WORLD
ECONOMIC
FORUM

Community Paper

Reimagining Digital Identity:
A Strategic Imperative

January 2020

This community paper has been published by the World Economic Forum as a contribution to a
project, insight area or interaction. The findings, interpretations and conclusions expressed herein
are a result of a collaborative process facilitated and endorsed by the World Economic Forum,
but whose results do not necessarily represent the views of the World Economic Forum, nor the
entirety of its Members, Partners or other stakeholders.

Contents

Reimagining Digital Identity: A Strategic Imperative

The world today is exploding with digital connectivity. People, organizations and internet-enabled devices of all kinds are all interacting with one another digitally. Users have come to expect the seamless, fast, convenient and personalized experiences that life online has brought, and their expectations are only set to soar. New opportunities emerge as digital disruptions take place across every sector, from the delivery of telemedicine and digital prescriptions, to the gig economy and the development of an increasingly liquid workforce, to digital banking via devices in the internet of things (IoT), to the digital transformation of supply chains and the provision of government services.

Advances in technology are profoundly changing the ways in which organizations and individuals interact with one another. Just a few years ago, few could imagine entering a stranger's car or inviting a stranger met online into the home to help with household chores or care for loved ones. Today, millions of transactions like these take place daily.

However, difficulties with asserting identity in a digital world fuel uncertainty and a lack of trust that limits the adoption of services offered online, however valuable they might be. To cite but one negative experience: today a family using a digital platform to contract a caregiver for an elderly relative is likely to encounter difficulty in validating the caregiver's identity and the authenticity of their qualifications. It may be impossible to confirm that the caregiver is the same person who provided

their personal information on the platform. The digital revolution has also brought with it new forms of fraud, identity theft and misuse or abuse of personal data. Cybersecurity incidents have become a pervasive and seemingly permanent threat to personal data privacy, threatening the foundations of trust on which society functions.

To reduce such risks and increase user confidence, organizations typically add checkpoints intended to identify, verify and reverify individuals. These mechanisms often add unwanted friction and also entail sets of steps that users must repeat across multiple organizations with which they interact, filling in the same information again and again. Moreover, these mechanisms are often limited in their effectiveness in reducing the risks of identity fraud while raising justified privacy concerns.

> **Identity**: Who a person or organization fundamentally is – a combination of attributes, beliefs, personal/organizational history and behaviour that together constitute a holistic definition of the individual or organizational self.
>
> **Identification**: The act of verifying identity; proving who people and organizations say they are.

REIMAGINING DIGITAL IDENTITY

	FROM		TO
DESIGN	Siloed customer interactions; repeated digital identity processes in each domain and organization	→	A collaborative ecosystem that unifies digital identity across business units and multiple sectors
OWNERSHIP	A business unit or company that "owns" the identity of its users, causing fragmentation and poor experiences	→	Users who own their own digital identity; business units and companies that collaborate, eliminating silos and creating seamless user experiences
REPUTATION	Lack of trust in validating digital transactions due to identity fraud and security issues	→	High degree of trust, reliability, and security across the value chain in digital transactions based on trusted digital identity
VALUE	Limited opportunity to meaningfully use digital identity due to fragmentation and lack of interoperability	→	High level of value made possible through interoperability across domains and use cases, helping to create new ecosystems and business models
USER CENTRICITY	Negative experiences and lack of user control due to the prioritization of business functions over holistic user value and experiences	→	User empowerment through user control of what data they share, improving their experiences across their digital context

These issues are increasingly salient as digital approaches become the norm. The heart of the problem is that individuals and organizations must be able to trust that others are who they claim to be in every online transaction. For that, they need a more useful, valuable, trusted, private and secure way to reliably identify themselves and the entities related to them in the online world. In short, organizations need to reimagine and transform the way digital identities are managed today.

> As the amount of digital interactions is increasing, users are demanding connected, seamless experiences that are personalized, fast and trustworthy. Digital Identity is indispensable to provide users with the means to establish reliable digital interactions across services. As initiator of a Digital Identity coalition, ING believes user-centric digital identity is strategic and collaborative: customers have agency over their data and interactions while companies can make personalized, connected and secure customer experiences their new value proposition.

Bernard Lhermitte, Chief Operating Officer, ING Luxembourg

Both regulatory and social pressures contribute to the need to reconceive digital identity. While individuals might choose to share more of their data in exchange for specific benefits, regulations are becoming more stringent to protect against the rise in the misuse of identity data. Against the backdrop of technological advancement, users themselves and regulatory bodies tasked with protecting them are both demanding that users be empowered with greater control over the management of their data. Organizations must embrace the culture of user-centricity if they are to gain and maintain user trust and remain competitive.

This paper explores the urgent need for businesses to change the ways in which they think about and manage identity in the evolving realm of online commerce and beyond, and how and why this demands top priority attention from business leaders.

The urgency for change – an identity status quo not fit for digital life

In a globalized economy, companies operate in highly competitive landscapes where many struggle to respond to the disruptions brought by new technologies and new market players. With so much that needs to change to reap the benefits of the digital economy, why does identity matter? Why must it be a top priority?

Every organization today already has some identity capabilities in place. While these may not always be

perceived as broken, they have hardly changed for decades and most still rely on manual (unautomated), paper-based processes. The reason why better digital identity matters is that the current way of operating is not fit for purpose in the ever-developing digital world.

