a company is taking their security and privacy seriously. Biometrics and secure tokens in particular can help companies clamp down on fraud without bogging down authentication. These options are gaining attention from bad actors as well, as cybercriminals are investing in improvements to deepfakes and other schemes to trick biometric security methods.

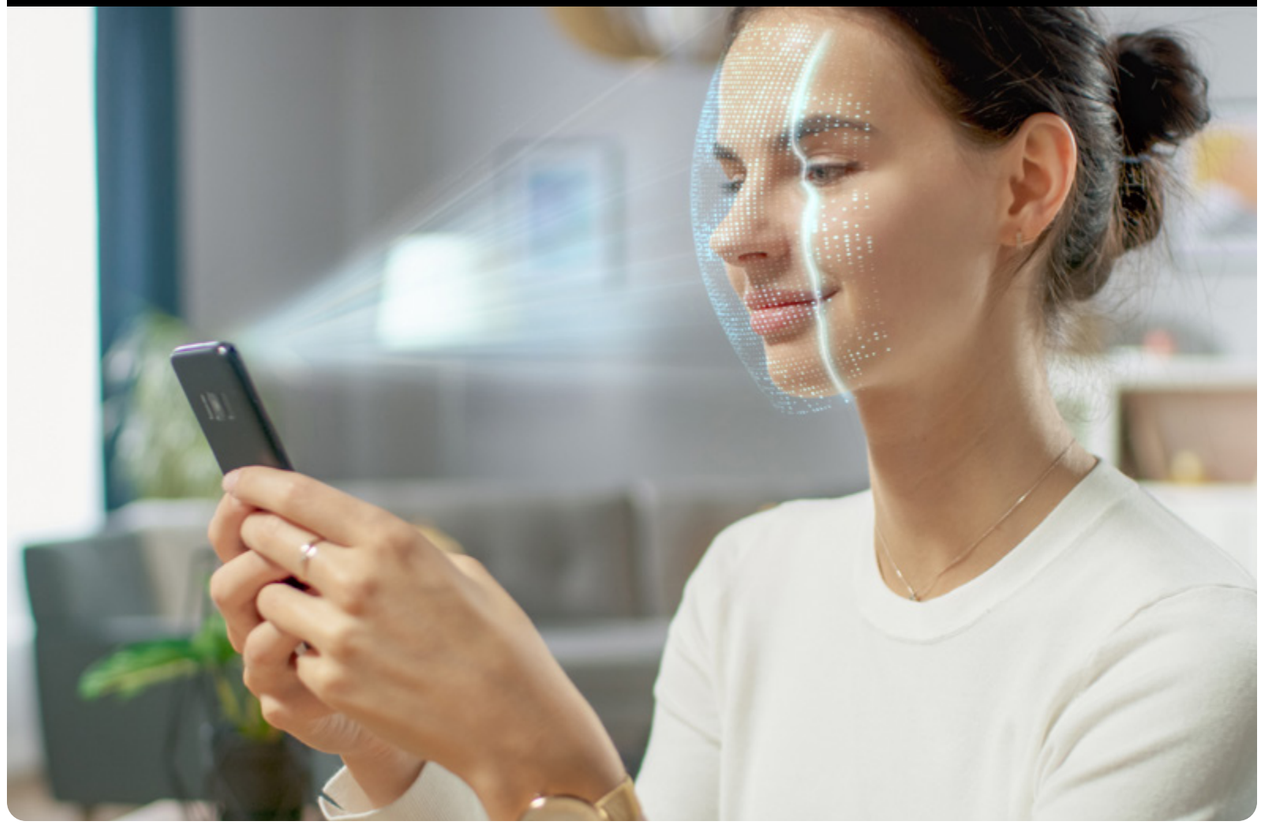
Many consumers remain concerned about their privacy. Even companies using the latest authentication technology require users to provide personal information that can help them deter fraudulent activity — and customers ultimately have to trust those companies with sensitive details. Companies also must combat any lingering apprehension consumers may have regarding biometric technologies and other advanced authentication tools by illustrating the care with which their sensitive data is handled.

