WHITE PAPER

The Future of Identity

Proving who we are across the physical and digital worlds.

Steve Ritter, Chief Technology Officer, Mitek

"Who are you?" is a question that has been fundamental to business and social life throughout history. But never has the answer held such far-reaching implications for the daily lives and possible futures of so many individuals and enterprises.

Today our ability to prove who we are across the physical and digital worlds is a key factor in how much access we have to the ever-expanding bonanza of mobile/online information and services. In our businesses, how we ask for and verify proof of identity from customers and potential customers is a key factor in how successful we will be.

This is a pivot point. Both conceptually and practically, identity will be far different in the years ahead than in all the centuries before.

What's changing? For better? For worse? In this paper we share our point of view about today's state of identity and how to steer toward a more advantageous future of identity for us all.

Mitek

July, 2019

Identity in a world "where everybody knows your name" and no one can keep a secret

For centuries identity has been a concept rooted in the physical world, important largely for local transactions.

The concept has evolved, of course, from eras when a person's identity came from being a member of a roving band of hunter-gatherers, or the son or daughter of someone. As societies developed, identity expanded to include notions of residency or citizenship in a town, city or nation.

Still, for all that time, until very recently, the assertion and validation of identities took place primarily through face-to-face interactions. People could run a tab at the neighborhood pub or grocery because the owner knew them by sight. You went to government offices to get a driver's license or apply for a passport. Sitting down with a branch manager was how most people opened bank accounts and applied for loans.

That changed, of course, with the internet, which enables us to purchase goods and services, and interact with people all over the world. For some of these transactions and interactions, we have to establish an account and provide some sort of proof that we are who we say we are.

"Sometimes you want to go where everybody knows your name."

The theme song of the '80s sitcom *Cheers* evoked nostalgia for a time when our sphere of interaction was largely defined by neighborhoods. Today digital connections are extending that sphere across the globe. People and organizations thousands of miles away address us by our first name–but how do they know who we are?

In the early days of global connectivity, knowledge-based methods that rely on secrets such as passwords and question/answer sets worked pretty well for identity verification. But today, with hacking, big data processing and artificial intelligence tools widely and inexpensively available to individual fraudsters and massive criminal networks alike, "secure" stores of personally identifiable information (PII) are constantly being breached. There's no such thing as a secret anymore.

And that has far-reaching implications for consumers, business and government. Let's take a look at the state of identity in today's connected world.

HOW IT WAS

HOW IT IS

The best and worst of times

Nineteenth-century novelist Charles Dickens was a keen observer of societies in the midst of tumultuous change. If he were here now, it would be right up his alley to write tragicomedies about stolen, misused and misunderstood identities. Still, Dickens' stories usually had an upside, with characters transcending the limits of their lives to experience greater opportunities and good fortune. Living in today's connected world is similarly a mixed bag of "best of times" and "worst of times."

Certainly, the upside for both consumers and businesses is tremendous. As Chris Skinner, consultant and commentator on global financial services, says in his 2018 book *Digital Human*:

"This digitalization of the planet is bringing about a major transformation. Everyone on the planet will be included in the network and everyone on the planet will get the chance to talk, trade and transact with everyone on the planet in real time. Unlike the Industrial Revolution during which only a limited number of humans gained access to wealth and trade, this digital revolution will give everyone a chance."

But because the traditional method of face-to-face identity verification is no longer practical, and the relatively recent method of knowledge-based verification is no longer reliable, consumers and businesses now face more risks than ever before.

It's not just that our personally identifiable information is being hacked...

Consumers and businesses today also face rising risks because many of the organizations we transact with online aren't using reliable methods to verify a user's identity.

If there were any doubt about that, in May 2019, the U.S. Government Accountability Office (GAO) issued a report outlining its concerns that six federal agencies were still relying on information in the files of consumer reporting agencies to conduct remote knowledge-based identity verification. The report called for urgent change in light of the heightened risk—following the 2017 massive breach of data at Equifax—that an attacker could obtain and use an individual's PII to answer verification questions.

As the shift to digital transactions picks up speed, businesses have an urgent need to adopt new identity verification approaches suited to a world without secrets. In the financial services sector, for instance, the percentage of banking products consumers can open through digital channels has jumped from 43% to 76% over just the past two years—and about 90% of these can be opened from mobile devices.