Today, these identity systems are complex, siloed, different one from another and relatively unautomated, even within a single organization. Consumers desire seamless, convenient online experiences with minimal friction. Yet today they must interact with an unprecedented number of service providers, each of which requires them to continually reassert and reverify repeatedly their identity. The digital identity status quo fails to meet consumer expectations. The current models are ripe for disruption and positive change.

> Our digital world is disrupting traditional industry boundaries and pushing out the frontiers of how we deliver excellent digital services and user experiences. Digital identity sits at the centre of how we provide that seamless and frictionless experience for users. The opportunities to grow in this digital world will be determined by how well companies put user-centricity, digital identity and user consent at the centre of their go-to-market strategies

Michael Bültmann, Managing Director, HERE Technologies Berlin

Users can easily cite numerous examples from their daily lives of the inadequacy of prevalent digital identity models. To apply for a job, prospective employees typically need to provide proof of their educational credentials, which may take potential employers weeks to verify. Job seekers are likely to have to repeat this process numerous times with multiple potential employers. Similarly, setting up a new company involves governmental entities confirming multiple documents; the average time this process takes ranges from one to six months.[1] Moreover, the process is typically manual. The opportunity costs entailed by delays in application processing, repeated validation of the same set of information and manual, paper-based processes are significant on both sides.

Businesses must understand that they will be required to redesign and rethink their relationships with their customers to remain competitive in a changing business landscape. As user expectations change regarding how digital identity is managed, organizations must reposition themselves regarding how they interact with their customers.
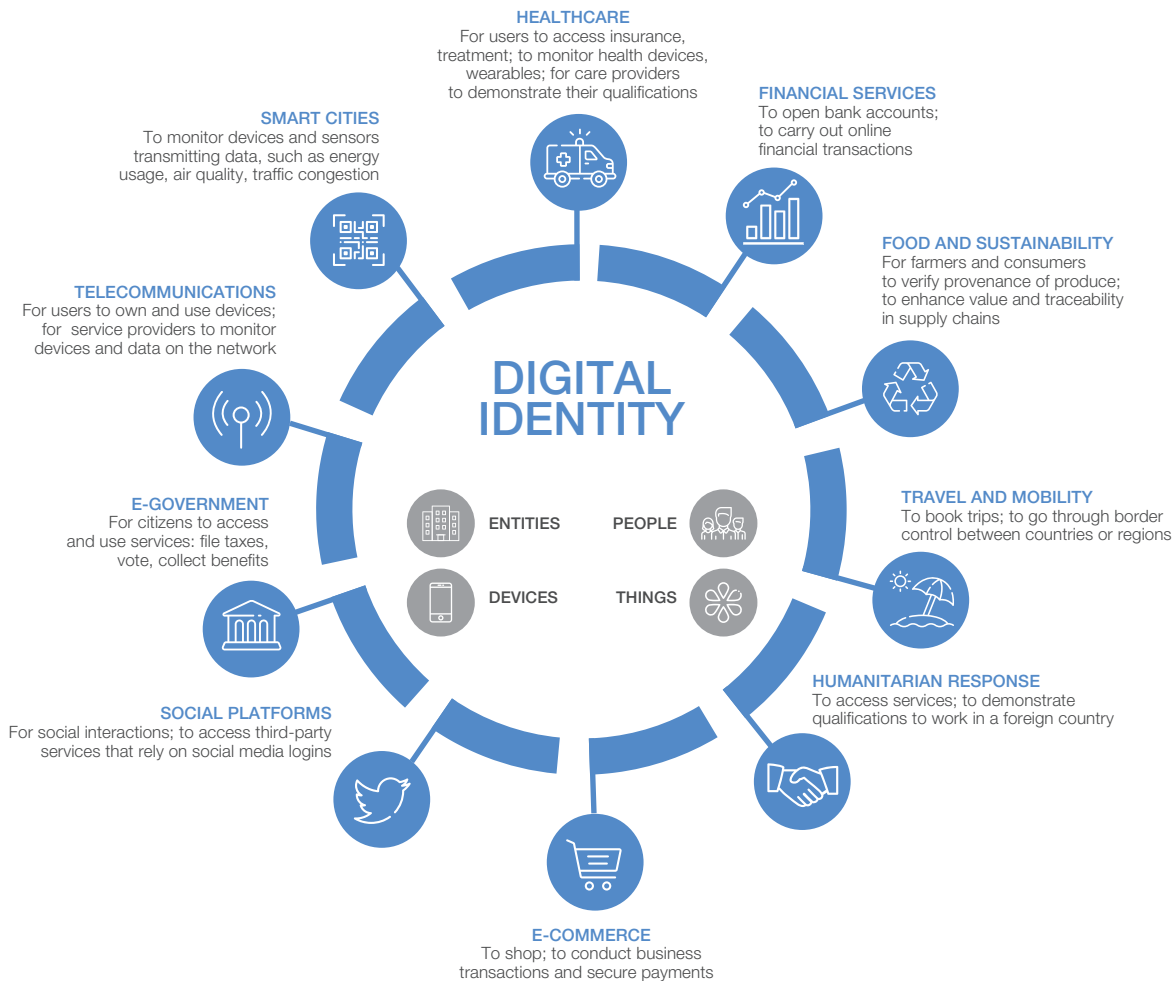
And the time to act is *now*. The digital identity revolution has already begun.