The December/January edition of the Digital Identity Tracker, a PYMNTS and Jumio collaboration, examines how companies can build trust with their customers by emphasizing transparency at every level, including in how they collect, use and potentially share customer information. It also details how those companies that establish a reputation for supporting ethical and transparent digital identity practices can earn new customers, keep existing ones satisfied and grow their market share.

Thought Leadership Team
PYMNTS.com

Feature Story

IBIA On Easing Consumer Privacy Concerns Surrounding **Biometrics Use**



BIOMETRICS REQUIRE USERS TO TRUST COMPANIES WITH THEIR PERSONAL DATA, CREATING THE CHALLENGE OF REASSURING CONSUMERS THAT THOSE COMPANIES ARE HANDLING THAT DATA IN A SECURE AND ETHICAL MANNER.

Securing personal data is a leading concern of consumers, as is not knowing what personal information companies have collected.

Growing numbers of consumers are engaging in online interactions and transactions, and the majority want better user experiences — even if those experiences require handing over more personal data. Organizations developing and implementing biometric technology will influence public perception with the choices they make, whether they focus on user engagement or public policy development.

Robert Tappan, managing director for industry trade group International Biometrics + Identity Association (IBIA), said it is paramount that organizations using biometrics maintain transparency and ensure biometric identity verification protects both consumers and their data.

"We believe that it is essential to communicate with people about what biometric information is being collected, what it will be used for, with whom it will be shared and for how long it will be retained," Tappan said.

SECURING PERSONAL DATA WITH BIOMETRICS

Handling the biometric information collected for identity verification requires companies to respect both people and data, ensuring biometric applications protect privacy and minimizes bias, according to Tappan. Companies using biometrics also must have processes in place for remedying problems such as inaccurate matches should they occur.

“Companies have a duty to ensure privacy and integrity and the responsible use of biometric information,” he said. “Our member companies also want to work with policymakers to develop biometric legislation that facilitates appropriate reporting, oversight and other accountability measures.”