However, while consumers appear increasingly willing to trust digital product and service providers, we have to ask ourselves: Is this trust fully warranted?

"GAO is making recommendations to six agencies to strengthen online identity verification processes...

"...until these agencies take steps to eliminate their use of knowledge-based verification, the individuals they serve will remain at increased risk of identity fraud."

U.S. Government Accountability Office
GAO-19-288, May 2019

[1] 2019 State of Digital Sales in Banking, FinTech Futures, April 2019

“Identity is the foundation of trust.”

Filip Verley,
Identity Innovator

And trust is the foundation of:

Global financial services like mobile banking,
Self-serve payments/money wires,
Virtual currency exchanges

Online marketplaces

Peer-to-peer services/sharing platforms

Transportation, travel and hospitality industries

Cryptocurrencies

Cloud-based data storage and management

and just about every new digital business anyone will ever dream up

Upping the upside—what works now

To fully realize the upside of living in the connected world, we have to be able to trust. Do the organizations we're digitally interacting with as consumers deserve our trust? Can our customers trust us? Not as completely as we'd like to think.

Like the government agencies whose risky identity verification methods were cited by the GAO, some businesses still rely on knowledge-based authentication. In the financial services industry, companies using such archaic methods risk noncompliance with know your customer (KYC) and anti-money-laundering (AML) regulations. And while other industries may not be under such heavy regulatory oversight, organizations that simply take a user's word on their identity without security measures, or the word of third-parties (that may also be doing ineffective verification), are engaging in risky business.

Of course, the precision needed for identity verification varies with context. We surely want organizations to take more care when they're involved with our money, livelihoods, healthcare, legal matters or sensitive information. But it probably matters less if we're scheduling a rideshare or booking a vacation rental.

Still, there's a general and growing expectation that the process of signing up for any service and purchasing any product should be secure as well as very fast and easy. Even some business lenders today are promising a decision "in less than three minutes."

Digital providers are constantly challenged with balancing the need for speed and ease against the need to minimize risk. Based on Mitek's experience working with thousands of companies in multiple industries across the globe, organizations successfully achieving that balance are generally following similar principles.

"The process of identity verification touches almost every industry, making identity an essential element in every transaction."

World Economic Forum, Jan 2018

"By 2022, digital businesses with great customer experience during identity corroboration will earn 20% more revenue than comparable businesses with poor customer experience."

Don't Treat Your Customers Like a Criminal, Gartner, April 2017

Many of the digital providers that are successfully meeting consumer expectations for speed, ease and safety have several characteristics in common. These include:

1. Emphasizing the two sharpest points of the verification triad

Identity verification (IDV) processes have traditionally looked for evidence in some combination of "something you have," "something you know" and "something you are." In fact, because they were easiest to implement with consumers, "something you know" passwords and question/answer sets became the predominant methods. But today, with the impossibility of keeping this information truly private, emphasis has shifted to the other two points of the verification triad.

Something you have

One thing many people—an estimated 79% of the world's population—have is a government-issued ID such as a driver's license or passport. With today's IDV technology, we can use this predominant method of proving identity in the physical world to create a reliable identity in the digital world. Consumers simply use another thing most of them have, a mobile phone, to snap and submit a picture of the ID, which is then analyzed by software to determine if it is authentic.