The power of collaboration across companies and industries

Society requires trust to function. In a world that relies increasingly on the storage of information in digital form, digital identity constitutes an essential component of trust. In order to establish trust for any online transaction, all parties must know the identity of the people and entities with whom they are interacting and must have confidence that they really are who they claim to be – and that they are still the same people or entities they have claimed to be previously. Specifically, all parties must know that the sources of credentials used to assert identity claims are valid and reliable, and that those claims themselves are verifiable.

Individuals today use their digital identity in every aspect of life, with every service provider and authority with whom they interact. Yet today, most businesses build and maintain their own siloed identity capabilities centred on their own needs to conduct business, meet regulatory requirements, compete in the marketplace, and offer and deliver products and services based on the accepted norm that "owning" the users' identity will provide competitive advantage.

HEALTHCARE
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications

FINANCIAL SERVICES
To open bank accounts; to carry out online financial transactions

SMART CITIES
To monitor devices and sensors transmitting data, such as energy usage, air quality, traffic congestion

FOOD AND SUSTAINABILITY
For farmers and consumers to verify provenance of produce; to enhance value and traceability in supply chains

TELECOMMUNICATIONS
For users to own and use devices; for service providers to monitor devices and data on the network

DIGITAL IDENTITY

ENTITIES   PEOPLE

DEVICES   THINGS

TRAVEL AND MOBILITY
To book trips; to go through border control between countries or regions

E-GOVERNMENT
For citizens to access and use services: file taxes, vote, collect benefits

HUMANITARIAN RESPONSE
To access services; to demonstrate qualifications to work in a foreign country

SOCIAL PLATFORMS
For social interactions; to access third-party services that rely on social media logins

E-COMMERCE
To shop; to conduct business transactions and secure payments

From healthcare to banking to paying taxes, the repetition of the process of providing identity credentials online is not only frustrating for users but also costly and inefficient for organizations. If organizations could choose to collaborate and share their identity capabilities, society as a whole would benefit. Organizations would benefit from reducing costs and inefficiencies by improving customer experiences, enabling them to focus on building new services founded on trusted digital identity. Collaboration across the public and private sectors offers the potential to create new models of secure, useful digital identity based on user agency and user choice – models that leave no one out and leave no one behind.

Globally, this is already taking place across multiple sectors. Several banking consortiums, for example, have already started to collaborate in building new shared digital identity capabilities to not only enable their customers to verify their identity but also to take advantage of the trust created in other areas of their lives, such as renting an apartment or setting up a new mobile phone.

Example: The **itsme** app in Belgium can be used with more than 100 partners across multiple sectors, including financial services, telecoms, public services and healthcare. Belgium Mobile ID, the consortium that runs itsme, has been able to establish the system-wide adoption by fostering inter- and intra-sector collaborations and ensuring that security and privacy are its top priorities. [2]

The benefits to businesses

For businesses, a trusted identity can generate new markets and lines of business, better customer experiences and higher-quality data, as well as provide protection against fraud while protecting consumer privacy. For both producers and consumers, a good digital identity system can open up the world of online commerce to new jobs, supply chains, partnerships, products, services and experiences.

For example, if patients and their medical devices can be securely identified and authenticated, and medical data accessed safely and ethically online, good digital identity could lay the foundations for a new wave of medical innovation. Secure identity tracking of products and goods across global supply chains could establish the provenance of products and boost consumer confidence in ethical sourcing, enhancing producers' income and helping in the fight against such abuses as counterfeiting and child labour. Seamless verification of people and connected devices is essential to delivering individualized and integrated services in "smart cities".

The push to enable seamless travel is a prime example of how the need for change often originates from the intersection of a critical business priority with changing industry trends. One promising recent initiative in this area is the Known Traveller Digital Identity (www.ktdi.org) programme. KTDI not only reinvents the customer experience but also enables a systemic change and the creation of new value for businesses and all other stakeholders involved.

At the same time, they want their digital interactions to be reliable, safe and respectful of their personal freedoms, and especially of their privacy. Consumers expect control and autonomy in deciding which data they share during any interaction, with whom, and for how long. Yet while hyperpersonalization can enable businesses to reap significant benefits, if it is not implemented by empowering users, they may experience it as a violation of their privacy.

New business models are emerging across all sectors. An estimated 70% of new value created in the economy over the next decade is expected to be mediated by digitally enabled platforms, such as those that already enable ride sharing, property rentals and freelance work in the "gig economy."[6] Such new models increase workforce fluidity, which presents new liabilities and risks for businesses in hiring and paying the people who work for them. It becomes increasingly challenging and essential for businesses to be able to verify the identity of all their hires, in ways that are equally secure and convenient on both sides.

✈ Reimagining the mobility ecosystem: Known Traveller Digital Identity

As global air travel is set to increase by more than 50% by 2030, governments, airports and airlines need to be able to process passengers more quickly and safely in places where space and resources are limited.[3] Today, many of the "pain points" in air travel result from the need to establish trust in passenger identity. To support and reap the benefits from the projected growth in air travel, digital identity must be reimagined collaboratively by all parties in the air travel ecosystem. The incentives for improvement are substantial. Passengers will be afforded more seamless and personalized passage through check-in, security, customs and immigration. Border security personnel will be enabled to focus key resources on areas of risk rather than wasting them on trusted travellers. Governments will be able to leverage trusted traveller identity as a starting point for redeploying it for access to other services in other sectors. Airlines will be able to board passengers more quickly and offer them more personalized services. Airports will also be able to support greater flight volumes. The wider travel and

⚛ Tackling new vulnerabilities in the sharing/ platform economy

As businesses that offer services via online platforms become increasingly popular, ensuring trust in all actors involved is of paramount importance. Ensuring the safety of passengers in ride-sharing cars, assessing food hygiene in food-delivery networks, or checking the legitimacy and credentials of doctors across hospital networks becomes not only more important but also more complex. Secure digital identity can create trust in the sharing economy, reducing fraud and enabling business to offer new high-value services.