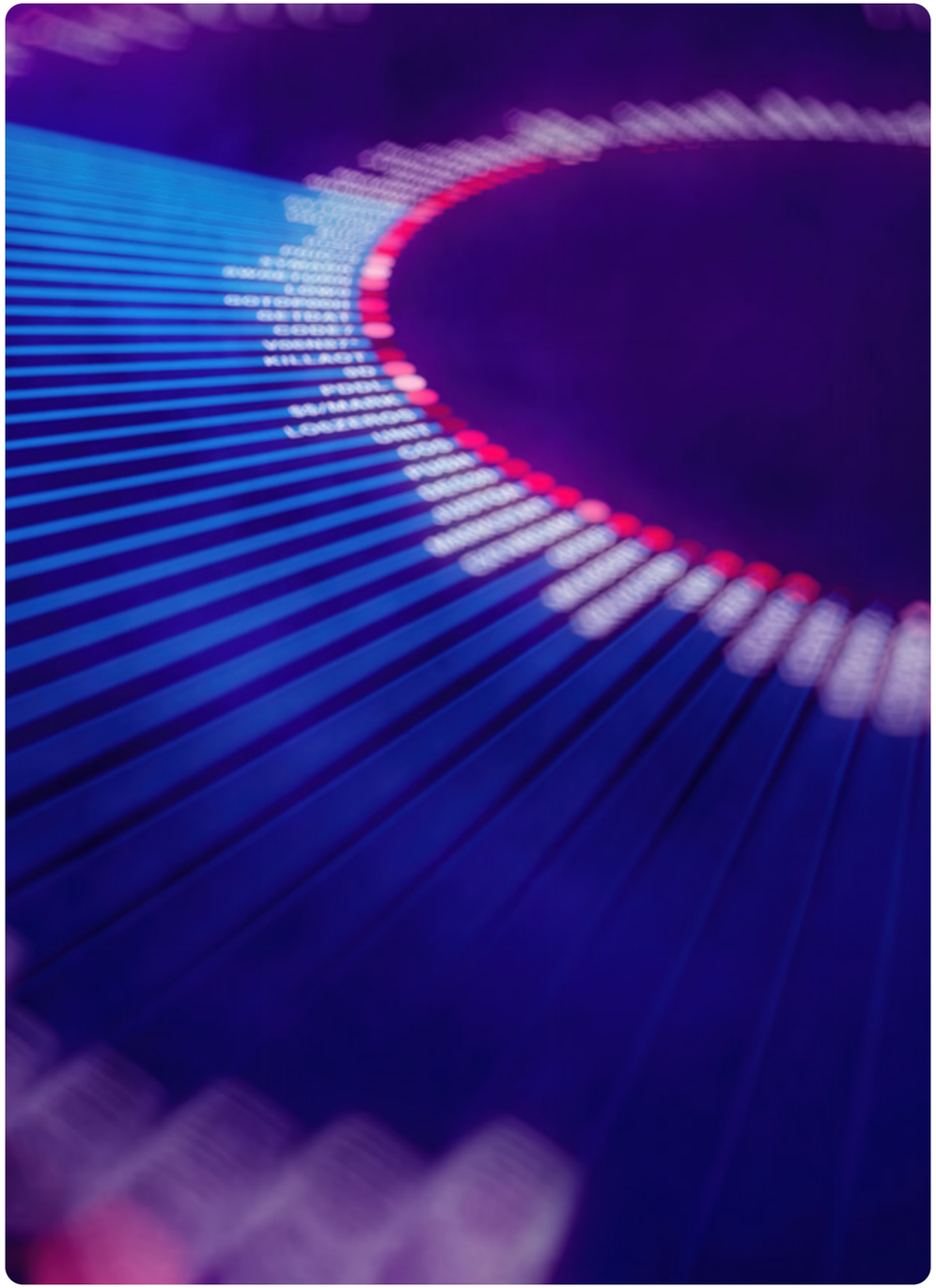
BUILDING USER TRUST

Tappan said consumers must have a clear idea of not just what biometric data is collected, but also how it is used and retained, including how long the data will be kept. Organizations must ensure the only individuals with access to biometric data are those authorized for that purpose and secure the privacy and integrity of user data.

“There needs to be an ironclad, trust-based relationship between the individual providing biometric information and the company that is collecting the biometric data,” he said.

Accountability to users is essential for both the organizations that employ biometrics and the developers behind the technology, Tappan said. All parties involved must work to ensure those using biometric technology are not just armed with the latest capabilities but also up to date in understanding how to use them.

“First and foremost, biometric technology developers and users need to work together to develop and provide training to the individuals operating biometric systems,” Tappan said. “They need to conduct operational performance assessments on a regular basis when deploying these technologies and regularly upgrade these systems to ensure the use of the most accurate, secure and privacy-protective technologies available.”



THE BIOMETRICS ARMS RACE

While biometrics offer added security, the same bad actors who have developed techniques for skirting other security solutions are unlikely to give up just because fraud scheme execution becomes more difficult. As with any identity verification technology, biometrics technologies face attacks to gain access to secure data. A report from the Dawes Centre for Future Crime identified deepfakes as the most serious criminal threat posed by artificial intelligence (AI). Deepfakes have the potential to be used as a tool in defeating biometric identification, and the industry is responding with its own advancements.

"The goal is to make continuous improvements to make these technologies better and more accurate and, therefore, more trustworthy and secure," Tappan said. "No technology is ever 100% correct all of the time. Certainly, some technologies need to be continuously refined and improved. Nevertheless, biometric technologies are far superior in accuracy overall compared to unassisted human assessment."

For the industry, that means constantly improving existing methods for identifying an individual using biometrics, as well as developing new technologies that use additional identifiers, such as behavioral biometrics. As deepfakes become more sophisticated, biometric developers are creating ever more sophisticated methods for catching them and using AI to spot signs of manipulation that humans cannot detect.

User demand for storing and accessing personal data in the cloud continues to trend upward, presenting temptation to those seeking to gain access to that data for criminal ends. Biometrics-based solutions offer the most advanced method of verifying identities, but those employing the technology still face challenges in everything from creating secure frameworks to providing transparency to users and staying ahead of bad actors.