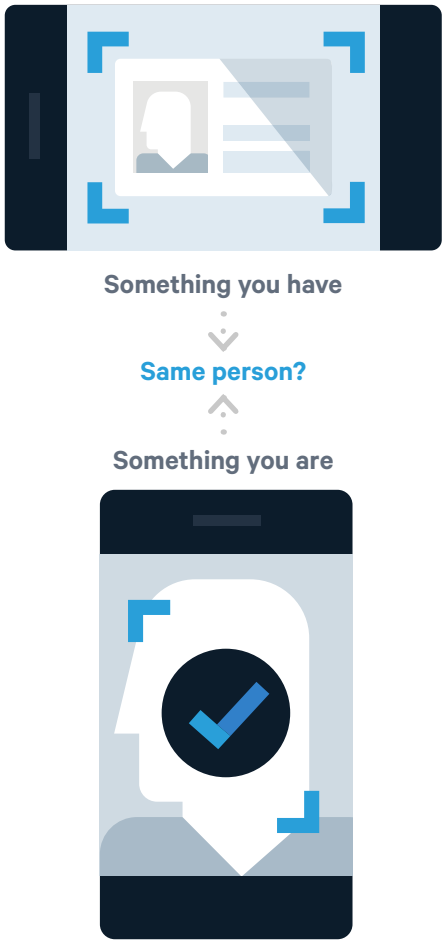
Something you are

When consumers also submit a selfie, IDV technology can compare it with the ID image to see if they match—verifying the individual in the selfie is the legitimate owner of the ID. This comparison is based on facial recognition, a form of physical biometrics that compares minute measurements of facial geometry to identify a person's unique combination of distinguishing characteristics.

Other forms of physical biometrics—predominantly fingerprint, but also iris and voice recognition—are being widely incorporated into mobile devices. Often, they're combined with a simple password for end-user access to the device and its installed apps. But biometric recognition doesn't actually prove that the individual setting up the biometric profile is who they claim to be. For that, there needs to be an additional step, such as the association of a government-issued ID with the initial biometric scan.

While physical biometrics are popular because they improve security while reducing friction for end-users, they also raise privacy concerns and can become less secure as the technology spreads. Criminal networks and hackers are drawn to big payoffs, and the more widely biometrics are deployed, the bigger the potential haul from hacking. Researchers have already proven fingerprint, iris and voice biometrics can be compromised, although it takes a high level of skill and effort.

Easily available artificial intelligence tools will further lower this bar. A New York University researcher[2], for instance, recently used machine learning to create a sort of "master key" fingerprint which enabled him to log into mobile devices and even home security systems.



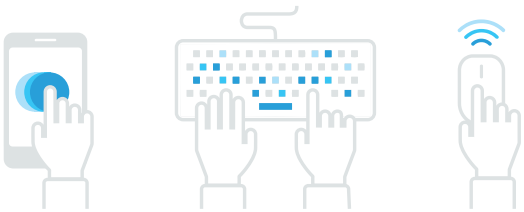
[2] Machine Learning Masters the Fingerprint to Fool Biometric System, NYU Tandon School of Engineering, Nov. 2018

Breaches of stored biometric data are still quite rare, but can be significantly more damaging than previous PII breaches. While consumers are routinely notified
of compromised information and warned to change passwords, physical characteristics can't be changed.

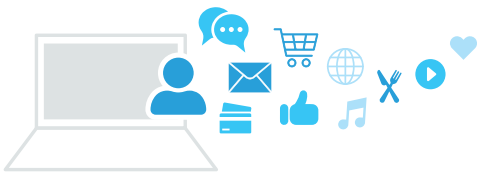
Breaches of biometric data could put us at risk in many new and unexpected ways, potentially for the rest of our lives. Organizations that fail to secure biometric data are therefore exposed to enormous legal risk.

Behavioral analysis is another form of biometrics technology, and while it offers potentially greater security than physical biometrics measures, it is raising additional concerns about privacy. Behavioral analysis identifies us through patterns in how we move on our digital devices (like pressing, swiping, scrolling, typing and moving a cursor) or what we do (like habitually visiting certain websites or frequently making certain online transactions). For the most part, sensors in phones and code on websites are picking up this information without our knowledge. That's good in the sense that it's a passive, completely unobtrusive IDV method, meaning there's zero friction for the end user. Perhaps not so good, we don't know what the profiles from behavioral biometrics and other data are saying about us and how they're being used for purposes beyond IDV.

Behavioral biometrics identify you by:



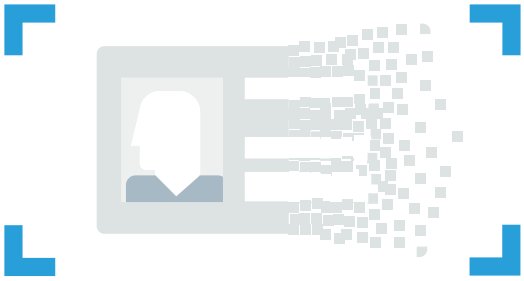
Your characteristic online gestures



Your habitual online places and activities

Instantly piece together a digital identity from shards of live-sourced data

Or, AI bots can swarm over an ID to find its flaws



2. Mobilizing an army of AI bots in an instant

To meet consumer expectations for security, speed and ease, digital providers are choosing IDV solutions that incorporate AI. It's the only way to perform massively complex verification tasks invisibly in the background, in an instant.