The internet of things challenges businesses too, with burgeoning expectations not only from consumers but also from regulators for the protection of user data privacy. In the realm of digital identity, manufacturers and consumers inevitably share responsibility for how their things connect, recognize and trust one another, and share information. Smart companies will choose to view their interests as convergent with those of both consumers and regulatory bodies.

hospitality sectors will, in turn, benefit from access to trusted identity data provided directly by travellers themselves, by offering more personalized services. The right set of incentives exists for every actor in the ecosystem.
If built right, a new regime of trusted digital identity could help businesses win and maintain competitive advantage and enhance brand loyalty. Research indicates, for instance, that Starbucks has recently incorporated artificial intelligence and hyperpersonalization into its digital identity strategy to understand users' behaviour while enhancing their retail experience, increasing the company's marketing effectiveness by 300%.[4] By 2023, initiatives like this will help reduce customer churn by 40% and increase lifetime value by 25%.[5]

Consumers today increasingly expect companies to deliver highly personalized services and experiences tailored to their individual characteristics, behaviours and preferences.

> "
> To truly make the digital world work for all, we must rethink traditional notions of digital identity and break down artificial barriers. We need a new model that starts with the commitment to the fundamental individual right – "I own my identity and I control my identity data." And we need businesses, governments, NGOs and others to forge partnerships and invest resources in support of a common framework, principles and standards.
> "

Ajay Bhalla, President, Cyber & Intelligence, Mastercard

Opportunities to Realize New Value, Now

Collaborative innovations in digital identity among industries and between sectors is not only inevitable in the future: they are already happening, generating value for businesses and customers and helping businesses to realize efficiencies and growth.

Reducing friction in connected health	Gaining efficiency and certainty in financial services
Across the healthcare ecosystem in the United States, according to conservative estimates, more than $2.1 billion is spent annually by hospitals, doctors and health insurers to maintain provider data. The Synaptic Health Alliance brings together insurers and diagnostic services providers to solve problems in verifying physicians' public information. The consortium was founded to explore the possibilities for new technologies to enhance authentication, resulting at the same time in the creation of a new forum for identifying new use cases for collaboration. [7]	In Colombia, three of the major banks are driving a new identity verification platform named SoyYo ("I am I"). An initial pilot study is looking to streamline the onboarding of users to multiple services, increase user convenience by consolidation of services in a single app, while at the same time reducing costs for the participating companies. The collaborating banks have received clearance from the Colombian regulatory body that oversees marketplace competition. New business models are thus being created to reduce friction while increasing the trust in customer interactions across sectors.

Increasing customer experiences through connected cars	Driving trust and interoperability in the gig economy
The rapid evolution of connected vehicles presents significant challenges for advancing reliable transactions that require a trusted digital identity for service delivery. The location platform HERE showcases innovative technology that builds explicitly on consumer trust – a prerequisite for autonomous driving solutions. Co-owned by a consortium of automotive companies, and part of the digital identity alliance Verimi, HERE offers user-led, end-to-end location services "for devices, people, and things".[8]	To help ensure trust and safety for female employees in India, Accenture has partnered with local background checking service company Betterplace to pilot a blockchain-based solution called Safedrive. First, the data of the driver is shared with the employee prior to the journey to give visibility of the their identity. When picking up an employee, the driver takes a photo of themselves, which is authenticated on the blockchain and matched with their validated background data. Once confirmed, the employee is then notified. By empowering drivers to authenticate their identity from their smartphone device, Accenture allows their female workforce to gain a higher level of assurance for their journey, increasing female workforce participation." [9]

New value opportunities across industries and sectors

1. **Financial services**
   Several use cases in the financial services sector reveal how amenable the industry is to collaborative initiatives that seek to create a better digital identity model. Financial services businesses are, in general, strongly regulated and consequently, one of the most trusted organizations for consumers. The sector also bears significant costs associated with establishing and maintaining trust in identity, from identification and verification capabilities (ID&V) to know-your-customer/client (KYC) utilities to fraud detection and data-protection solutions.

   How can digital identity generate value?
   A collaborative bank-led digital identity, such as BankID, can help organizations reduce costs by using pre-verified information, potentially reducing the $60 million an average bank spends on KYC each year.[10]

   Example: **Sweden's BankID** is one of the earliest adopters in the world of a digital identity solution that distributes and reduces the costs of verification. A cross-industry

verification system encompassing the private and public sectors, BankID was initially set up by the country's major banks. The system now boasts nearly 8 million users (nearly 100% of the market), enabling them to complete a variety of transactions.[11] Similarly, **LuxTrust** is a consortium initiated by the main banks and the government of Luxembourg – to authenticate users by verifying their identity to complete and sign secure transactions online across banks, postal services, and other national services.[12]

2. **Mobility**
   Both the growth of international air travel and the advent of increasingly connected cars generate multiple interactions in which establishing and maintaining a trusted identity is essential but cumbersome. After a typical international flight, for example, travellers may have to provide proof of identity as many as eight times in a row, needlessly raising costs for organizations and impacting the overall user experience.