PYMNTS Intelligence

How Companies Can Manage **Consumers' Privacy Concerns** In The Age Of Digital Identity Solutions

Consumers have become dependent on digital interactions, and they are focusing more on privacy as a result. They want to feel secure and avoid processes that take too long when sharing their personal information, but their skepticism of technology can serve as a major stumbling block. One survey revealed that 82% of United States adults are concerned that their online data may not be secure and that 82% also would like to have a better understanding of the personal information companies have collected. Just 39% said they know where their online data is stored, in fact.

Regardless of their data-related concerns, 59% of consumers said they would be happy to allow companies greater access to their personal data if doing so gives them a better user experience. This means organizations stand to attract new customers — and engage and retain existing ones — if they can implement digital identity solutions that offer customers smooth onboarding and authentication experiences that do not skimp on security and privacy.

This month, PYMNTS examines consumers' desires for privacy and security as they continue to tackle everyday activities such as banking and shopping digitally. It also examines what consumers really want from companies that have access to their personal data.

PRIVACY CONCERNS ARE UBIQUITOUS, BUT REASONS VARY

Consumers in certain markets tend to take old-school approaches to storing personal information. Research shows that U.S. consumers' most preferred storage solution for personal details is to jot them down on paper: 54% of adults prefer this method, according to one study, including 68% of those in the 18-to-24 age range. While 49% of adults are comfortable using some electronic storage method to secure sensitive information, those ages 18 to 24 were most comfortable using a cloud-based method.

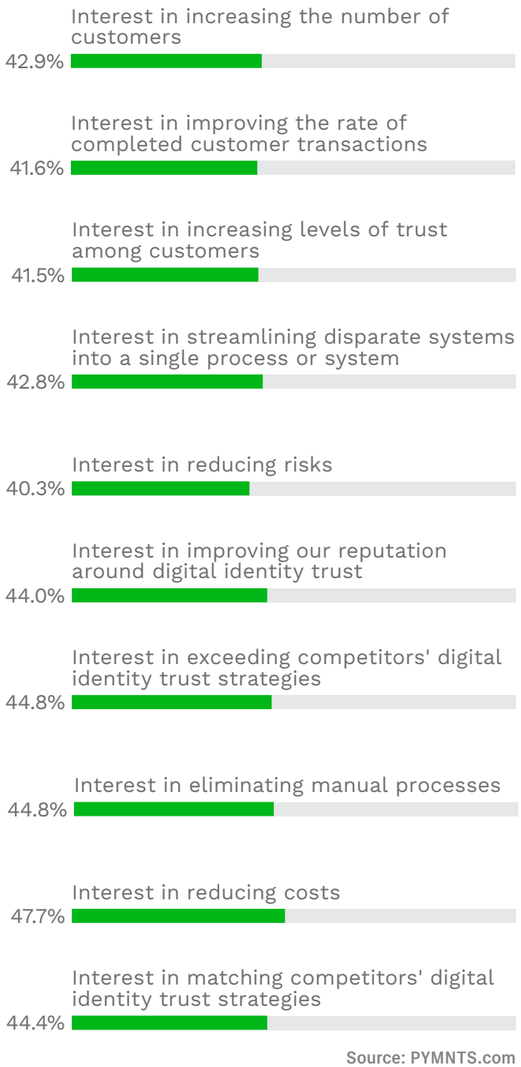
Still, 80% of U.S. adults say they have concerns about storing their private data on the cloud, a sizable majority. The sources of these concerns vary. The most common concern, shared by 31% of adults, is that their information might be stolen, yet 18% said they are worried they will forget the password to access their data and 15% fear their data could be sold or shared without their permission.

Despite these concerns, only 9% of North American consumers feel strongly that they understand how to keep their personal data secure, and just 18% believe they have the tools to navigate the world of data privacy. Most North Americans also report being suspicious of what companies do with personal information, and 69% want better explanations from technology companies about how they make money and handle personal data.

