

A black and white photograph of several clownfish swimming around a large sea anemone. The image is partially obscured by a dark, semi-transparent shape that frames the text area.

RESEARCH REPORT

The Consumer Digital Identity Landscape 2021

**Migrating to Personal
Identity Ecosystems**

Table of Contents

03	Executive Summary	24	Benchmarking Today's Consumer ID Experience
05	Introduction	35	Moving to Personal Identity Ecosystems
06	The Identity Lifecycle	41	Building Personal Identity Ecosystems
09	Consumer-Centric Market Drivers	44	Appendix
11	The Digital Identity Landscape	45	About Us

Chief Editor:
Nick Holland, Director of Research

Contributing Authors:
Jennifer Berry, President
Will Charnley, Advisory Manager
Cameron D'Ambrosi, Managing Director
Travis Jarrae, CEO
Vatsal Jhawar, Analyst
Alice Zhou, Research Manager

Executive Summary

Consumer identity management remains firmly anchored upon the legacy concept of one identity to one service. Accustomed to these siloed proprietary ecosystems and the resulting mechanisms for identity verification and authentication, consumers have proven unwilling to embrace attempts to centralize these functions into digital wallets. Adoption of proprietary digital wallets by relying parties and service providers remains low due to the lack of an engaged user base, reluctance to commit engineering resources to lengthy integrations, along with competitive and regulatory concerns around data privacy. As such, users and providers alike remain unwilling to make the first move towards adopting and implementing the next generation of digital identity federation technologies.

Consumer digital identity today is split into two distinct categories – established, paid for services that attempt to address the threats of the current paradigm, such as antivirus, password managers, and consumer identity theft protection, and services that are in their infancy, such as eIDs / Civil IDs, digital identity wallets and Self Sovereign Identity (SSI).

The continued evolution of digital identity within its original silos has generated a number of negative externalities that impact consumers today. Liminal ran a study of 1,500 consumers to better gauge their sentiment, concerns, and behaviors around digital identity:

- Consumers are required to personally navigate a fragmented identity landscape forcing them to adopt identity management practices that are at best risky, and at worst, plain dangerous. Over 44% of consumers use just two to five password variants for all accounts, with 16% using the same password for all accounts.
- Consumers are forced to jump through identity verification and authentication hoops across the account lifecycle that are cumbersome and often badly designed around legacy architecture and manual processes. 42% of consumers have abandoned an online or mobile account application due to friction at onboarding.
- Lack of transparency relating to how consumer data is being used and shared causes consumers to avoid using certain platforms and technologies. For example, a quarter of consumers state that they actively avoid using biometrics due to privacy concerns and three-quarters of consumers have chosen “Do Not Track” as an option for sharing their personal data with third-parties in the Apple ecosystem.
- Consumers are ill-informed when it comes to best practices for protecting their

identities. This is evidenced by a third of “highly knowledgeable” consumers using the same password for all online accounts.

- Consumers have considerable, well-founded concerns about becoming victims of identity theft. Nearly half of consumers are concerned or very concerned about identity theft and one in ten consumers have been a victim, with a likelihood that older consumers will be victims on multiple occasions.

Signs are good that consumers will adopt digital wallets if the circumstances permit — 60% of consumers were likely or very likely to store their driver’s license on their phone, and 55% were likely or very likely to store their passports. The ability to vote in a national election via smartphone was also seen as an attractive capability, with half of survey respondents expressing that they would be likely or very likely to do so if this was possible.

Unlocking the current one to one marketplace will require the development of Personal Identity Ecosystems (PIEs) as the connective tissue between consumers and service providers, streamlining four consumer identity traits that are fundamentally important to them:



Privacy: the consumer’s ability and right to own, control, restrict, remove and protect their digital identity. These are fundamental traits at the core of digital identity wallets and self sovereign identity initiatives.



Commerce: the consumer’s ability to leverage services to initiate online transactions and payments.



Reputation: the consumer’s ability to manage their online presence and information about them.



Data protection: the consumer’s ability and right to protect their data, systems, devices and digital identity from fraudsters and thieves.

Moving past the current one identity to one service paradigm will require the implementation of PIEs as the connective tissue between consumers and service providers. This will allow consumers to move from the current centralized identity management architecture to one where identity is decentralized, at first as a one-to-many digital identity wallet, where the user is at the center of the ecosystem and able to choose where their identity is accessed, and eventually as a many-to-many digital wallet ecosystem.

Introduction

Consumer Identity is Broken

It should come as a surprise to absolutely no one that consumer identity is in need of an intervention. Decades of neglect have led to the current state of play – identity fraud is rampant and consumers are justifiably paranoid about the lack of control that they have over their digital destinies.

The crux of the problem lies in the exponential expansion of digital services across our daily lives, intensified by a pandemic that heightened an ever-growing reliance on the internet to meet increasingly remote lifestyles. Despite more robust and user-friendly technologies coming to market, consumers are still using weak forms of identity management built on layers of labor-intensive friction and are forced to complete cumbersome analog identity verification tasks shoehorned into digital interfaces. It is little wonder that nearly half of consumers have abandoned an online financial services application due to friction.

Further compounding consumer distrust, an entire industry has developed based upon the harvesting and reselling of consumer identity data. Consumers largely lack understanding of how their data is being captured, monetized, and circulated, and are unable to easily opt-out of the ecosystems that capitalize on their information. It's a system that, put simply, is broken. In the words of Michael Schrage of MIT,

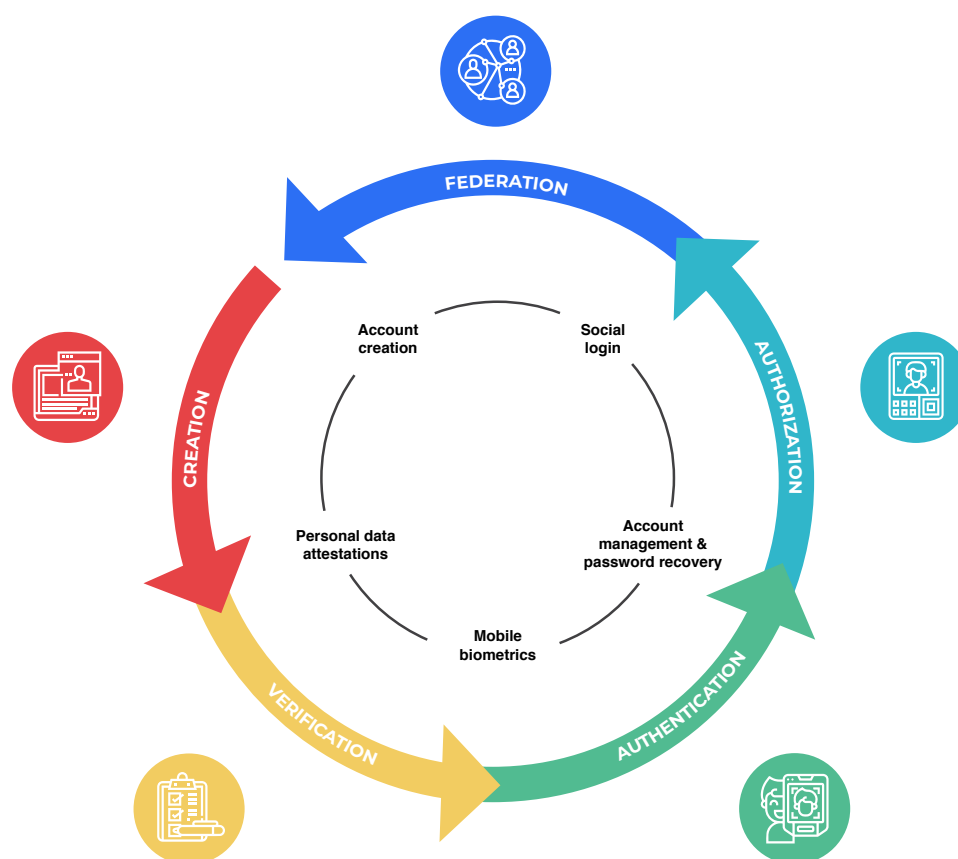
“Profitability predicated on customer friction, intrusion, and irritation simply isn’t sustainable.”¹

As this report highlights, a considerable amount of work must be done to rebuild the trust between consumers and service providers, but the challenge is not insurmountable. It will, however, require a comprehensive recalibration of current identity architecture to address consumer pain points, most notably, the breaking down of today's 1:1 ecosystem of consumer to service provider relationships and building Personal Identity Ecosystems (PIEs) that will facilitate migration to trusted, decentralized consumer identity management.

The Identity Lifecycle

There are five distinct stages to the identity lifecycle – creation, verification, authentication, authorization, and federation (Exhibit 1).

Exhibit 1



Source: Liminal Advisory Services



Creation: Onboarding a user requires the development of the presence for the first time through data resources and trusted third parties. The creation of an account does not require a learning curve by the user or by the organization. Instead, it requires verifying the digital identity that the resources and trusted third parties have on hand.



Verification: Since an organization could not know that the person entering credentials was the user, early verification through passwords had little value. The organization needs a link between the user and something unique to the individual's identity. This can come in the form of biometrics, a verified ID, or a third-party database, including government sources, social identity, or a user's phone number.



Authentication: When a user attempts to access an account, the organization must ensure that the person has the right credentials and that those credentials have not been shared with someone else. Biometric data, behavioral biometrics, and when and where the person tries to access the site can all help provide this proof. This ensures that the person is who they say they are.



Authorization: Based on authentication, the organization then needs to ensure that the individual only accesses the system at the level they have credentials for. Allowing authentication does not necessarily allow full access to a system — bank customers do not have access to the vault simply because they have passed as an authenticated user. Authorization ensures that the credentials are used only at the level of access allowed.



Federation: The less siloed an organization, the better their ability to have a clear view of the user, from onboarding, to client management, to compliance, to customer retention. If every entity within the organization has this clear view and a lack of overlap in the data used, then the organization can hold a stronger view of the customer. Interoperability across organizations and partners also requires consistency in the type of data used to ensure strong identification.

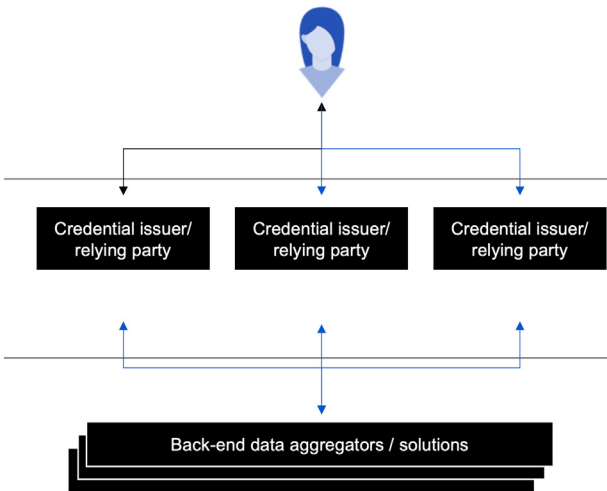
These five components of the identity lifecycle develop an ecosystem of trusted relationships, creating a flywheel for more robust confidence that an individual is who they claim to be.

This trusted relationship ecosystem lays the foundations for commerce, travel, banking, education, healthcare, and even democracy.

However, a fundamental problem with consumer identity management today is that it is built on one identity to one service – consumers are as yet unwilling to embrace digital wallets and are accustomed to isolated, proprietary ecosystems based on technology (Exhibit 2). Conversely, service providers are reluctant to commit to lengthy integration procedures for these proprietary systems and remain concerned about data privacy with third parties. As such, users and providers are both unwilling to make the first move in implementing identity federation.