   How can digital identity generate value? Digital identity solutions can enable user-led passport-free travel. For the aviation sector worldwide, this system-changing approach could save $150 billion across the aviation sector worldwide, while creating up to $305 billion worth of value for the industry through increased profitability. [13]

Example: **Clear Digital Identity** is a utility that not only enables users nearly frictionless boarding at airports and train stations but also faster entrance at sports stadiums and even one-tap payment at stadium concessions.

3. Healthcare
Seamless, secure sharing of medical information between organizations is a precondition for efficiency in emerging connected healthcare systems and could offer potential benefits exceeding, in the US, 1% of GDP – equivalent to $205 billion.[14] For healthcare players, a patient-led connected health experience offers more targeted and sustainable treatments even at home, reducing the cost of processing health records and of hospitalization, and opening the door to truly personalized, targeted healthcare.

How can digital Identity generate value? Savings from seamless and secure sharing of medical information could equal 50% of US GDP according to McKinsey.[15]

Example: **Estonia's digital identity system** has increased the efficient use and accuracy of the country's health data, reduced administrative burdens and facilitated new services, with 99% of prescriptions transacted electronically.[16] With advances in technology and precision medicine sure to spill over into other sectors, ensuring trust is essential to improving existing processes and unlocking value in the health sector.

4. The gig/sharing economy
Emergent digital technologies and peer-to-peer networks are creating new marketplaces and business models predicated on sharing and collaboration rather than ownership and siloed data. With 50% of US workers potentially becoming freelancers by 2027 and the sharing economy expected to grow to $335 billion in revenues by 2025, there is a huge opportunity for businesses to capitalize on this growing sector.[17] [18] However, problems remain in validating the identity of actors and users throughout the marketplace. Good digital identity will build confidence and trust, improving the economic potential for businesses of many kinds.

How can digital Identity generate value? The key to growth in gig/sharing economy is creating higher levels of trust, which leads to repeat selling and user confidence. With 61% of users stating that they will not trust other parties in a peer-to-peer transaction, good digital identity will enable the creation of new marketplaces and business models based on trusted interactions, and through them, new revenue streams.[19]

Example: Just 26.2% of sharing-economy platforms currently require new users to verify their identities by submitting identification documents online.[20] These digital platforms, such as for car sharing, apartment exchange or food delivery, all require trust for consumers to undertake transactions. Providing secure solutions to ensure that authentic trust is embedded in the relationship improves the user experience, leading to increased confidence and higher economic value.

> "
> Schiphol's vision is to implement a seamless passenger journey throughout the airport. Addressing digital identity collaboratively enables all partners, airlines and government to take the step towards seamless travel, while enhancing overall security and driving value for each participant. Digital identity reduces the required passenger actions to a minimum – even allowing them to take place before arriving at the airport – and airport partners obtain efficiencies by adopting a more "information-based" approach and performing necessary passenger checks earlier in the process.
> "

Dick Benschop, Chief Executive Officer of Royal Schiphol Group

The Risks of Not Getting Digital Identity Right

Reliable digital identity enables users to always know who has access to their data, enables organizations to access verified information and limits the risks of litigation and new legislative oversight. The risks of failing to get digital identity right are significant. Failure to comply with data privacy standards and security regulations can result in hefty fines – £183 million for British Airways, equivalent to 1.5% of its worldwide turnover and 10% of its profit in 2017.[21]

Getting identity wrong can lead to escalation of current market challenges across multiple domains:

- **Proliferation of identities**: For millions of people, to have a digital identity means to cope with proliferating identities, which can feel overwhelming. Businesses that exacerbate online identity fragmentation endanger user loyalty as well as the significant investments they have made in their identity systems. The more identity capabilities and services there are, the more difficult it is to gain market share, adoption and trust.
- **Insufficient user control**: Good digital identities offer users choice in determining how their identity data can be used. Inconsiderate customer data use can cause irreparable reputational damage.
- **Poor user experience:** Negative experiences lead for consumers to active avoidance and for businesses to diminished reputation and negative media attention, all resulting in reduced revenues. Some 70% of online shopping carts are currently abandoned before purchase is completed, translating to a $4 trillion loss in potential revenue globally.[22]

- **Trust and the internet of things**: Good digital identity also needs to consider interactions and transactions using IoT devices. With the exponential growth in IoT, the need for robust mechanisms to authenticate the identity of each device and verify the entities accountable for transactions in which it is involved are critical to preventing fraud and ensuring trust.

> "
> Digital identity is essential to the growth and viability of our digital economy, and fundamental to every organization, across every sector. It enables organizations to build trust with their customers, streamline and secure their operations. To succeed, the reimagining of digital identity is needed. Collaboration in digital identity across sectors and organizations is crucial to foster growth and deliver better business outcomes in the digital world.
> "

Paul Daugherty, Chief Technology & Innovation Officer, Accenture

The threats to success are significant for businesses as they look to improve user experiences and build and maintain brand loyalty:

Trust
Organizations offering digital services must facilitate trust in the total digital environment or risk losing consumer confidence in their brands. Already, lack of trust costs global brands $2.5 trillion annually as users desert them for competitors. [23]

Security and compliance
The massive volume of personal data collected by organizations creates an ever-growing attack surface. The more identity data organizations collect, the greater the investment required to protect this data – while the true costs of regulatory non-compliance may be as much as 2.71 times higher. [24]

Fraud
Consumers already maintain, on average, 92 online accounts – a number projected to surpass 200 by 2020. [25] The costs of identity authentication and fraud redress are projected to reach $28 billion by 2023. [26] Organizations that fail to keep up with changing expectations and merely contribute to the accumulation of redundant digital identity information also increase systemic risks of fraud.