FIGURE 1:

Select interests firms consider "very" or "extremely" important to adopt or improve for consumer identification

Portion of firms that plan to invest in digital authentication solutions that cite select interests as "very" or "extremely" important to adopt or improve for consumer identification



Source: PYMNTS.com

Companies that address these concerns have much to gain, as 63% of North American consumers said organizations' data-handling methods and ethics would influence whether they choose to do business with such entities.

Some consumers have stuck with businesses despite data breaches or failures to protect sensitive data, but this decision could have more to do with a perceived lack of alternatives rather than enduring trust. Sharing personal information with companies is a "necessary evil" for 67% of consumers, and 85% are on the lookout for companies they feel they can trust.

SOLVING THE PRIVACY DISCONNECT BETWEEN BUSINESSES AND CONSUMERS

While 76% of business leaders said there is a crisis of consumer trust in technology companies, 80% gave their own companies an A or B grade in regard to tapping solutions that protect user data, and 55% believe consumers' trust in their technology is rising. The story is different among consumers, however, with 21% saying their trust in businesses' technology is growing and 28% saying their trust is waning.

Companies largely put themselves on the hook when it comes to being responsible for privacy and security: 58% said this responsibility falls on them rather than on government regulators or consumers. Additionally, 85% said their companies are compliant with the highest security and privacy standards set by governments around the world.

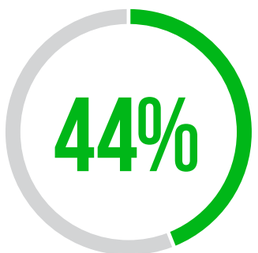
© 2022 PYMNTS.com All Rights Reserved

What consumers want and what companies are prioritizing may not always be in alignment, however. Consumers are concerned about data breaches and other failures, but they are even more attuned to matters regarding data transparency. Forty-four percent of consumers want to see visible action and full transparency after a data breach, 39% want to know how companies use or monetize their data and 39% value transparency in how their data is shared.

Authentication-related friction can frustrate customers, but data shows that the added sense of security more than offsets this dissatisfaction in most cases. Research suggests businesses may in fact focus too heavily on eliminating friction at the cost of ensuring security — a move that ultimately can harm customer satisfaction. This is particularly notable as consumers gain familiarity with seamless authentication methods such as biometric identification and secure tokens that can improve transaction security while reducing friction.

Customers still want transparency among businesses offering innovative authentication solutions, and clear communication from companies can assure users that the digital identities they use to access personal data are secure. Many governments are setting the groundwork with legislation to protect consumers' digital identities.

Consumers will continue to expect companies to transparently and responsibly handle and manage their personal information. Governments are all but certain to step up their regulatory efforts as well. Companies adopting the right digital identity solutions to keep their customers' experiences fast without compromising security and privacy will be best positioned to build consumers' trust in the long term and earn their continued loyalty.