For example, determining that the snapped picture of a government-issued ID is an image of a legitimate, original and unaltered document involves an immense number of tiny, detailed checks, comparisons and measurements. Mitek Mobile Verify® does it in a few seconds by unleashing hundreds of AI bots to swarm over the image, each one performing a different task. Computer vision algorithms check the portrait on the ID to make sure it's a human face, examine image quality (very low and very high can both be red flags) and look for suspicious shadows indicative of photocopying or digital alteration. Machine learning algorithms examine font usage and consistency. Deep learning algorithms find subtle problems, such as slight irregularities appearing on or between certain letters. An additional level of machine learning then takes all the outputs from this army of AI bots, decides how much weight (relative importance) to give each point of evidence and answers the questions: Is this identity genuine? Does it belong to the applicant?

Behavioral biometrics involve similar levels of complexity. A Mitek partner for instance, continuously collects the digital footprints left by an individual's online activity and uses AI bots to piece together these shards of live-sourced data into a holistic, current view of that individual's identity.

The methods used by Mitek and and their partner analyze data across the physical and digital worlds, and allow for the fact that both are imperfect and always changing. Using AI to combine lots of different types of evidence enables nuanced adjustments to what's available or unavailable, clear or less clear in each individual case. AI bots can also learn as they see new consumer behavioral trends and new document counterfeit techniques. And additional bots can be brought in to perform new tasks, expanding the concentration of intelligence invisibly at work in the background during moments of identity verification.

3. Encompassing global diversity

Today, identity verification has to be global in scope. Not only are our individual spheres of interaction expanding, but a growing share of consumer and business transactions are moving onto global marketplaces and platforms that support cross-border delivery, payments, contract handling, insurance and finance.

The problem, of course, is that there's currently no international standard for physical ID documents or digital IDs (more on this in the next section). Until these emerge, IDV solution providers with a global reach are essential for cross-border identity verification.

For instance, to determine if the driver's license you snap and submit from your phone is a legitimate government-issued ID, Mitek Mobile Verify® matches the snapshot to one of thousands of document templates from around the world collected in its repository. It then compares the snapped image to the template at the levels of overall structure and minute detail, to ensure components like biographical information, signature block, portrait area, machine readable zone (MRZ) and barcode are exactly where they should be. Extracting information from these elements, the software also checks to make sure the ID data is internally consistent—for example, confirming that the data encoded into the MRZ and barcode match up with the biographical information.

4. Combining methods in flexible and innovative ways

Because both the physical and digital worlds are imperfect and changing, you need flexibly to implement multi-factor IDV tailored to different situations.

For instance, you may want to use a gradual verification method—which reduces onboarding abandonment rates—to design the sequence of steps in a specific way. Similarly, a waterfall process should follow your escalation rules to trigger automated requests for additional information and/or routing to a human verification expert.

You will also want flexibility to tailor what happens within each component of your IDV process. For example, you might be willing to accept black-and-white ID images in some cases, while in others you want to analyze color as a way of judging document fidelity. Maybe for some applications, you care only about the information on the back of the ID, but for others comparing front and back is critical. IDV should let you emphasize and denote specific components of the process as needed.

Across global markets, IDV also needs to accommodate cultural differences. Case in point: MoneyGram has found that in some parts of the world, most consumers are happy to start the onboarding process by snapping an image of their physical ID. They see it as a time-saving process that eliminates typing, since the online application form automatically populates with information extracted from the scanned image. In other parts of the world, however, consumers prefer to start onboarding with SMS code verification.

MoneyGram uses ID snapshots as a step-up check at the end of the process, and many customers who are asked to snap their ID like the idea that extra steps are being taken to protect them.