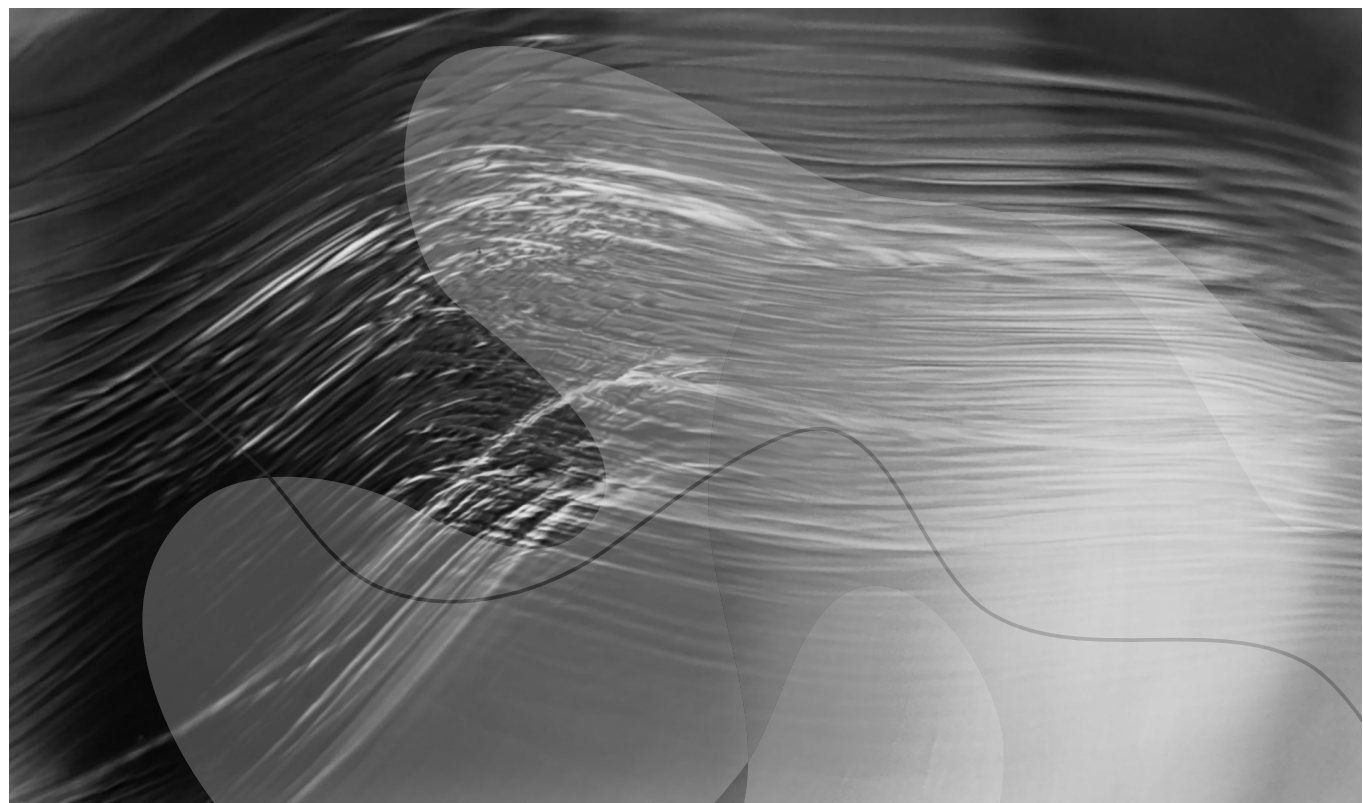
Exhibit 2

Consumer impact of complicated back-end user data management systems

Current State	Description	Impact to Consumers
	<p>Consumers engage with companies and institutions individually, furnishing and managing myriad identity connections</p> <p>Many businesses/organizations collect consumer data, issue credentials/accounts, and exchange data through consortiums or vendor agreements</p> <p>Businesses proliferate, exchange, and consolidate consumer data from various sources into back-end databases</p>	<ul style="list-style-type: none">▪ Fragmented credential management▪ Lack of privacy and user control▪ Inconvenience and friction▪ Consumers lack technical knowledge to protect themselves▪ Informed consumers continue to ignore best practices▪ Potential for data breaches, resulting in increased identity theft risk (consumer) and reputational damage (enterprise)

Source: Liminal Advisory Services

This “chicken and egg” conundrum is at the heart of issues facing consumer identity today. Without a central consumer identity platform providing the connective tissue, consumers are forced to manage one identity per online service.



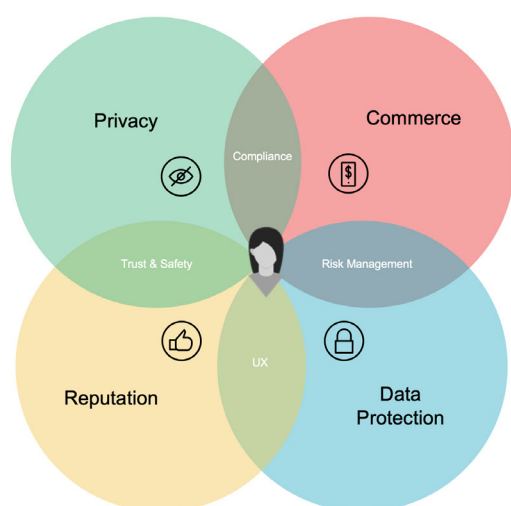
Consumer-Centric Market Drivers

When we refer to “consumer digital identity,” we refer to functions that are initiated by a consumer, rather than functions that are initiated by a party without the explicit consent of a consumer. These include activities that are specifically dedicated to protecting consumer digital identities, such as antivirus, identity theft protection, and password generators, as well as emerging functions that will enable consumers to have control over the federation of their digital identity data, such as eIDs / Civil IDs, digital identity wallets and self-sovereign identity.







Consumer digital identity lies at the intersection of a number of dynamics – privacy, reputation, data protection, and commerce (Exhibit 3). Harmoniously managing these demands delivers an optimal experience when it comes to identity management – consumers clearly want to conduct transactions digitally, in part because traditional retail channels remain a more challenging environment during a pandemic, but also because of a steady but consistent march towards digital commerce since the dawn of the internet. COVID-19 was an accelerant on an already well-lit fire.

Exhibit 3

As high-value transactional data, digital identity supports foundational consumer and enterprise functions, such as commerce, privacy, data protection, and reputation



Major Drivers For Change

-  Consumers demand privacy-centric solutions
-  More governments provide citizens access to services online
-  Consumers use mobile device for high assurance transactions
-  Open banking has conditioned consumers to control their data
-  Growing concerns around IoT data protection and privacy
-  Rise of the gig economy requires reputation management

Source: Liminal Advisory Services

Digital consumption is universally accessible today via laptops and smartphones, but consumers are likely to be deterred from doing so if privacy, reputation, and data protection are not adequately addressed. In combination, these attributes support the formation of consumer trust. Developing this trusted relationship is foundational for sustained consumer

adoption of existing digital functions such as shopping, banking, and communications, as well as forming a bedrock for incremental functions such as medical care, international travel, purchasing of age-restricted goods and services, and conducting civic activities such as voting.

There are a number of macro trends that are shaping the changing consumer identity landscape.

Governments accelerate changeover of legacy systems and processes:

- Governments are increasingly offering online services to their citizens, requiring robust digital verification and authentication, particularly as digital wallets include higher-value services such as storage of digital driver's licenses, passports, and health records, and potentially even the ability to vote in national elections.

Rising regulatory pressure around consumer data privacy and protection:

- With the implementation of regulations like the Second Payments Services Directive (PSD2), open banking is becoming increasingly mainstream, with consumer banking and payment data shared by third parties. Security is a fundamental component of open banking, as is consent management – enabling customers to opt-in or out of where their data is shared and with whom. With open banking demonstrating how well-managed consumer data can be beneficial to a wider ecosystem, the model is increasingly appealing to other industries – again, with the caveat that the consumer is central to the federation of personal data and can withdraw this privilege at any time.

Technological advances create new identity challenges:

- Consumer-centric IoT technology is becoming increasingly pervasive in our daily lives with the proliferation of smart speakers, connected appliances, and home monitoring equipment. The myriad companies in this space, many producing devices with low levels of security, have generated a minefield of privacy and data protection issues. Concerns relating to the capture and usage of the significant personal data exhaust generated by IoT devices are also pushing consumer identity management to the forefront.

Shifting industry vertical demands creates new use cases:

- The gig economy is driving demand for more robust proof of identity as consumers increasingly rely on complete strangers for transportation, food delivery, accommodation, and many other personal daily functions. It will be imperative for digital platforms to vouch for the integrity of individuals that we are collectively allowing to enter our physical environments.

The Digital Identity Landscape

When we discuss the identity ecosystem, we refer to the Liminal Digital Identity Landscape, a proprietary mapping of solution segments and how they interact with one another to form the broader digital identity industry.²

The COVID-19 pandemic has forced consumers and businesses alike to transition aggressively to a digital first mindset. This encouraged industry to improve procedures and to make them easier for consumers to understand and handle. However, this has not gone far enough. Consumers have inherited numerous issues from a digital identity landscape that has been allowed to develop organically:

- **Consumers are required to manage a fragmented identity landscape themselves which forces them to adopt identity management practices that are at best risky, and at worst, plain dangerous**
- **Consumers are forced to jump through identity verification and authentication hoops at onboarding and beyond that are cumbersome, often derived from legacy analog practices that are shoehorned into digital interfaces**
- **Lack of transparency relating to how consumer data is being used and shared is causing consumers to avoid using some platforms and technologies**
- **Consumers are ill informed when it comes to the best practices for protecting their identities**
- **Consumers have considerable, well founded concerns about becoming victims of identity theft**

Two important takeaways come from these issues:

- 01** First, consumers don't want to have to pay to solve these problems. They don't understand the issues involved and even fewer know the best way to circumnavigate the hurdles. It's becoming a competitive advantage for enterprises that incorporate these fixes and solutions for the consumer, which has led to a significant shift towards consolidation.
- 02** Second, it creates an opportunity for forward-thinking organizations that offer a way to solve these issues for the consumer, more directly. This moves the identification industry from one that has focused on the B2B or B2B2C business models, to one that can operate in the B2C space as well.