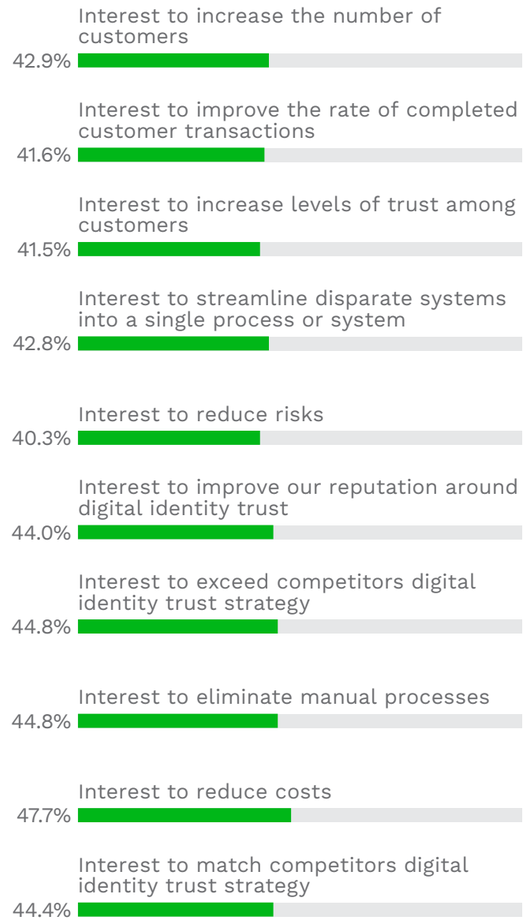


SHARE OF CONSUMERS WHO WANT TO SEE **VISIBLE ACTION AND FULL TRANSPARENCY** AFTER A DATA BREACH

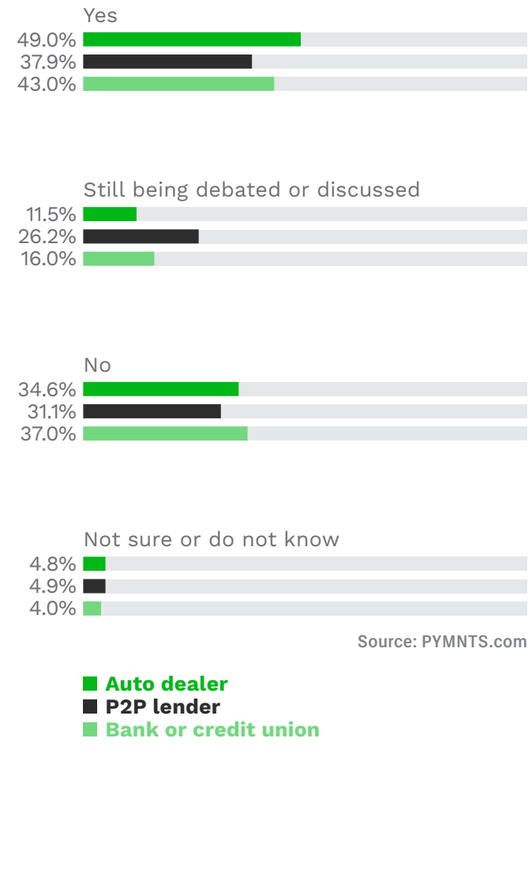
FIGURE 2:

Select interests firms consider "very" or "extremely" important to adopt or improve for consumer identification

2A: Firms' plans to invest in digital authentication solutions, by "very" or "extremely" important goals



2B: Firms' plans to invest in digital authentication solutions, by industry segment



Source: PYMNTS.com

NEWS & TRENDS

DIGITAL IDENTITY SECURITY AND PRIVACY DEVELOPMENTS

AIR TRAVELERS GROWING MORE COMFORTABLE PROVIDING BIOMETRIC DATA

More consumers who have been on the fence about using biometric identity solutions appear to be coming around as a result of the pandemic, particularly when it comes to travel. A recent International Air Transport Association (IATA) survey found that passengers were growing more comfortable with sharing biometric data and that convenience was weighing heavily on their decisions. It showed that 73% of passengers now are willing to provide their biometric data to access more streamlined experiences, up from the 46% who said the same in 2019.

The global health crisis's influence on travel processes cannot be overlooked when analyzing these findings. Travel processing now takes from 1.5 to three hours on average, even though air traffic levels currently are 70% lower than they were before the pandemic's onset. Data shows that 86% of passengers who say they have undergone a biometric-based screening report their experiences were positive, but only 36% of all consumers have undertaken biometric scans and more than half still have concerns about data breaches and misused information. It will be up to biometrics providers to ease consumers' concerns regarding the technology's security and privacy to further boost usage.

PRIVACY INTERNATIONAL OUTLINES FINDINGS RELATED TO MOSIP DIGITAL ID SYSTEM

Some organizations are examining the development of digital ID systems worldwide with an eye toward ramifications relating to infrastructure, security and privacy. United Kingdom-based nonprofit Privacy International recently launched a series to investigate the digital identity solutions in place in India and Estonia as well as the Modular Open Source Identity Platform (MOSIP) being used across Ethiopia, Guinea, Morocco and the Philippines.

The group's first report centered on MOSIP. The platform operates as an open-sourced, modular application programming interface (API)-based foundational digital ID system, meaning various components can be replaced seamlessly. The report also outlined the steps a nation would need to undertake to transparently and legally implement the system. Privacy International concluded that the platform marks a significant step toward the implementation of an updatable ID system based on privacy, though there still are some logistical and regulatory kinks to address.