"By being innovative about IDV, I think we can take a friction-filled process and 'flip it on its head' so that instead of a hurdle to the customer experience we're trying to deliver, it becomes an enjoyable part of that experience."

Nash Ali, Head of Risk and Payments, MoneyGram International

Toward a better future of identity—what needs to change?

Solutions that work today for identity verification won't necessarily be enough for the future. By 2020, half of the world's population will be online—with the other half expected to be connected by 2025.[3] And every single one of these individuals will be affected by complex issues of digital identity.

As the World Economic Forum (WEF) has pointed out: "Our digital identities are increasingly embedded in everything we do in our daily lives...If we act widely today, digital identities can help transform the future for billions of individuals, all over the world, enabling them to access new economic, political and social opportunities, while enjoying digital safety, privacy and other human rights."[4]

How do we get to that future—the kind of future of identity most of us want? Here's Mitek's view of what lies ahead:

Everyone will have a digital identity providing a high level of assurance

There are two big problem clusters that need to be solved before everyone will have a high-assurance digital identity.

The first, disenfranchisement, is centered in the developing world's low-middle income economies, where it's estimated over a billion people have no formal proof, digital or physical, of their identity. Many countries have not historically had the means to register births or uniquely identify people already living within their borders. Global initiatives like the World Bank's Identity for Development (ID4D) are underway to change this, and technology will help. Similar to how mobile phones enable regions without telephone landlines to leapfrog into the modern age, inexpensive smart phones, image processing and biometrics should make it possible to overcome the lack of systems for physical credential distribution and jump right to digital IDs.

The second problem cluster, dependability, is a challenge for mature economies as well, including those with universal government digital ID programs (like Estonia) and those that have so far left the question of digital ID up to the private sector (like the U.S.). At both ends of this spectrum, and everywhere in-between, there are questions about whether consumers, businesses and government agencies can depend on the security of the processes used to issue, store and verify digital IDs.

Even Estonia's Smart-ID was breached through phishing attacks in 2019. This commercial app, which jumped into the void created by the 2014 discovery of vulnerabilities in the country's chip-embedded national ID card, is being widely adopted across the Baltic states. Meanwhile, some other national initiatives, including India's Aadhaar project, raise concern because they're based on a central database and single technology stack—a potential single-point-of-failure.

[3] UN Broadband Commission sets global broadband targets to bring online the world's 3.8 billion not connected to the Internet, ITU January 2018
[4] *Identity in a Digital World,* World Economic Forum, 2019

In addition to security issues, the dependability of a digital ID is affected by how many people are using it and what they can use it for. Global consulting firm McKinsey&Company has suggested that relatively low adoption rates so far for digital IDs in the UK, Germany and Austria may have to do with a "lack of advanced data sharing functionality" needed to support a wide range of use cases.[5] Even in India, where Aadhaar adoption is above 90%, citizens are unable to fully depend on this digital ID for the full range of transactions they need in digital life, since the range of applicable use cases is still limited.

The U.S., of course, is a mishmash, with consumers still having to establish their identities multiple times in multiple ways with nearly every digital product and service provider they interact with. Dependability of these digital IDs varies based on how well each of these commercial and government entities handles security and how willing they are to allow the identity credentials they issue to be used by other entities.

Cooperative ventures, such as the joint effort by Mastercard and Microsoft to develop "a single, reusable digital identity," aim to lead the way to greater unification and simplicity. Platforms like Apple Pay, Amazon PayPal and Facebook Libra are also vying to become a trusted authority for cloud-based identity-as-a-service. But growing concerns about the trustworthiness of big tech make it less likely they'll be allowed to assume this crucial responsibility. Perhaps public-private initiatives, like the ID2020 Alliance, will be more palatable. We might even see a cross-industry effort in conjunction with the relatively apolitical National Institute of Standards and Technology (NIST).