Consumer Digital Identity Segments

Consumer digital identity today is split into two distinct categories:

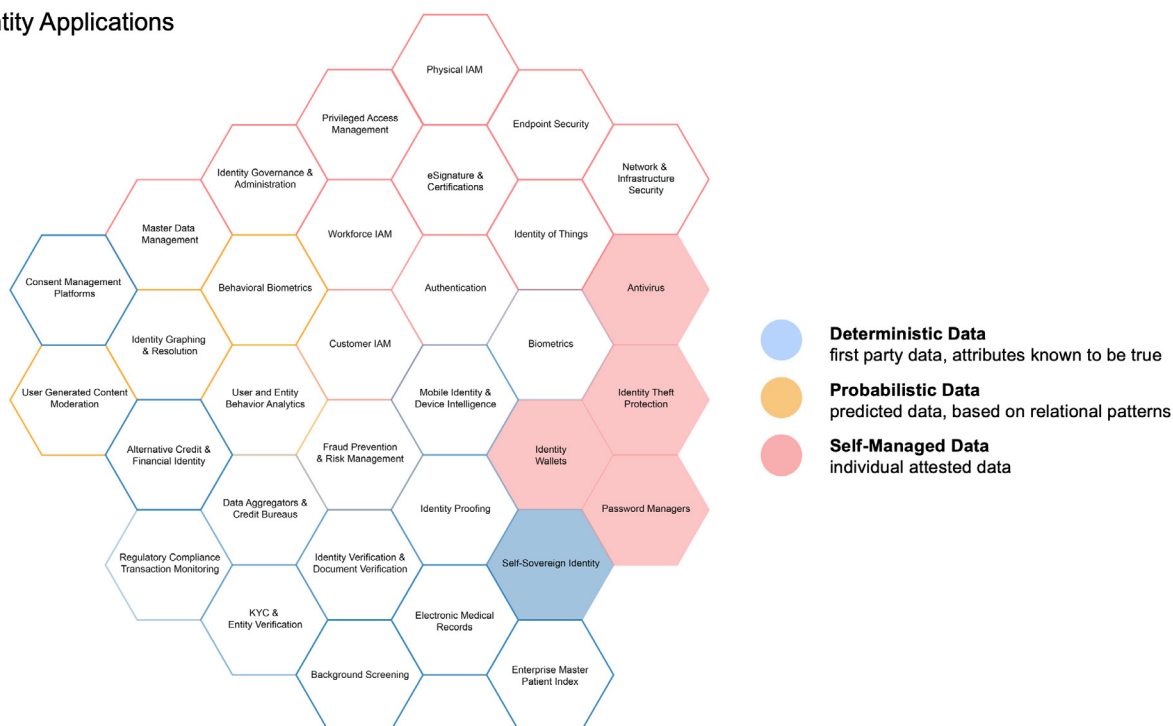
- Established, paid-for services designed to address cybersecurity threats preemptively, such as antivirus, password managers, and consumer identity theft protection
- Services that are in their infancy, such as eIDs / Civil IDs, digital identity wallets and self-sovereign identity

While consumers are somewhat familiar with companies offering cybersecurity services, these companies are, for the most part, addressing symptoms of the current state of identity management rather than more fundamental issues pertaining to the way that consumer digital identity has been allowed to evolve. eIDs / Civil IDs, Digital identity wallets and self-sovereign identity are intertwined as technologies that will pave the way for the re-architecting of consumer digital identity in the coming years.

Exhibit 4

Liminal 2021 Digital Identity Landscape

Consumer Identity Applications



Antivirus

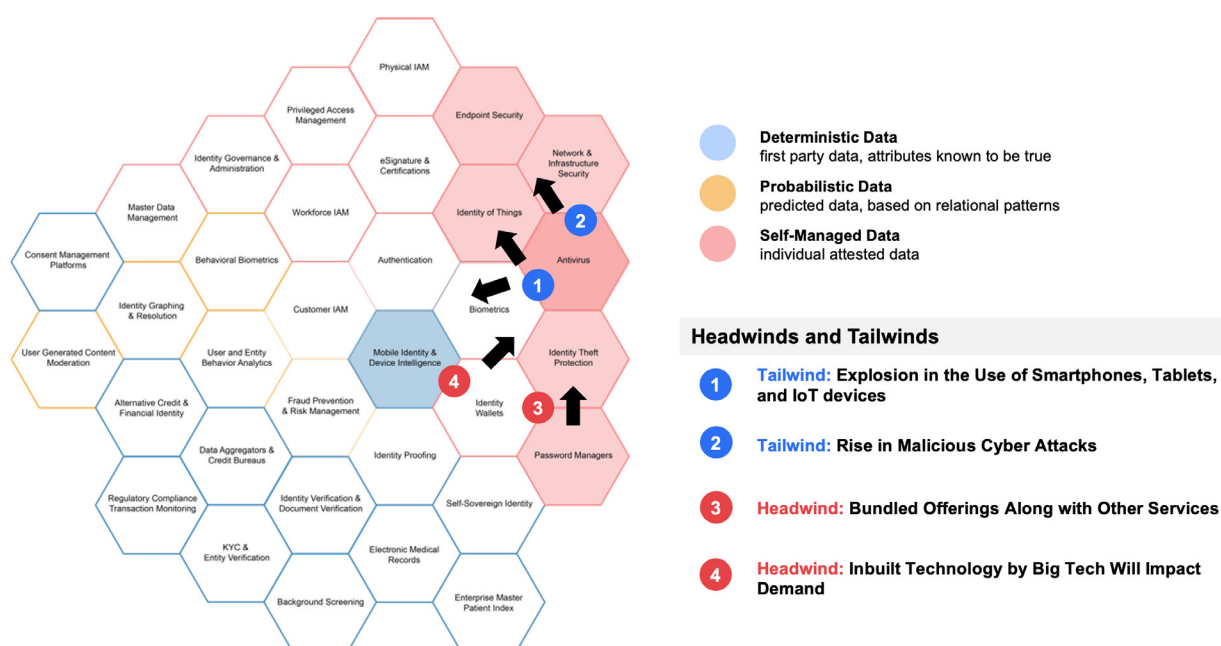
Antivirus software runs in the background and works as a gatekeeper to prevent, detect, and remove viruses and malware that put identity data at risk. While this originally had a single focus, Antivirus now goes beyond protecting computers and extends across smartphones, tablets, and IoT devices to prevent social engineering techniques, advanced persistent threat (APT), and botnet Distributed Denial-of-Service (DDoS) attacks. Antivirus services, while widely available and commoditized, are one of the few cybersecurity services that consumers are accustomed to paying for, and therefore provide a valuable entry point for upselling of other data protection services.

Why Antivirus Matters

Despite being one of the oldest countermeasures to cybersecurity attacks, developed in the early 1970s, antivirus is still an important tool in the arsenal of fraud and cyber risk mitigation today. Attackers have evolved over time, matching the changing architecture and platforms of computing, including the rise of the cloud, use of mobile devices, the development of app stores, and more. As a result, antivirus providers now offer a plethora of solutions to meet this changing environment, including traditional detection tools, as well as services designed to prevent cybersecurity incidents. Antivirus tools are also often sold bundled with consumer identity theft protection and password manager apps, offering a holistic consumer protection solution. With evolving threats such as ransomware still reliant on rogue software infiltrating networks, antivirus software is as important as ever (Exhibit 5).

Exhibit 5

Antivirus: headwinds & tailwinds



Market Tailwinds:

- Explosion of smartphones, Tablets, IoT devices: as consumers become increasingly connected, so do the opportunities for cyberattacks across a diffuse attack surface of multiple IoT devices and smartphones.
- Continued proliferation of cyberattacks: the velocity of cybersecurity attacks has not abated and criminals are continuing to diversify in tactics. Virus protection remains critical.

Market Headwinds:

- Bundling with other offerings, embedded technology in big tech: increasingly, antivirus is a service offered as a component in a bundle of other services such as identity theft protection and home insurance, or in the background by big tech companies, diminishing its value as a standalone service.

Consumer Identity Theft Protection

Consumer identity theft protection solutions monitor personal data for anomalies and provide paths for identity restoration in the event of theft. Identity theft services include reimbursement options and legal support to help undo any damage incurred to credit, reputation, or fiscal standing due to identity theft. These are often sold as a component of a larger bundle of cybersecurity services such as antivirus, as well as with insurance for physical items such as home and auto.

Why Consumer Identity Theft Protection Matters

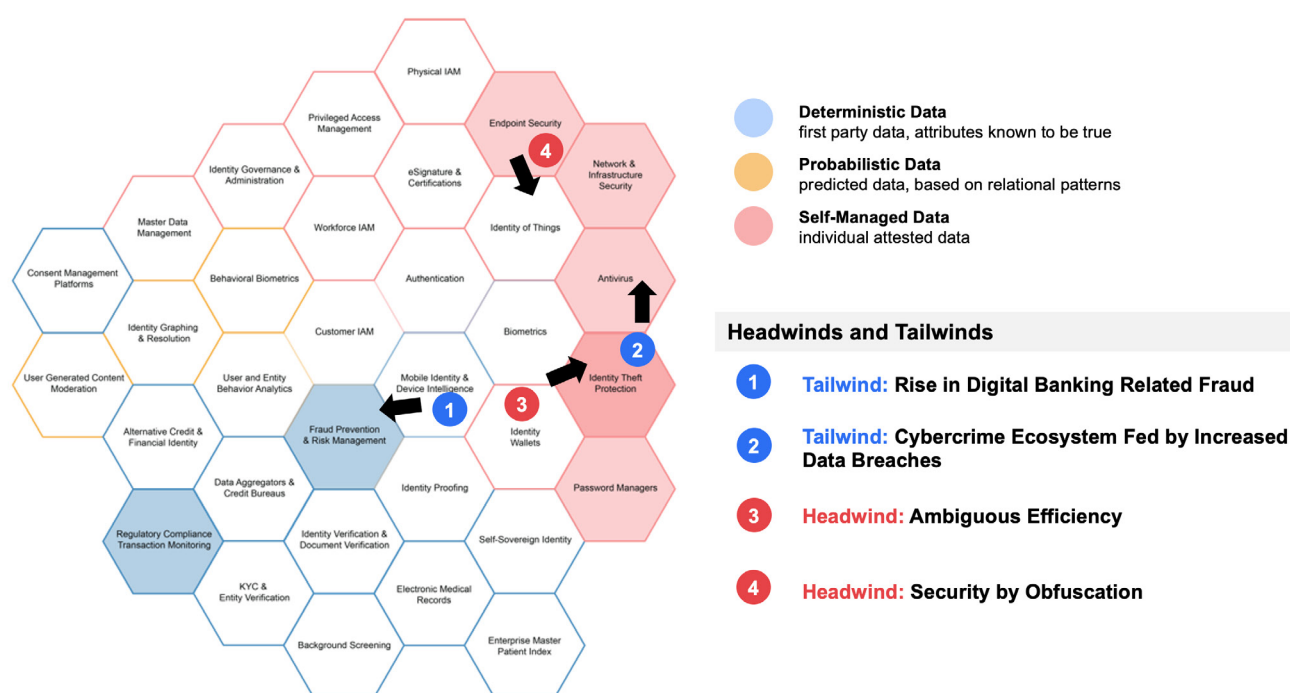
In 2020, 86% of all data breaches were financially motivated and organized criminal groups were behind 55% of breaches.³ Each data breach continues to feed the wider cybercrime ecosystem, which becomes more connected and sophisticated each day. Once sensitive data has been exposed, it can be subject to a wide array of exploitation mechanisms. In some cases, the data itself can be simply sold as a black market asset, with prices for a stolen digital identity ranging from less than \$1 to \$450, depending on the information available.⁴ Both public and private entities may provide identity theft services to individuals who may have been the subject of a data breach to help monitor their credit accounts and/or restore their identities in the case of identity theft. As of November 30, 2018, the United States Office of Personnel Management (OPM) has committed \$421 million in funding for a suite of credit and identity monitoring, insurance, and identity restoration services to approximately 22 million individuals affected by its 2015 data breaches.⁵

In the instance of a data breach, consumers may immediately opt-in to identity theft protection services. In September 2018, the provision of a federal law within the U.S. made it free for consumers to place credit freezes with the three nationwide consumer reporting agencies (i.e., Equifax, Experian, and TransUnion). Credit freezes can restrict businesses from accessing an individual's credit report and prevent the illicit opening of a new account or loan in the

individual's name. The efficacy of short-term identity monitoring solutions is debated. Because fraudsters can use stolen information for years after a data breach, efforts to mitigate damage control may be out of any one consumer's individual control. This is one of many reasons why digital identity solutions work as a holistic approach to safeguarding personal information (Exhibit 6).