KYC FRAGMENTATION LEAVES SECURITY GAPS THAT SINGLE-VENDOR PLATFORMS COULD PLUG

Organizations may confront several hurdles as they seek out digital identity solutions to combat fraud, particularly in the increasingly fragmented know your customer (KYC) market. A variety of vendors in the space are focused on niche areas, prompting many enterprises to form their defenses from multiple providers' solutions. Unfortunately, this piecemeal approach can leave technological and logistical gaps that can create inefficiencies and weak points for fraudsters to exploit, Robert Prigge, CEO of digital identity solutions provider Jumio, said in a recent PYMNTS interview.

Prigge explained that organizations could spot bad actors more easily and simplify administration by using a single-vendor solution, which would lead to better experiences for consumers and businesses alike. It also would prevent enterprises from having to integrate with multiple platforms and manage numerous contracts and vendors to maintain compliance. He concluded that the need for single-vendor solutions is likely to promote further consolidation of solutions in the future, with a handful of platforms emerging as key industry leaders.

GOVERNMENT-RELATED DIGITAL ID **DEVELOPMENTS**

NJ DRIVERS RAISE CONCERNS OVER LAW ALLOWING THEM TO VERIFY REGISTRATION VIA MOBILE DEVICE

A New Jersey law that would permit drivers to use their mobile devices rather than physical documents to verify their vehicle registration is drawing scrutiny from some drivers concerned about the implications of handing over their unlocked smartphones to law enforcement officials. The law is not yet in effect, however, and the New Jersey Motor Vehicle Commission has 18 months to implement security safeguards as it creates its electronic registration system. The solution will allow residents to prove their registration is current by showing law enforcement officers electronic copies or images of the documentation, such as a photo of the registration. Michigan enacted a similar law in 2017, and Tennessee followed in 2019.

New Jersey legislators said there are several safeguards in place to prevent misuse by law enforcement officials. The law permits officers to observe only the registration as it is presented on the device and forbids them from searching it, for example. Officers also are required to ignore any information they observe unintentionally, including text messages that pop up on the screen while they are in possession of a device. New Jersey drivers still are permitted to show a physical copy of their registration if they do not want to hand officers their phones.

MISSISSIPPI MOBILE ID PROGRAMS OFFERS STATE ID VIA MOBILE DEVICES

Mississippi is another state working to expand access to digital ID alternatives for its residents. The state recently announced that residents can install a mobile app, Mobile ID, that contains a digital version of their driver's license or state ID. The program currently is voluntary and is not intended to be a wholesale replacement for physical ID in some instances. Physical documentation still is required by law enforcement or for travel-related processes such as boarding an airplane. Most information is stored in the Mississippi Department of Public Safety (DPS) database, and the only information stored in the app is the user's driver's license and phone number, which the DPS uses to locate the person's records. Accessing the information on the device requires a facial recognition scan, a fingerprint scan or a PIN code.

The state purports that the Mobile ID program is more secure and private than using a physical driver's license for certain applications. The app permits age verification without providing the user's specific date of birth, for example, and push updates from the DPS ensure the information on the app is up to date. The app is available for devices using Android and iOS operating systems.

SCOTTISH NHS ELECTRONIC COVID-19 PASSPORTS EXPOSE USERS TO SECURITY RISKS

Government agencies that fail to adequately secure their digital identity solutions can make residents vulnerable to fraud. The Scottish National Health Service (NHS) recently found itself in hot water after its COVID-19 status app was revealed to be leaking private information to third parties. The app was intended to help users verify their vaccination statuses and limit contact between vaccinated and unvaccinated individuals. The app was implemented in October and made available to any fully vaccinated individuals 12 years old or older to prove their vaccination status via a QR code certificate. Residents 18 years old and older are required to show a vaccination certificate if requested to do so when accessing venues that could pose considerable COVID-19 transmission risks.