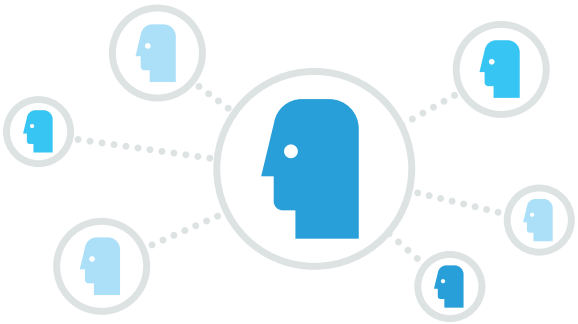
Global standards make digital identities workable across borders

The creation of international standards for exchange and verification of identity information will be a big step toward bridging the various identity credentials and requirements of different countries. The idea is to enable interoperability and transferal of trust by creating an umbrella standard that national standards can refer to and apply to their own requirements.

Globally, a variety of efforts aimed at this objective are underway by international organizations, such as the Decentralized Identity Foundation (DIF).

There's also a joint task force of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Even the extremely fragmented U.S., where states all issue their own driver's licenses, has recently taken a step toward standardization. Most state-issued licenses now comply with the REAL ID standards required for boarding federally regulated commercial aircraft.

We think there's a good chance international standards akin to those underlying the internet will eventually become widely adopted for digital identities. Over time, as countries continue to conduct their own experiments with various identity verification approaches, there will be convergence around a set of best practices. Increasing momentum for cooperation and joint-solution development is likely to occur even in the U.S., especially as businesses see their counterparts in other parts of the world reaping economic benefits from uniform digital ID programs.



Individuals will have visibility and control over how they're recognized online

While a frequent criticism of centralized national identity systems is that citizens have no visibility into the information compiled about them and how it is used, the same can be said for ultra-decentralized approaches.

In the U.S., for instance, identity technology is being embedded into layers of apps, programs and devices—and there is little or no regulatory restraint on how the providers of these components use our information. (One provider of an anti-spam-call app actually repurposed data from its users for an identity verification business it was running as a sideline.) Often there's a request for

[5] Digital Identification: A Key to Inclusive Growth, McKinsey Global Institute, Jan 2019

permission to tap our contacts, location and other data, even though the information is not necessary for the function. Opting out usually means we can't use the function at all.

There's also the issue that as behavioral biometrics spread, the very notion of identity may be evolving beyond what we can comprehend, much less control. Companies are gathering up our digital footprints to distill highly dense profiles representing who we are. (One IDV company claims it can verify 70-80% of consumers from just phone numbers, which "opens the door to a treasure trove of information available to probabilistically link" to other forms of personal data.)

"Digital identities have evolved. They are no longer simple and isolated pieces of information about individuals, but complex webs, crossing the internet... the sum total of the growing and evolving mass of information about us, our profiles and the history of our activities online...[and] inferences made about us, based on this mass of information, which become new data points.

"The result for individuals is a decreasing understanding of or control over how they are represented online. With that digital representation determining so much of how we live our lives, these changes add up to a rewriting of the social contract, and we are barely even aware of it."

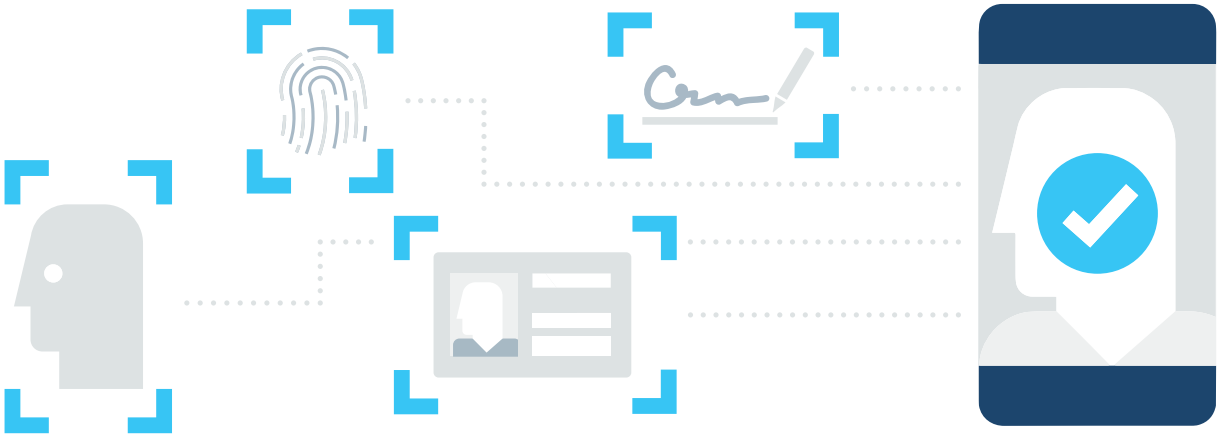
Identity in a Digital World, World Economic Forum, 2019