Exhibit 6

Identity Theft Protection: headwinds & tailwinds



Source: Liminal Advisory Services

Tailwinds:

- Rising digital banking fraud, increasing data breaches: as with the market for antivirus, the continued onslaught of cyber threats and data breaches are motivating factors for consumer investment in identity theft protection solutions.

Headwinds:

- Ambiguous efficiency: the inability for consumers to see a direct benefit in paying for identity theft protection is a deterrent from investment. Further, these services are often offered free of charge as an after-the-fact reparation effort for consumers that may have had their PII exposed in a cybersecurity incident -- consumers may simply wait for the next breach of the identity information to occur to secure a new subscription.

Password Managers

Given the prevalence of passwords as a form of authentication despite numerous attempts at deprecation, they persist as the gatekeeper for the majority of online accounts. If the average consumer has 100+ digital accounts to manage, it is highly unlikely that password hygiene is being adhered to. The role of the password manager application is to semi-automate the process of generating strong passwords for each unique login, solving the problem of there being more accounts per consumer than can manually be managed, and the complexities of generating sufficiently complex passcodes. As research highlights further on in this report, less than 10% of US consumers use password managers today.

Why Password Managers Matter

In 2020, 37% of data breaches were a result of stolen or misused credentials. 58% of all victims had personal data compromised.⁶ Once sensitive data has been exposed, it can be subject to a wide array of exploitation mechanisms.

Poor password hygiene is a driving force behind security breaches — particularly in businesses, where 81% of all breaches are said to be due to compromised passwords, presenting an opportunity for password managers with enterprise customers.⁷ Password management services address this problem by encouraging automatically-generated, “unguessable” passwords that are unique to each online service, and storing these passwords so that users do not have to memorize them (Exhibit 7).

Consumers across the globe still require additional awareness, and adoption, of recommended digital privacy and security practices. 71% of U.S. consumers report being concerned about the security of their personal and financial information. 50% feel very confident they are taking appropriate online safety precautions, 53% claim to have strong password hygiene practices, yet only 24% use a VPN.⁸ To increase adoption, password managers must increase customer awareness of the value of using a password manager, educate customers on the onboarding procedure, and gain customers’ trust.

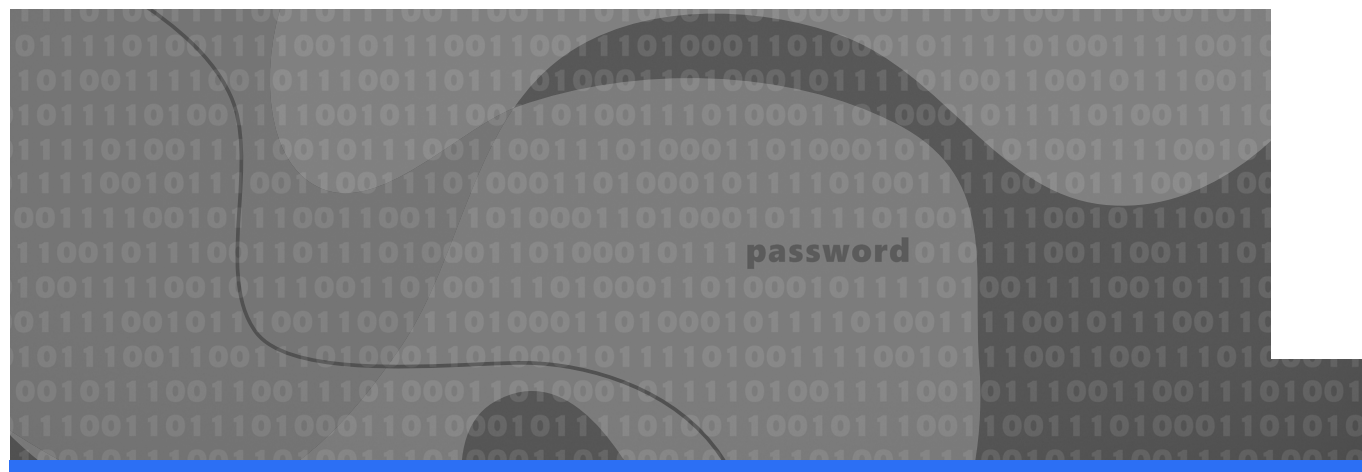
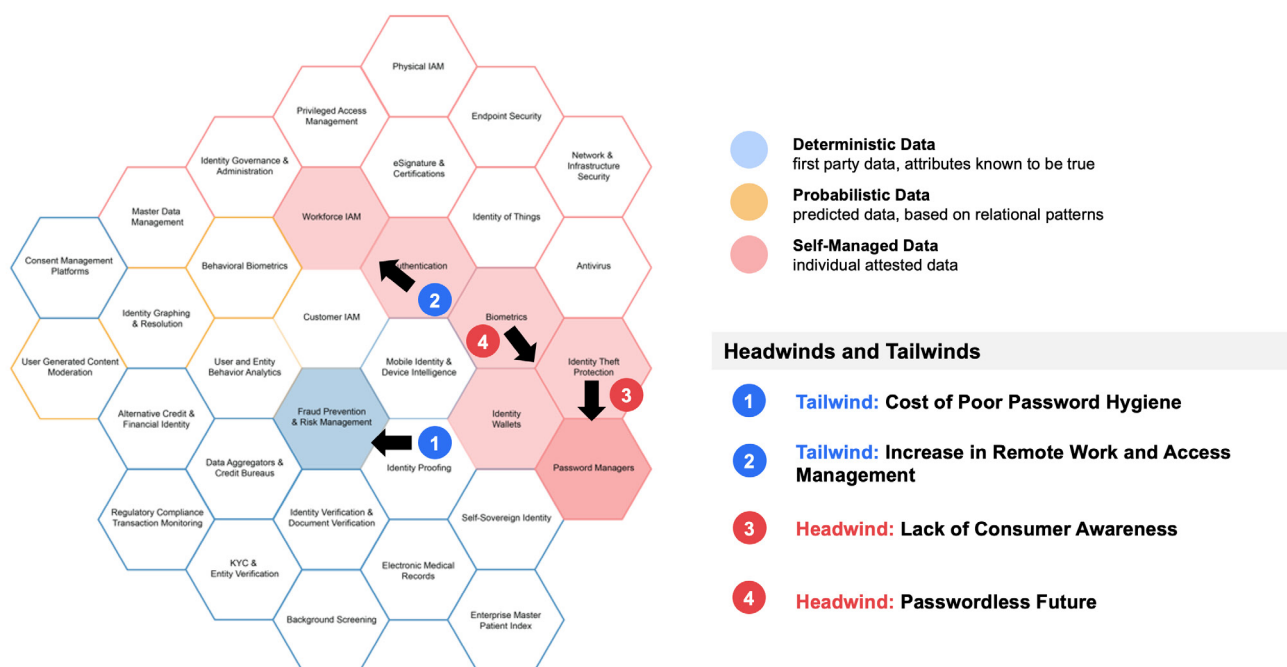


Exhibit 7

Password Managers: headwinds & tailwinds



Source: Liminal Advisory Services

Tailwinds:

- Cost of poor password hygiene: passwords and bad password management are the Achilles heel of cybersecurity. Password managers are an appropriate stopgap measure for an industry that is still heavily reliant on a password-based architecture for authentication.
- Increase in remote work and access management requirements: with a post COVID-19 workforce that is now increasingly remote, organizations are more likely to mandate password managers for their employees, which can be expected to increase awareness and drive usage into non-work applications.

Headwinds:

- Lack of consumer awareness / apathy: consumers appear mostly ambivalent about using password managers and are unable to connect the dots between bad password management and cyber risk. Further, these services typically require subscriptions for premium offerings.
- A passwordless future: while the death of the password has been long coming, it may finally be a reality as big tech pushes for passwordless alternatives. With the demise of passwords comes the associated demise of password managers.

Electronic IDs (eIDs) & Civil IDs

As a generic term, the European Commission has described eID as a means for people to prove electronically that they are who they say they are, allowing an entity (citizen, business, administration) to be distinguished from any other, to gain access to a panel of services, and often to fulfil different roles (e.g., a civil servant, a lawyer, or a parent) depending on the context.⁹

Why eIDs & Civil IDs Matter

The various benefits, such as enhanced security, privacy preservation, ease of administration, and high scalability of eID cards have incentivized the global adoption of eID schemes, enabling eIDs to become an increasingly popular alternative to traditional card-based IDs. While many countries have adopted digital schemes / eID globally, Europe is currently a pioneer with a total of 22 eID schemes (18 notified and 4 pre notified).

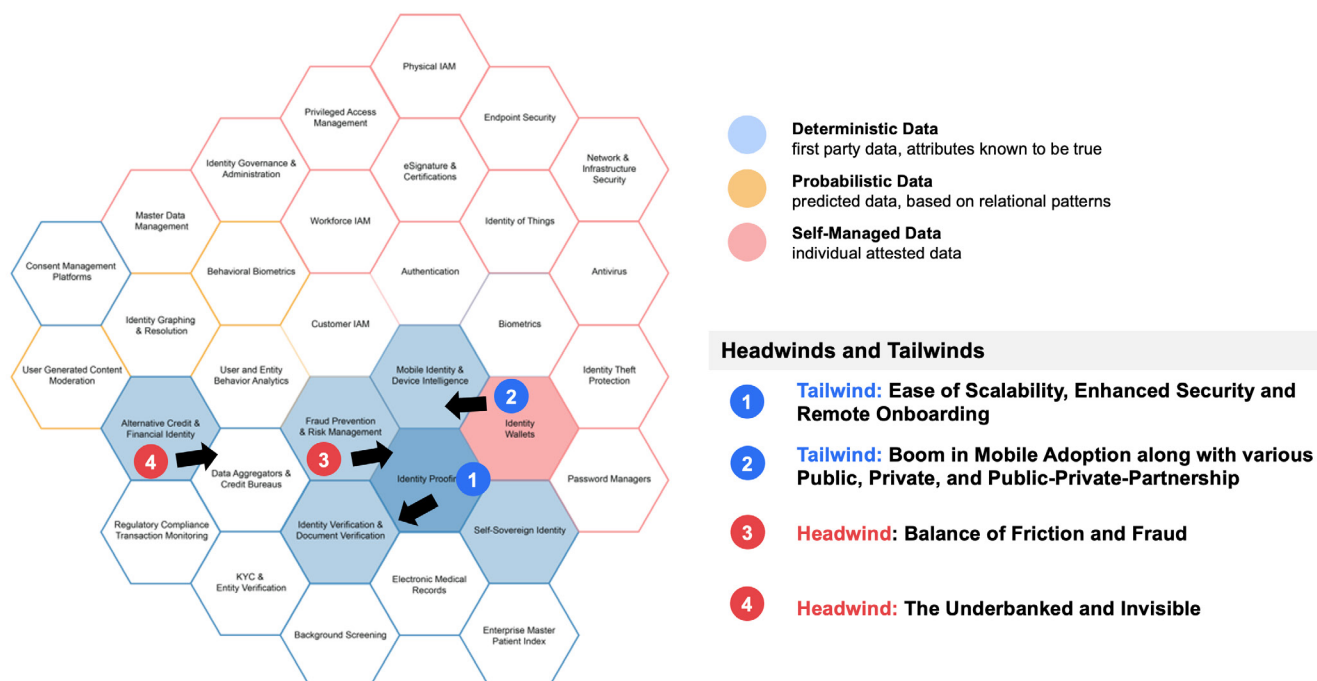
eID projects can be driven by different parties, emerging as public initiatives, private initiatives, or public-private partnerships (PPPs). The difference in driving parties leads to varying user onboarding approaches. The use of eID also varies region-by-region. In many regions, such as UAE and Colorado, eIDs can be used as proof of identity to access both government services as well as private sector activities such as online banking and digital payments, whereas in other regions, eIDs are limited for access to certain specific public services.