Personal data points stored in the app — such as names, birthdates and vaccine records — were revealed to have been shared with a number of companies, including Amazon and Microsoft. News of the leak comes amid existing resistance to the app related to long lines and unhappy customers taking out their frustrations on venue staff when required to verify their vaccination status. The Scottish government said not all third parties identified as receiving information from the app had access to sensitive data.

MOBILE DEVICES
TAKE ON DIGITAL ID ROLES

APPLE PATENT INDICATES TECHNOLOGY FOR SECURE ID PROVISIONING AMONG MULTIPLE DEVICES

A new Apple patent application suggests the company plans to enable the use of its iPhones and Apple Watches as primary ID devices beyond applications such as digital driver's licenses. The company has been working with state-level governments to encourage digital ID recognition using mobile devices. The latest patent application describes designs for sharing private, identifiable information among a group of mobile devices without engaging with or compromising the personal information of any individual user.

Apple said one potential use case for the technology could involve an individual purchasing group tickets to an event, then electronically provisioning the relevant electronic certificates to individual members' devices. The provision system would not store any credentials, the company said, and it would have no knowledge of the individual certificate holders until each device connects to the system for verification. The system would not have access to certificate users' personally identifiable information (PII), and private information would be exchanged only between buyers and sellers during initial purchases.

The growing importance and continued challenges of digital authentication

PYMNTS.com | jumio

Businesses face a number of challenges in implementing and improving digital authentication, while the need for such security measures has become apparent as more consumers conduct transactions online.

Sacrificing growth for better digital security

79% of surveyed businesses would prefer to increase the security of digital transactions, regardless of whether doing so limits acquisition of new customers.

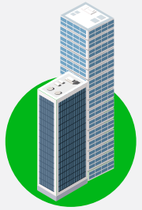
85%
Portion of auto dealers prioritizing security over acquiring customers

70%
Share of P2P lenders prioritizing security over acquiring customers

83%
Portion of banks and credit unions prioritizing security over acquiring customers

71%
Share of large urban area businesses prioritizing security over acquiring customers

79%
Portion of city businesses prioritizing security over acquiring customers



86%
Share of town or rural businesses prioritizing security over acquiring customers

Overcoming digital authentication barriers

Businesses planning to invest in digital authentication solutions have a number of hurdles to overcome, both internal and external, but some of the biggest hurdles involve being certain that customers are prepared to handle changes to digital authentication.

51%
Portion of businesses with customers lacking the skills to navigate digital authentication

47%
Portion of businesses with digital processes that resulted in false identities

48%
Share of businesses with customers lacking the technology to navigate digital authentication

47%
Share of businesses that lack the financial resources needed to implement digital authentication

Coordinating fraud prevention with customer-facing operations

The lack of coordination between fraud-and-risk management teams and customer-facing operations hinders identity verification and authentication processes, preventing them from becoming more efficient. More mature companies struggle less than others, but almost half of them still lack coordination between these two key aspects.

Companies in business more than 30 years

45%	Tightly coordinated
6%	Coordinated
49%	Not coordinated

Companies in business fewer than 10 years

21%	Tightly coordinated
5%	Coordinated
74%	Not coordinated

DIGITAL IDENTITY TRACKER®

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

ABOUT

jumio.

When identity matters, trust Jumio. Jumio’s mission is to make the internet a safer place by protecting the ecosystems of businesses through cutting-edge online identity verification and authentication services that quickly and accurately connect a person’s online and real-world identities. Jumio’s end-to-end identity verification solutions fight fraud, maintain compliance and onboard good customers faster.

Leveraging advanced technology including informed AI, biometrics, machine learning, certified 3D liveness detection and human review, Jumio helps organizations meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 225 million identities issued by over 200 countries and territories from real-time web and mobile transactions. Jumio’s solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, California, Jumio operates globally with offices in North America, Latin America, Europe and Asia-Pacific and has been the recipient of numerous awards for innovation. For more information, Please visit www.jumio.com.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at **feedback@pymnts.com**.

DISCLAIMER

The Digital Identity Tracker® may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED “AS IS” AND ON AN “AS AVAILABLE” BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.