User confidence

Consumers want and expect convenience and security in equal measure. Today, 57% of customers say they are uncomfortable with how companies use their personal data. The lack of consumer data confidence leads to a decrease in trust and revenue. Companies that fail to ensure trust in transactions can only exacerbate declining consumer confidence. [27]

New business threats

Large technology companies are entering new markets, blurring industry boundaries and disintermediating customers from traditional relationships with companies. These technology companies and other disruptors are well-placed to drive value from digital identity and control user experiences. To succeed in this competitive landscape, traditional companies across multiple industries will benefit from joining collaborative systems that put consumers in control of their own identities.
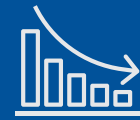
Limiting growth

With businesses losing up to 30% of potential revenue because of inefficiencies in user journeys and the lack of digital identity interoperability, the lack of a cohesive and secure digital identity strategy within corporations and across entire industries to reduce siloing blocks potential growth.[28]

One crucial element for effectively confronting all these threats is innovative collaboration, within lines of business, within industries and between the public and private sectors. Perhaps most important is for companies to reimagine their online users themselves as potential collaborators in reinventing how organizations construct and manage digital identity.

Next Steps for Leadership: Achieving Business Results

Collaborative, user-centric digital identity is key to creating new business value. In today's continually evolving interconnected digital world, a window of opportunity is open to take advantage of fast-changing technology to fulfil and even exceed rising user expectations. Companies need to begin *now* to address and manage digital identity differently, to get it right.

The digital world relies so heavily on currently prevalent methods of verifying digital identity that the challenges of transforming them based on new industry-wide, let alone cross-sector, collaborative models may seem daunting.

Leaders need to consider the following key questions to launch themselves on the journey to better digital identity:

1. **To achieve strategic clarity**: As technology disrupts global, regional and industry-wide landscapes, organizations need to redefine digital identity. How does digital identity form part of the user's experience in connecting to a company? How does digital identity align with a company's broader business strategy, help to uncover new value in the business's domain, mitigate user and business risks and foster long-term competitiveness?
2. **To design for users**: True user-centricity is the indispensable foundation of positive user experiences of digital identity. Does design for the digital identity of people, organizations and things put users at the centre? Is digital identity designed with incentives that foster interoperability?
3. **To establish ownership**: Current solutions to the problems posed by digital identity fragment users' identity and compromise their experience. Businesses must establish clear ownership of their digital identity

strategy, beginning by exposing silos within the company itself before addressing identity silos within and across sectors. Who is accountable for digital identity in top management?
4. **To lead systemic change**: As consumers shift from being customers of a business to customers within an ecosystem, businesses must move beyond the deep-rooted attitude of "owning" the individual user's digital identity. How does an organization ensure that a holistic, user-centric, collaborative digital identity is engrained in all its processes, including choice of partners and decision-making?
5. **To foster collaboration**: Organizational and sectoral actors must break down barriers among them to create better standards for digital identity, more seamless user experiences and, ultimately, more unified digital ecosystems. Who are the ideal collaborative partners for reducing friction and creating secure and convenient online experiences, and what are the needed trust frameworks, rules and tools of collaboration?
6. **To embed effective controls**: Protecting people and their information is essential to encouraging the adoption and maintenance of trusted digital identity systems. What safeguards are built into an organization's processes to ensure that risks to agency, choice, security and trust are transparent and manageable?

Where should leaders in the C-suite start?

C-suite leaders realizing the strategic importance of digital identity can take a four-step approach to start realizing the fullest potential value from good digital identity.

1	2	3	4
Assess	**Identify new value**	**Design**	**Build**
Assess the organization's situation regarding digital identity. The tool **Digital Identity: A Maturity Model** (see appendix) shows how strategic digital identity is represented in a company and highlights gaps that may prevent progress towards a networked model, which is where value can be created from digital identity.	To start evolving the organization's approach to digital identity and customer relationships, understand where new value can be captured. Highlight high-impact use cases that demonstrate the benefits of improved digital identity, including the creation of new value pools and gains in efficiency.	Reimagining digital identity means redesigning the ownership of identity within the organization and establishing new strategic partnerships to unlock value. Using the tool **Digital Identity: A Design Framework** for Digital Transformation Leaders (see appendix), businesses can understand the key questions to answer, technology choices available and holistic ownership of identity beyond mere identity management.	The maturity model and design framework highlight existing gaps and blocks that may inhibit the building of user-centric digital identity ecosystems. Create a roadmap focused on achieving the highest value and closing the biggest gaps by adapting the organization and fostering the strategic partnerships that will make user-centric digital identity an engine for growth.

Winning online businesses will be those that foster the most trusted relationships with their customers. To do so, companies will need to enable customers' direct, continuous access to their own data to allow where and when it used. This core principle of user-centricity will prove to be a key competitive differentiator that guarantees the realization of greater economic potential.