Europe is one of the leading regions for digital identity initiatives. eID in Europe is specified as a set of services provided by the European Commission to enable the mutual recognition of national eID schemes across borders. It allows European citizens to use their national eIDs when accessing online services from other European countries.



Exhibit 8

eID / Civil IDs: headwinds & tailwinds



Source: Liminal Advisory Services

Tailwinds:

- Ease of scalability and remote onboarding: the case for eIDs and Civil IDs is obvious in the enablement of myriad civil programs which are likely to cascade into adjacent initiatives. eIDs / Civil IDs also solve for the significant issue of onboarding abandonment due to onerous identity verification steps reliant on physical documentation.
- Boom in mobile adoption with various public / private partnerships: the proliferation of smartphones makes eID / Civil ID programs for mass populations far more achievable.

Headwinds:

- Balance of friction and fraud: eID / Civil ID programs are likely to be targets for fraudsters, particularly where fund disbursement is a component. These initiatives need to have robust fraud controls in place, yet not be so cumbersome as to dissuade adoption.
- The underbanked, unbanked, and invisible: while mobile penetration continues to rise, there is still a significant percentage of the population that exist without access to banking and other services. It is important that eID / Civil ID initiatives are designed to be inclusive of the less technologically literate population.

Digital Identity Wallets

Digital identity wallets are secure, smartphone-enabled applications that provide individuals with the power to manage their own digital identity credentials. Digital identity wallets offer citizens control over their data, including what information they share, when, and with whom. Digital identity credentials bridge the offline to online divide and provide access to services with additional privacy, security, and user consent. As smartphone manufacturers, card issuers, and government entities seek means of digital secure storage of credentials such as driver's license, passport, medical information, and more, the digital identity wallet market is set to grow significantly.

Why Digital Identity Wallets Matter

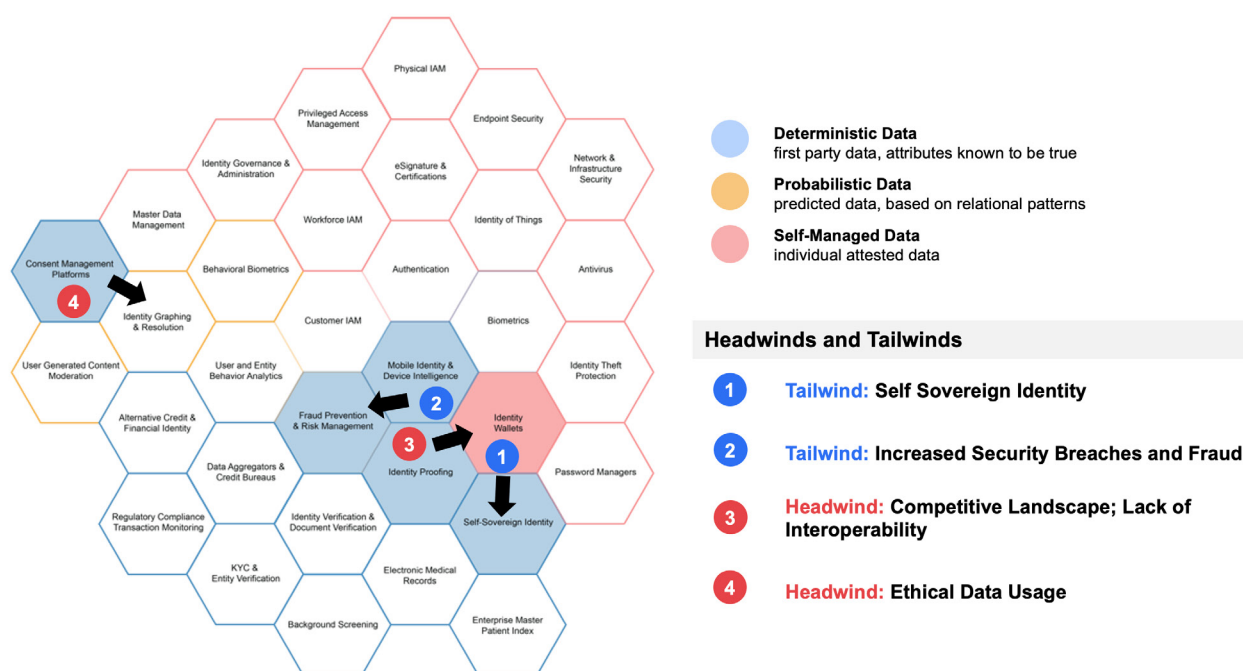
Because of the breadth of the consumer products and solutions in the market that manage personal identity data, there is no universal, all-encompassing digital identity wallet. Today, consumer digital identity data lives across a number of applications and mediums including physical documents, digital documents, hard drives, mobile devices, cloud applications, and more. The market has introduced discrete solutions for managing genealogy data, medical records, and other facets of consumers' personal identities; however, the solution segment has yet to create a widely adopted personal identity wallet. As more firms, both startups and large multinationals alike, focus on consumer digital identity, there will likely be greater convergence in the identity wallets segment, especially as Big Tech and financial services companies focus their efforts in the space.

Demand for digital identity wallets will be driven by consumers who have an appetite to expand their digital portfolio of personal identity information conveniently and securely. Factors such as the increasing number of security breaches and fraudulent transactions will also drive demand to help securely manage personal identity data. Future identity wallets may also overlap with the self-sovereign identity (SSI) solution segment, which is based on the concept of decentralizing all digital identity attributes such that individuals retain the autonomy of their digital identities (Exhibit 9).



Exhibit 9

Identity Wallets: headwinds & tailwinds



Source: Liminal Advisory Services

Tailwinds:

- Self Sovereign Identity trends: as outlined later in this report, Self Sovereign Identity (SSI) is a popular and achievable solution for rectifying the current identity management predicament of an unsustainably large number of 1:1 consumer to service provider relationships. Digital identity wallets are a fundamental step on this journey.
- Increased security breaches and fraud: the ongoing plague of cybersecurity attacks needs to be dealt with proactively. Digital identity wallets will be a critical step in mitigation efforts.

Headwinds:

- Competitive landscape, lack of interoperability: there are currently dozens of digital identity wallet initiatives in play. Interoperability between platforms, vendors, operating systems and other entities is not assured at this time, potentially leading to a balkanization of digital wallets, stifling adoption and use cases.
- Ethical data usage / big tech skepticism: there is a trust gap between consumers and digital wallet providers, particularly those offered by organizations that have been somewhat porous with personal identity credentials to third parties. Building trust will be an imperative, but this trust is likely to be fragile and could be easily destroyed with bad / unethical practices.

Self Sovereign Identity (SSI)

The goal of SSI is to promote the usage of decentralized identifiers (DIDs) that are decoupled from federated solutions, centralized registries, and identity providers. With SSI, individuals can maintain ownership of their own portable, interoperable, and consented digital identity attributes. SSI frameworks are popularly associated with distributed ledger technology (DLT) and blockchain technology. SSI is in its infancy but has significant appeal from consumers as a means of bringing control of the usage of PII back to the owner of the identity.

Why SSI Matters

Today, individuals possess dozens, if not hundreds, of digital identities -- from social media profiles to bank accounts. With progressive profiling, the amount of data that comprise those identities grows each time an individual uses a service. The data economy has become a centralized system with a few key players that have become data silos with vast PII data. The increase of fraud, data breaches, regulations, and companies being more transparent with their data has raised data privacy concerns. These rising concerns have created a new paradigm shift to SSI, giving users control of their data instead of being controlled by large institutions and monetizing from it, causing an interest in SSI in the market but adoption struggles.

SSI is making enterprises excited about blockchain's intersectionality into an identity use case. The potential SSI architectures have to offload digital identity processes to an external third-party network. Just as exciting enterprises are, they are equally unsure of the relatively nascent products. So, buyers in the industry are waiting for an SSI solution to have an overwhelming success story or illustrate longevity before going all-in. SSI concept is a bottom-up approach to identity that requires every user to control their own identities.

Additionally, an SSI product requires mass adoption of users before working effectively, given its dependency on the blockchain, considering that the SSI industry is still benefiting from strong institutional investment from significant participants such as IBM, Microsoft, and national governments. Suppose the industry can solve the SSI product and hypothetically make it a required digital identity process for a widely-adopted product like Microsoft Office. In that case, SSI could quickly become an industry-leading solution overnight.

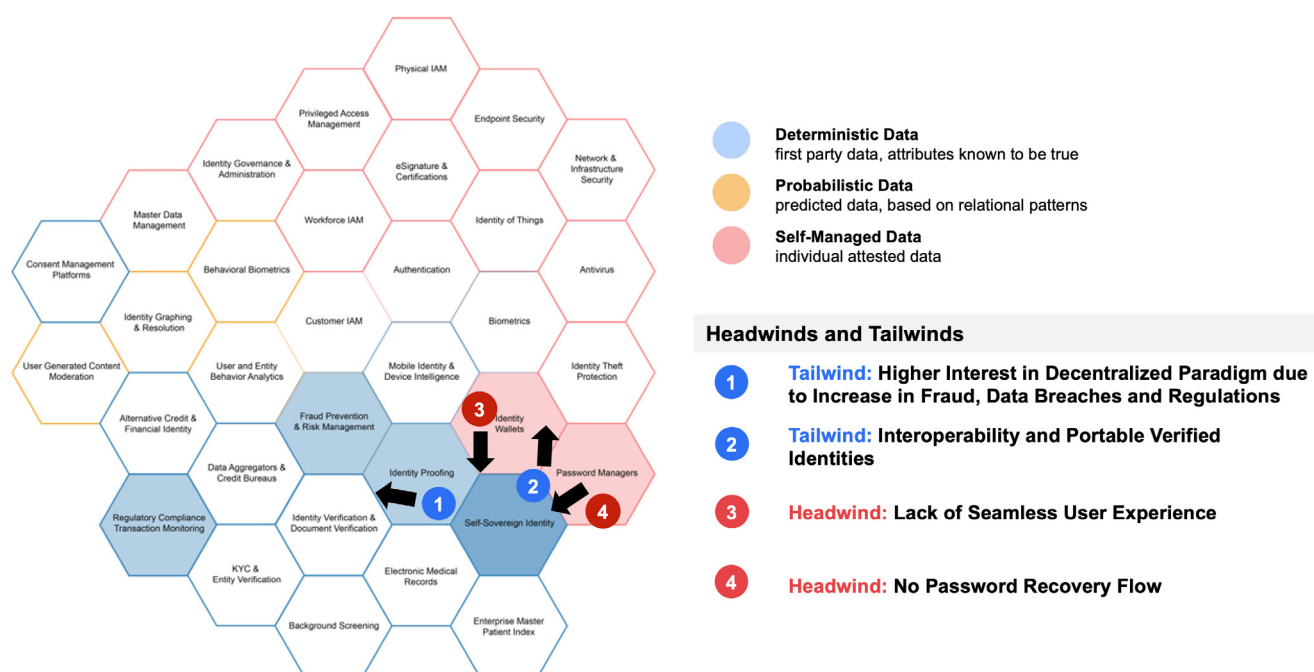
SSI needs a seamless user experience, portability, and data privacy to gain traction in the market. Currently, solutions in space have yet to meet consumer expectations for seamless user experience. During the onboarding experience, a user is proofed and issued an account recovery seed. If a user forgets/misplaces its credentials, they must use their account recovery seed to update their existing credentials. However, if the user forgets their seed, or in some cases, there is a systematic error, there is no mechanism to ensure account recovery.