Many companies are analyzing similar data to make inferences about us. Advanced analytics can even predict behaviors we've never shown before but are likely to, given statistical similarities with other people. Such inferences and predictions are also becoming part of our digital identity. Other companies are developing "continuous identity verification" processes from the constant data streaming in from our digital activity. The advantage is that these identities are always up to date. The disadvantage is that our identities are constantly changing without our knowledge, and the process could open the door to unwelcome surveillance.

Growing concern around the world for more transparency into digital identity data and processes is leading to more regulation, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (which, when it goes into effect in 2020, will be first to require disclosure of behavioral biometrics). It's also leading to technology innovations that facilitate identity verification while limiting disclosure of personal information unrelated to the transaction at hand.

More generally, we're seeing the emergence of the self-sovereign identity movement, which aims to give consumers online tools for managing their own lifelong, verifiable digital IDs, dispensing them as they choose and controlling the flow of identity-related information to product and service providers. Some of these efforts are being developed around blockchain-like hyper-ledger technology.

In our view, there's absolutely no doubt that more transparent approaches to digital identities are needed—and that they are the future.



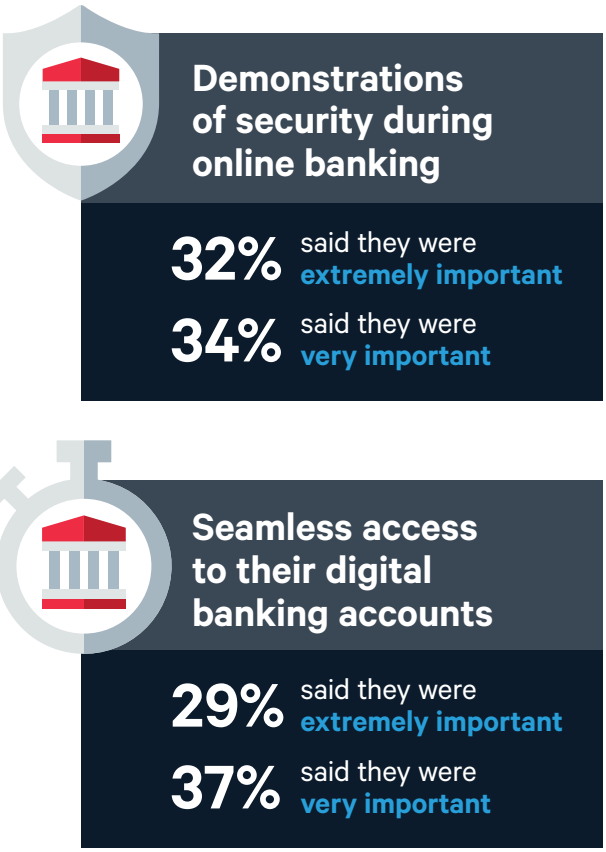
We've achieved a better balance of convenience and risk

Consumers will ultimately determine whether or not this statement comes true, but we're definitely starting to see a shift from a convenience-tops-everything attitude to a more measured, balanced approach.

Evidence of this shift can be seen in the Experian 2019 Global Identity and Fraud Report. Consumers were asked about their expectations on digital banking as shown in the graphs to the right.

So, consumers clearly want both—but especially for higher risk financial transactions or where PII disclosure is involved, they appear ready to put up with a little friction for better protection.

Mitek is seeing the same thing in our work with companies across multiple industries, all over the world. As consumers become savvier about digital transactions and more aware of what is at stake, the right balance between security and ease of use will naturally be found.



All together now...

Despite plenty of problems remaining to be solved, **we think the future of identity is looking good.**

Right now, we all need to think about what we want and work together to make it real. Because one thing's for sure: Identity is going to affect just about everything that happens in our businesses and lives going forward.

Tell us what you think.
Share your observations, ideas and concerns here.

Mitek