"

We want everyone to thrive in the digital world – no one should be left behind. That means educating everyone on how to keep themselves and their data safe online, which is something that we at Barclays are very passionate about. But it also means ensuring universal access to a safe, secure and easy-to-use digital identity, so that everyone can confidently unlock the benefits of the digital economy.

"

Jes Staley, Group Chief Executive Officer, Barclays

Solutions that support digital identity that are fit for purpose, inclusive, useful, secure and founded on offering user choice will benefit individuals as consumers by providing them with convenience, privacy, inclusion, security, agency and autonomy in all kinds of their online transactions. [31] These values can be realized through enterprise-level solutions but also, and perhaps even more significantly, through cross-enterprise, cross-industry and cross-sector collaborations. Moreover, businesses and entire industries and other organizations that support these values will further benefit individuals, their national community and global society by advancing an economy that is more inclusive, equitable and stable for all.

Acknowledgments

Appendices

Digital Identity: A Maturity Model

	1. Unaware	2. IT-driven	3. Fragmented	4. Pervasive	5. Networked
Business strategy and business model	– Businesses do not consider customer data and identities in making strategic decisions or in developing service models and product designs.	– Businesses recognise the importance of customer data but they do not consider it part of the broader business strategy. – A specific IT function, such as security, owns customer data.	– Businesses seek to build a single view of the customer. – Businesses use data ad hoc to inform strategy and monetize/use it as an asset. – Departments collaborate in basic ways.	– The industry/sector incorporates digital identity as a core element into business models and service design. – Standardization and mutual acceptance are established within and between industries.	– A good data strategy is mutually accepted across industry sectors and regions. – Strong webs of trust are established.
Customer interactions and relationships	– Businesses do not consider the digital context of the customer when designing and providing personal services.	– Businesses establish a high level of trust between the customer and the business through technology implementation. – The customer experience has a high level of friction.	– Customers have inconsistent experiences across businesses' lines of service and products. – Low-friction transactions, not holistic customer interactions, drive value for the customer.	– Customers have good experiences when interacting within industries. – Multiple systems and standards across sectors support good customer experiences.	– Businesses offer seamless customer experiences within and across sectors. – The evolved model of digital identity is accepted everywhere. – Customers and businesses recognize a high degree of mutual trust and value in their relationships.
Level of ecosystem collaboration	– Businesses focus only on the relationship with the customer.	– There is limited collaboration outside the business-customer relationship.	– Businesses enable collaborations with industry and sector players. – Guidance on interoperability principles is defined at the industry level.	– Businesses agree on standards for collaboration within the industry and sector. – Businesses collaborate to define legal guidelines and regulations to support the industry.	– Standard frameworks for customer data are defined across the industry. – Businesses implement regulations on cross-industry customer data exchange.
Operations and workforce management	– Businesses operate in siloes and have a limited view of the end-to-end customer journey.	– Collaboration across business siloes is limited; IT raises awareness of customer data through security training, etc.	– Business functions have some shared management of customer identities and data.	– Businesses support good collaborative initiatives at the business, sector and industry levels to increase awareness of customer data potential and risks.	– Businesses manage customer and workforce identities and data seamlessly across siloes. – Businesses adjust their operations across sectors to leverage networked digital identity.

Digital Identity: A Design Framework

Creating Value
For governments, businesses, individuals

Principles

Context	Geographies /countries	Industries /sectors	Use cases

Use cases:
Financial services (e.g. e-KYC, transaction proofing, subsidies allocation, etc.)
Gig and sharing economy (e.g. credentialling of gig workers and users, etc.)
Healthcare (e.g. doctor and employee credentialling, sharing trusted health records, etc.)
Mobility (e.g. seamless travel, authenticating car-sharing of drivers and riders, etc.)

Strategic clarity

- **Growing relevance of digital** identity as technology disrupts global, regional and industry landscapes
- **Digital identity's role** in digital transformation, value creation and long-term competitiveness
- **Economic and societal outcomes** that good digital identity can enable in an ever-changing digital context
- **Design elements and choices** to ensure that digital identity delivers value to organizations and key constituencies

Shared Ecosystem

Fit-for-purpose, inclusive, useful, offers choice, secure

Value model	Governance	Actors and roles	Technology and operations	Capacity
– **Gains** that identity could unlock (new business opportunities, enhanced customer experience) – **Pains** that identity could reduce (fraud, inefficiency, friction) – **Identity-enabled business models** (platform models, sharing and gig economy) – **Investment models and cost structures** to maximize returns	– **Appropriate policies** for collection, sharing and use of citizen/ consumer **identity data** – Mechanisms to tackle legal and ethical challenges and **guarantee safeguards** – Approaches to managing **trade-offs** – **Standards** across units, industries, and countries to ensure seamless user experiences – **New social contracts** among governments, businesses, individuals	– **Roles to support** sustainable and functional identity systems – and who should play those roles – **Critical partnerships** and relationships to establish among ecosystem participants – **Collaboration models** to explore among companies, industries, countries and sectors (government, business, civil society)	– **Choice of technology investments** for effective and sustainable identity models – **Shared models and frameworks** to enable interoperable, collaborative identity – **Technology and process design** to establish, verify and manage identity and related data in a **user-centric** way	– **Knowledge, skills and expertise** to build, design and deliver success – Investments in **shared capabilities** (cross-sector coalitions, regulatory sandboxes) – Approaches to **overcome internal and external barriers to change** and successfully transition from past models

Endnotes

1. Murray, Jean, "How Long Does it Take to Start a Business?", 2019, The Balance Small Business, https://www.thebalancesmb.com/how-long-does-it-take-to-start-a-business-3974594 (accessed 01/12/2019).