Consumers of SSI products are interested in portable verified identities between service

providers. This solution would rectify the frustration of managing separate digital identities across entities (Exhibit 10). Additionally, understanding a single source of accreditation standardizes an industry's expectation of assurance and identity.

Exhibit 10

Self-Sovereign Identity: headwinds & tailwinds



Source: Liminal Advisory Services

Tailwinds:

- Higher interest in a decentralized paradigm: as is illustrated later in this report, consumers would embrace the ability to have greater control of where their personal identity data is being shared, and to revoke access where needed.
- Interoperability and portable verified identities: the ability to federate identity via a decentralized system is architecturally far more open to interoperability and scalability than existing centralized paradigms.

Headwinds:

- Lack of seamless user experience, no password recovery flow: SSI products to date have been somewhat proprietary and lack a focus on UX.

Benchmarking Today's Consumer ID Experience

To identify key friction points relating to consumer digital identity today, this section of the report provides insights on how today's consumers are managing their digital identities based on a survey of 1,500 US online consumers conducted by Liminal in July 2021. The survey was designed to benchmark each of the problem statements listed below:

- **Consumers are required to manage a fragmented identity landscape themselves which forces them to adopt identity management practices that are at best risky, and at worst, plain dangerous**
- **Consumers are forced to jump through identity verification and authentication hoops at onboarding and beyond that are cumbersome, often derived from legacy, analog practices that are shoehorned into digital interfaces**
- **Lack of transparency relating to how consumer data is being used and shared is causing consumers to avoid using some platforms and technologies**
- **Consumers are ill-informed when it comes to best practices for protecting their identities**
- **Consumers have considerable, well-founded concerns about becoming victims of identity theft**

Fragmentation

Consumers are required to manage a fragmented identity landscape themselves

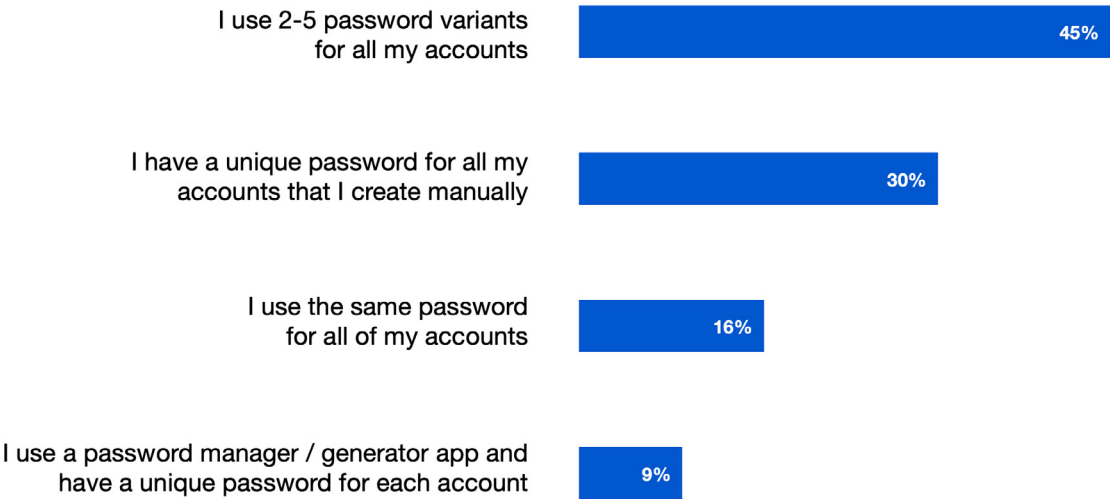
While the identity management industry is evolving quickly to encompass advanced technology such as behavioral biometrics, mobile signals, and AI to reduce fraud and alleviate consumer friction, the use of username/password combinations remains the de facto method for most digital access to the present day. The reasons for the tenacity of the password are simple – it's a technique as old as the internet, easily understood, and ubiquitous for consumers. Unfortunately, it is also at the epicenter of fraud and cybersecurity risk today.

The average consumer has to manage 100 or more online accounts which represents an unfeasible number of unique passwords to create and remember manually.¹⁰ As a result of this, consumers most commonly settle on 2-5 variations of the same password – 45% of US consumers follow this practice for password management today, while 30% state that they manually create a unique password for every account, 16% use the same password for all accounts, and just 9% use a password generator app to create and manage their passwords (Exhibit 11).

Exhibit 11

Consumer password management strategies expose cybersecurity risk

Question: Which of the following describes how you manage passwords for your online/ mobile accounts?



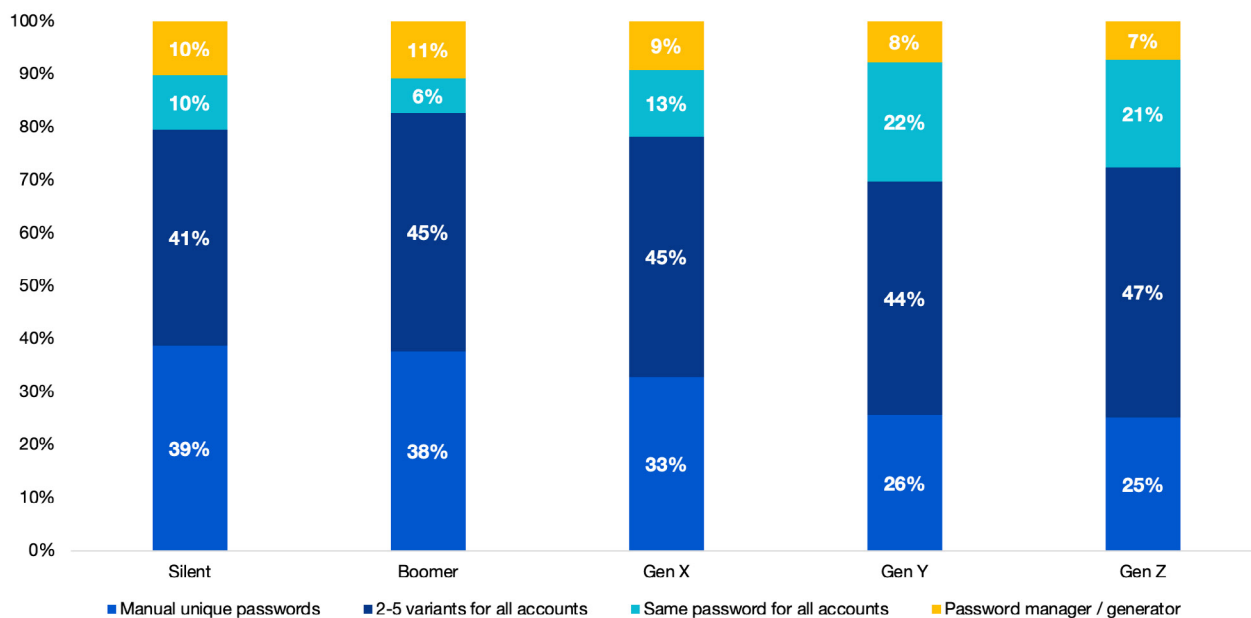
Source: Liminal Consumer Identity Survey

These findings are disturbing on a number of levels, not least that over 60% of consumers are using password management strategies that would mean a breach of a password for one account could provide fraudsters access to multiple other accounts using the same password or similar combinations. While 30% of consumers state that they manually generate a unique password for each online account, the sheer volume of accounts that are required to be managed leads to some skepticism of the honesty of these responses.

Analyzing the data by generation also yielded some concerning findings -- notably that password hygiene is getting worse with younger consumers. Gen Y and Gen Z are less likely to use password managers apps and are more likely to use a single password for all online accounts. In fact, Gen Y is more than twice as likely to use the same password for everything as Gen X, and three times more likely than Boomers (Exhibit 12).

Exhibit 12

Consumer password management behavior by age group, % of respondents



Source: Liminal Consumer Identity Survey

The key takeaways here – a significant majority of consumers are engaging in password management activities that are fundamentally insecure, and younger generations are either less concerned or in a state of apathy that their actions would have any reasonable impact in today's era of chronic data breach fatigue.

Friction

Consumers are forced to jump through identity verification and authentication hoops

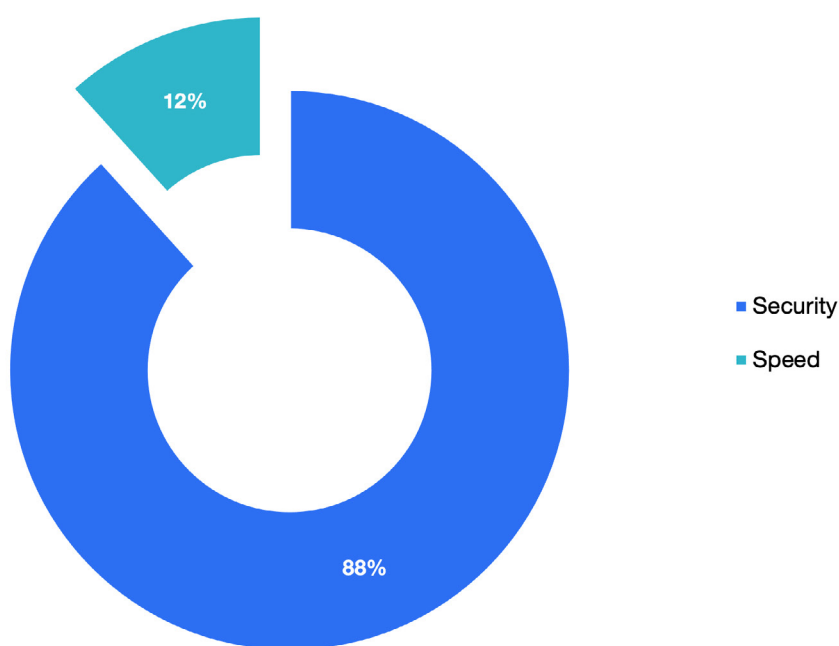
One of the fundamental questions that identity professionals are faced with is how to find the “goldilocks zone” of just the right level of security that will mitigate fraud and provide end-users with an assurance of protection, but not so much as to demonstrably slow down access to digital services.

On the surface, consumers are more concerned about security than speed when it comes to accessing online services – 88% specified security as their greatest priority, with just 12% specifying speed (Exhibit 13).

Exhibit 13

Recent consumer sentiment prioritizes security over the speed of accessibility

Question: What is your priority when it comes to accessing an online service such as banking or shopping: speed or security?



Source: Liminal Consumer Identity Survey

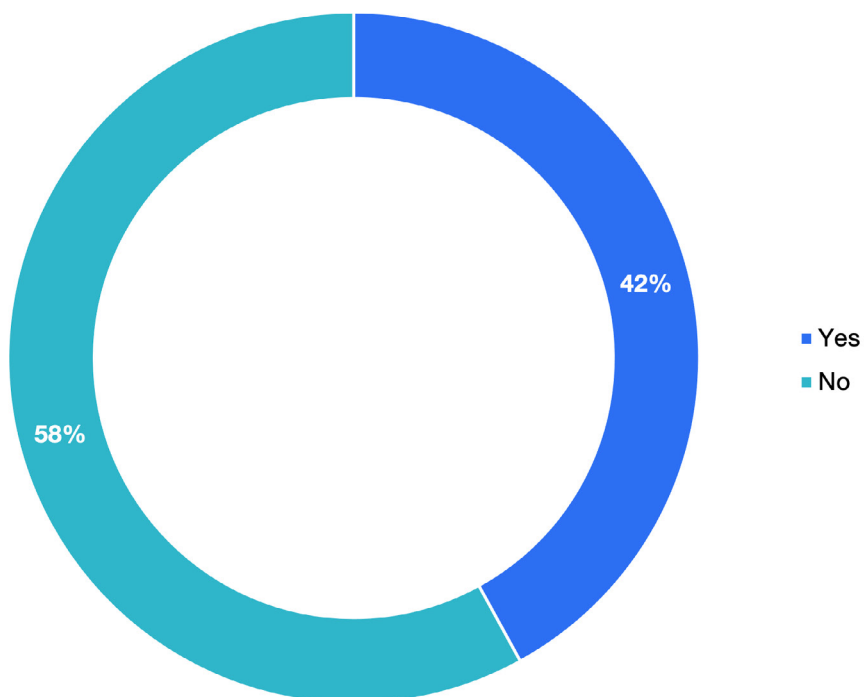
However, consumer tolerance for cumbersome identity verification and authentication processes is finite. This is particularly true for digital account opening.

Invariably, any form of financial account opening requires identity verification to meet regulatory requirements for AML and KYC, and this has traditionally been met with the provision of physical proof such as a passport or driver's license. While this process made sense in the era of in-person banking, in a digital-first age, this is a considerable speed bump – 42% of consumers have abandoned an online or mobile account application due to problems (Exhibit 14).

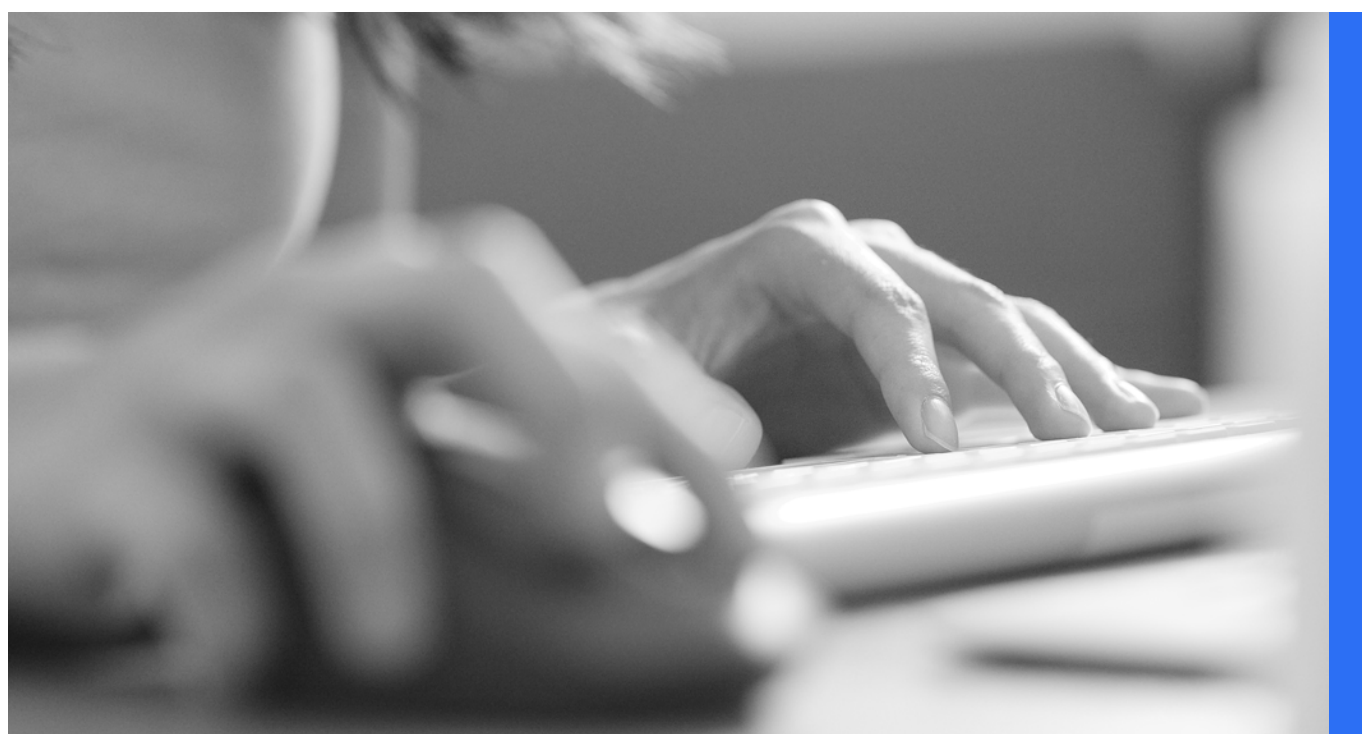
Exhibit 14

Consumer tolerance for friction in digital onboarding processes

Question: Have you ever given up on an online or mobile account application process such as a bank account or car loan application because of problems completing the application?



Source: Liminal Consumer Identity Survey

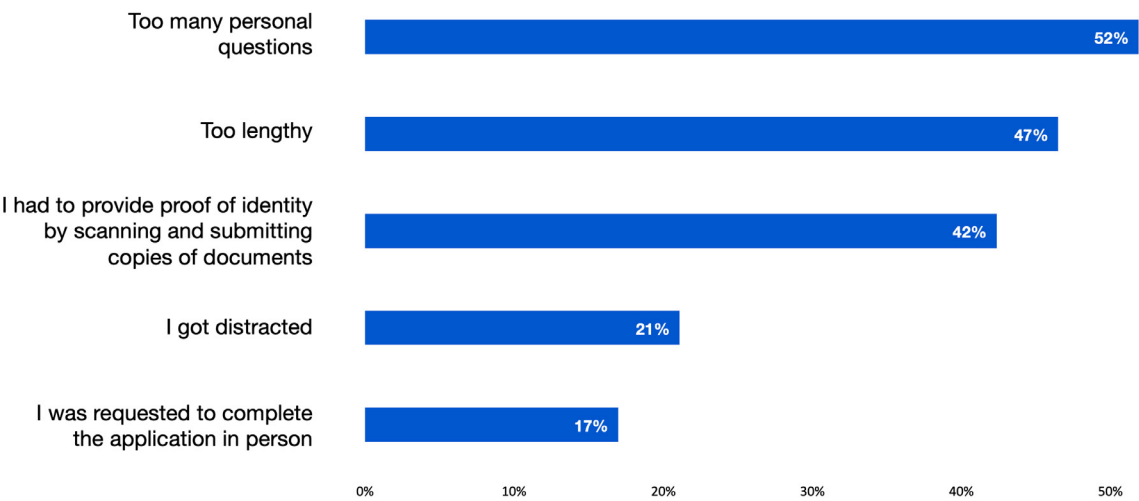


Some of these reasons may be unavoidable. For instance, some regulatory requirements around AML and KYC mean that long-form, intrusive questions are inevitable. However, some reasons for abandonment could be alleviated with technology. For instance, Electronic identity verification (eIDV) solutions offer a technological means of reducing legacy documentation requirements causing other forms of abandonment. Research by Liminal highlights that not investing in eIDV is a significant false economy in terms of lost revenues from loyal customers – in a financial services context, one dollar spent on eIDV is worth \$412 generated in customer lifetime value.¹¹

Exhibit 15

Additional friction built into digital account opening can lead to consumer abandonment

Question: Why did you abandon the application process?



Note: % of respondents based on whether a consumer has previously abandoned an online application process (n = 630)
Source: Liminal Consumer Identity Survey

Opacity

Lack of transparency relating to how consumer data is being used and shared is causing consumers to avoid using some platforms and technologies

A pervasive industry issue is that apps and services are often intentionally opaque when it comes to terms and conditions, with long legal jargon for consumers to accept and well-hidden information pertaining to what information is collected and shared with third parties. This obfuscation came to the surface with the 2018 Facebook / Cambridge Analytica scandal, when there was widespread outrage relating to how personal data was being improperly used to build voter profiles.¹² While this event may have passed and consumer outrage has largely abated, consumers still express significant concerns relating to how their data is being harvested and utilized.

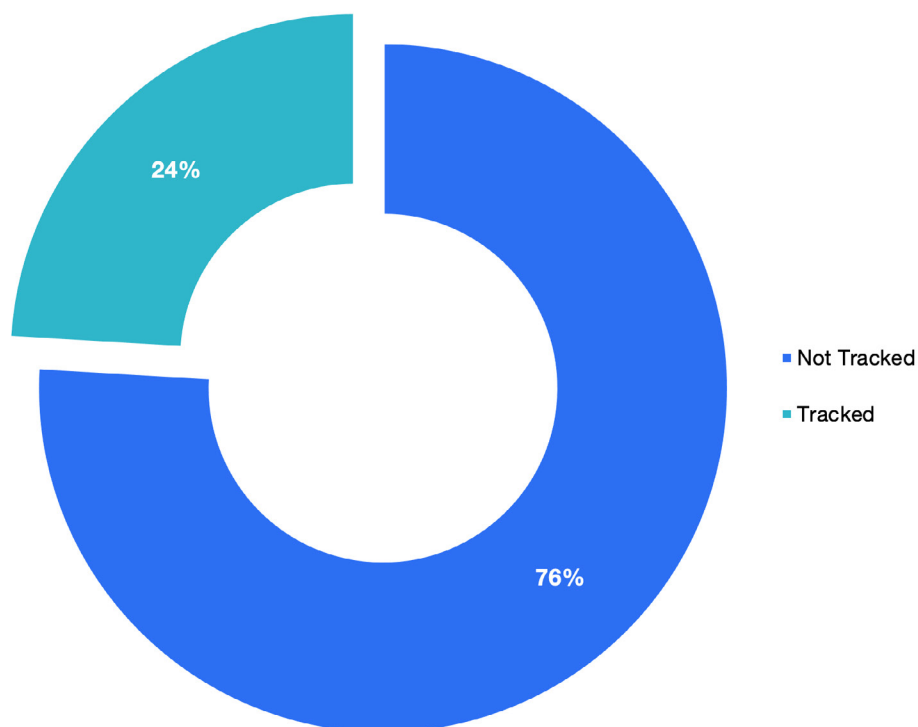
Smartphone OS developers have provided a more privacy centric approach to third-party permissions in recent months. As of April 2021, Apple iOS users were given the option to choose whether their data can be shared by app developers to third parties to track advertising or other data brokering services.¹³ Google's Android OS currently does not offer this service, but plans to do so later in 2021.¹⁴

Of Apple device owners that are aware of this feature, three quarters opt not to be tracked (Exhibit 16).