2. Itsme, 2019, https://www.itsme.be/ (Accessed 20/11/2019).

3. World Economic Forum, "Digital Transformation Initiative: Aviation, Travel and Tourism Industry", 2017, http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/wef-dti-aviation-travel-and-tourism-white-paper.pdf (accessed 20/11/2019).

4. DM News, "A.I. Informs Personalization for Starbucks", 2017, https://www.dmnews.com/customer-experience/article/13035303/ai-informs-personalization-for-starbucks (accessed 20/11/2019).

5. Gartner, "Gartner Predicts: In Search of Balance in Marketing", 2019, https://www.gartner.com/en/marketing/insights/articles/gartner-predicts-2019-in-search-of-balance-in-marketing (accessed 20/11/2019).

6. World Economic Forum, "Shaping the Future of Digital Economy and New Value Creation", 2019, https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation (accessed 01/12/2019).

7. Synaptic Health Alliance, "Improving Provider Data Accuracy", 2018, https://cdn2.hubspot.net/hubfs/4801399/18-SYN-001-Synaptic-Website/downloads/Synaptic_Health_Alliance_Blockchain_White_Paper.pdf (accessed 01/12/2019).

8. Here, 2019, https://www.here.com/ (accessed 02/12/2019).

9. Accenture, "Decoding Organizational DNA in FS: Trust, Data and Unlocking Value in the Digital Workplace", 2019, https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-wf-decoding-organizational-dna.pdf (accessed 03/12/2019).

10. Thomson Reuters, "Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity", 2016, https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html (accessed 15/1/2020).

11. BankID, "This is BankID", 2019, https://www.bankid.com/en/om-bankid/detta-ar-bankid (accessed 20/11/2019).

12. LuxTrust, 2019 https://www.luxtrust.com (accessed 10/12/2019).

13. World Economic Forum, "Digital Transformation Initiative: Aviation, Travel and Tourism Industry", 2017, http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/wef-dti-aviation-travel-and-tourism-white-paper.pdf (accessed 20/11/2019).

14. McKinsey, "Digital Identification: A Key to Inclusive Growth", 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Digital-identification-A-key-to-inclusive-growth (accessed 20/11/2019).

15. McKinsey, "Digital Identification: A Key to Inclusive Growth", 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Digital-identification-A-key-to-inclusive-growth (accessed 20/11/2019).

16. World Bank, "The Role of Digital Identification for Healthcare: The Emerging Use Cases", 2018, http://documents.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf (accessed 20/11/2019).

17. PWC, "The Sharing Economy", 2015, https://www.pwc.com/us/en/technology/publications/assets/pwc-consumer-intelligence-series-the-sharing-economy.pdf (accessed 20/11/2019).

18. Upwork, "Freelancers predicted to become the U.S. workforce majority within a decade, with nearly 50% of millennial workers already freelancing, annual 'Freelancing in America' study finds", 2017, https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017/ (accessed 20/11/2019).

19. HooYu, "Are Trust & Identity Holding Back Further Growth in the Economy", 2016, https://business.hooyu.com/sharing-economy-report (accessed 01/12/2019).

20. PYMNTS, "Who Are You?: Verifying Digital Identity in the Sharing Economy", 2019, https://www.pymnts.com/wp-content/uploads/2019/08/Who-Are-You-Verifying-Digital-Identity-In-The-Sharing-Economy_08_2019.pdf (accessed 01/12/2019).

21. Nuttal, Chris, "BA hit by biggest GDPR fine to date", 2019, *Financial Times*, https://www.ft.com/content/36f3272e-a19e-11e9-974c-ad1c6ab5efd1 (accessed 20/11/2019).

22. Baymard Institute, "41 Cart Abandonment Rate Statistics", 2019, https://baymard.com/lists/cart-abandonment-rate (accessed 20/11/2019).

23. Accenture, "Exceed Expectations with Extraordinary Experiences", 2017, https://www.accenture.com/_acnmedia/PDF-68/Accenture-Global-Anthem-POV.pdf#zoom=50 (accessed 20/11/2019).

24. Ponemon Institute, "The True Cost of Compliance with Data Protection Regulations", 2017, https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study (accessed 20/11/2019).

25. World Economic Forum, "Identity in a Digital World: A new chapter in the social contract", 2018, https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract (accessed 20/11/2019).

26. BCG, "A Great Digital Identity Solution Is One You Can't See", 2019, https://www.bcg.com/en-gb/publications/2019/digital-identity-solution-one-you-cannot-see.aspx (accessed 20/11/2019).

27. SalesForce, "State of the Connected Customer", 2018, https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/e-books/state-of-the-connected-customer-report-second-edition2018.pdf (accessed 20/11/2019).

28. Meek, Teresa, "Five Common Workflow Problems -- And How To Solve Them", 2017, Forbes, https://www.forbes.com/sites/kyocera/2017/08/10/five-common-workflow-problems-and-how-to-solve-them/#5f6e35c057cb (Accessed 05/12/2019).

29. World Economic Forum, "Identity in a Digital World: A new chapter in the social contract", 2018, https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract (accessed 20/11/2019).