Exhibit 16

Smartphone owners value privacy, indicate their preference to not be tracked

Question: You may have recently been notified by a mobile app that you can request that you are not tracked across other apps. Do you typically ask to be tracked or not to be tracked?



Note: % of respondents based on whether they were previously aware that a tracking vs. not tracking option exists (n = 1135)

Source: Liminal Consumer Identity Survey

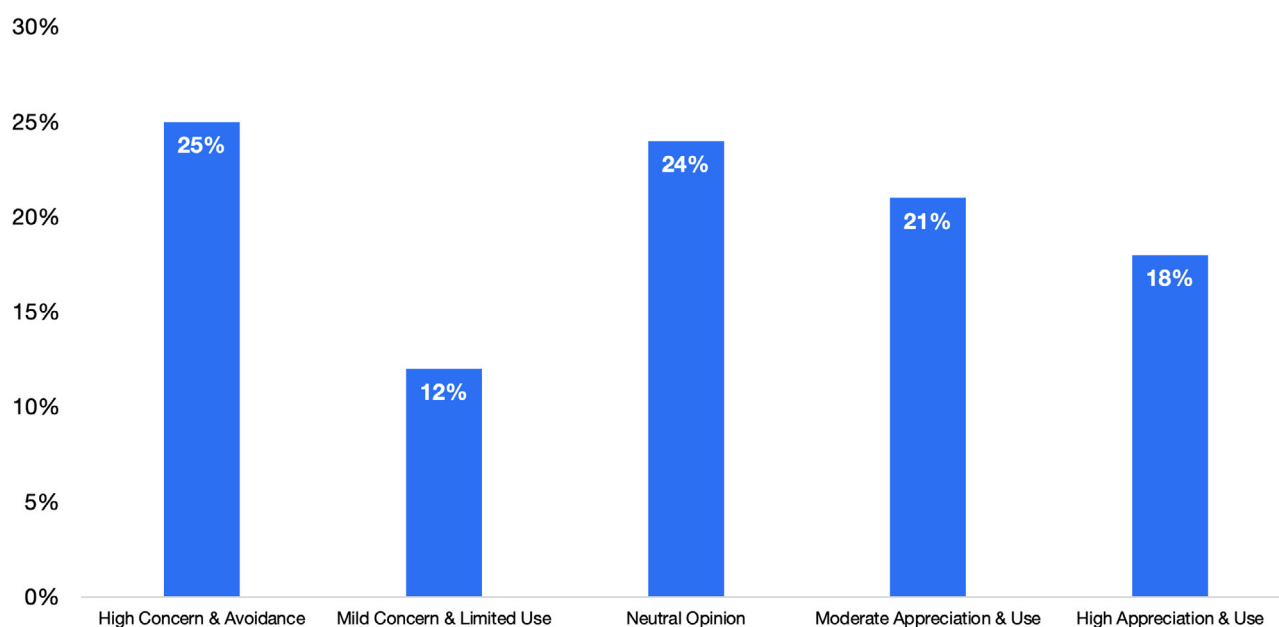
There is also consumer pushback relating to usage of certain authentication technologies. Biometrics are being touted as a solution to the inherent vulnerabilities of passwords and other deterministic data, and fingerprint and facial biometric capture are native capabilities on the majority of today's smartphones and tablets. However, there are consumer concerns about privacy that are stifling adoption.

Consumers were asked to rate their usage of biometrics on a security vs. privacy continuum – on one end of the scale, highly appreciating the extra security and using biometrics as often as possible, on the other, highly concerned about privacy implications and intentionally never using them. Responses were polarized – 39% of consumers appreciate the extra security and use them always or often, while 37% are concerned about privacy and use them reluctantly or intentionally not at all. More critically, a quarter of consumers state that they are very concerned about their privacy and intentionally never use biometrics (Exhibit 17).

Exhibit 17

Consumers demonstrate mixed sentiment around the adoption of smartphone biometrics

Question: How do you feel about using smartphone fingerprint scans or selfies to unlock apps such as banking and shopping?



Source: Liminal Consumer Identity Survey

That there is this degree of interest in greater control of digital identities telegraphs a significant need for stakeholders in the identity management industry to do a better job in articulating how technologies and platforms operate, what data is being captured, and how it is being used.

Knowledge

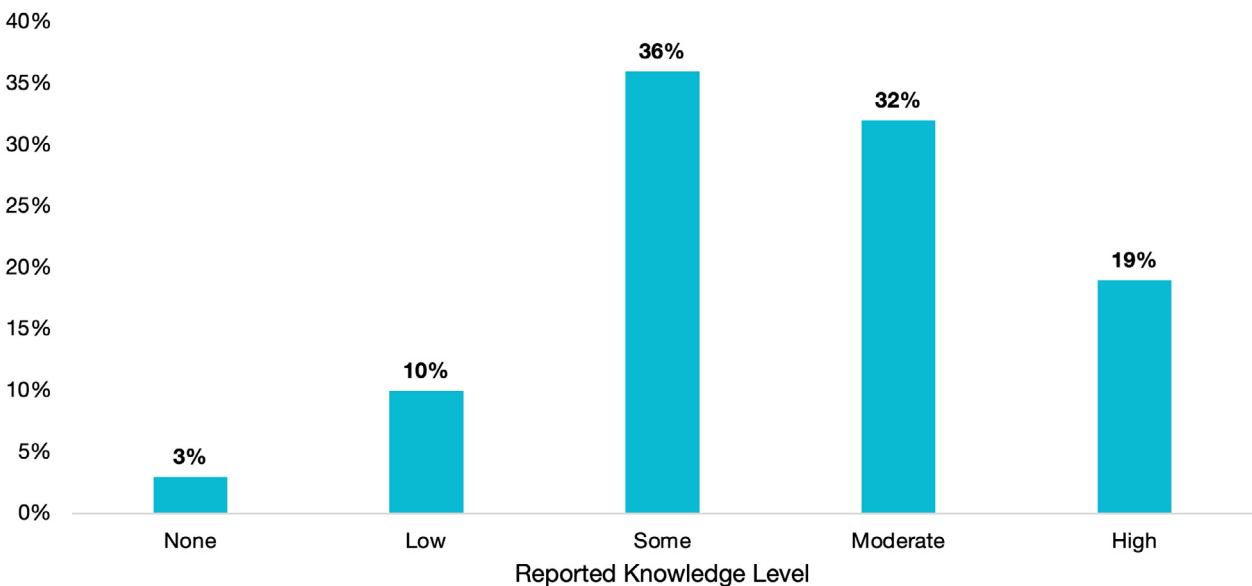
Consumers are ill-informed when it comes to best practices for protecting their identities

Quantifying knowledge relative to identity security is subjective; over half of consumers consider themselves to be knowledgeable or very knowledgeable when it comes to protecting their identity online (Exhibit 18).

Exhibit 18

Consumers consider themselves knowledgeable in protecting their identity online

Question: How knowledgeable do you think you are about protecting your identity online?

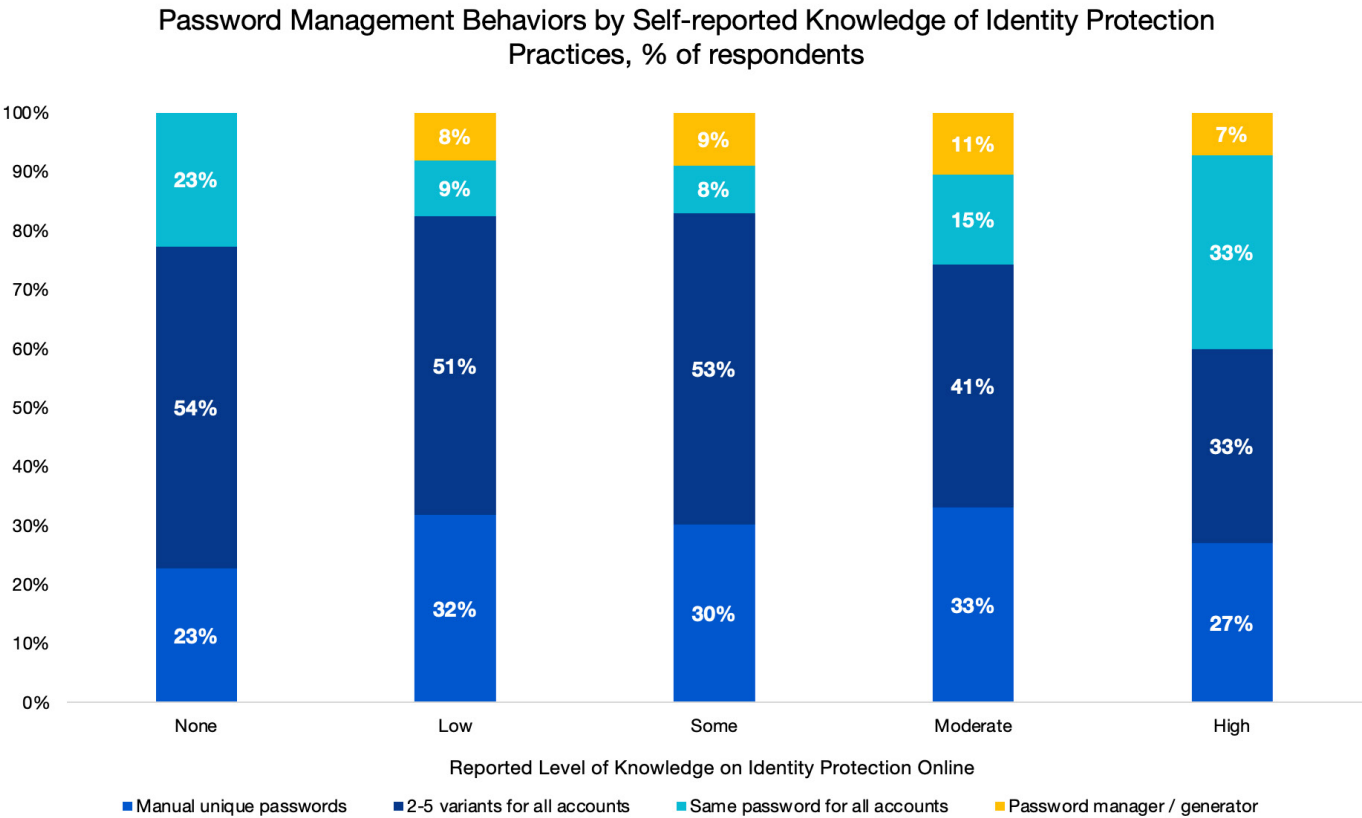


Source: Liminal Consumer Identity Survey

However, the activities of consumers point to the contrary. When cross-referencing consumer knowledge with password management activity, we can see that risky behavior isn't just being undertaken by those professing the least knowledge; a third of consumers that rate themselves as "highly knowledgeable" use the same password for all online accounts (Exhibit 19).

Exhibit 19

Consumers who rate themselves knowledgeable about online identity protection practices demonstrate behaviors that indicate an education gap



Source: Liminal Consumer Identity Survey

A similar pattern occurs in consumer attitudes toward biometrics – as “knowledge” of identity security best practices increases, there is an increase in both the willingness to use biometrics, but also an increase in the dedicated aversion to them – 30% of “highly knowledgeable” consumers actively use biometrics whenever they can, but 30% also actively avoid using them due to privacy concerns.

There is clearly a significant disconnect between perceived knowledge of identity security and basic identity security practices that knowledgeable individuals should be undertaking.

Fear

Consumers have considerable, well-founded concerns about becoming victims of identity theft

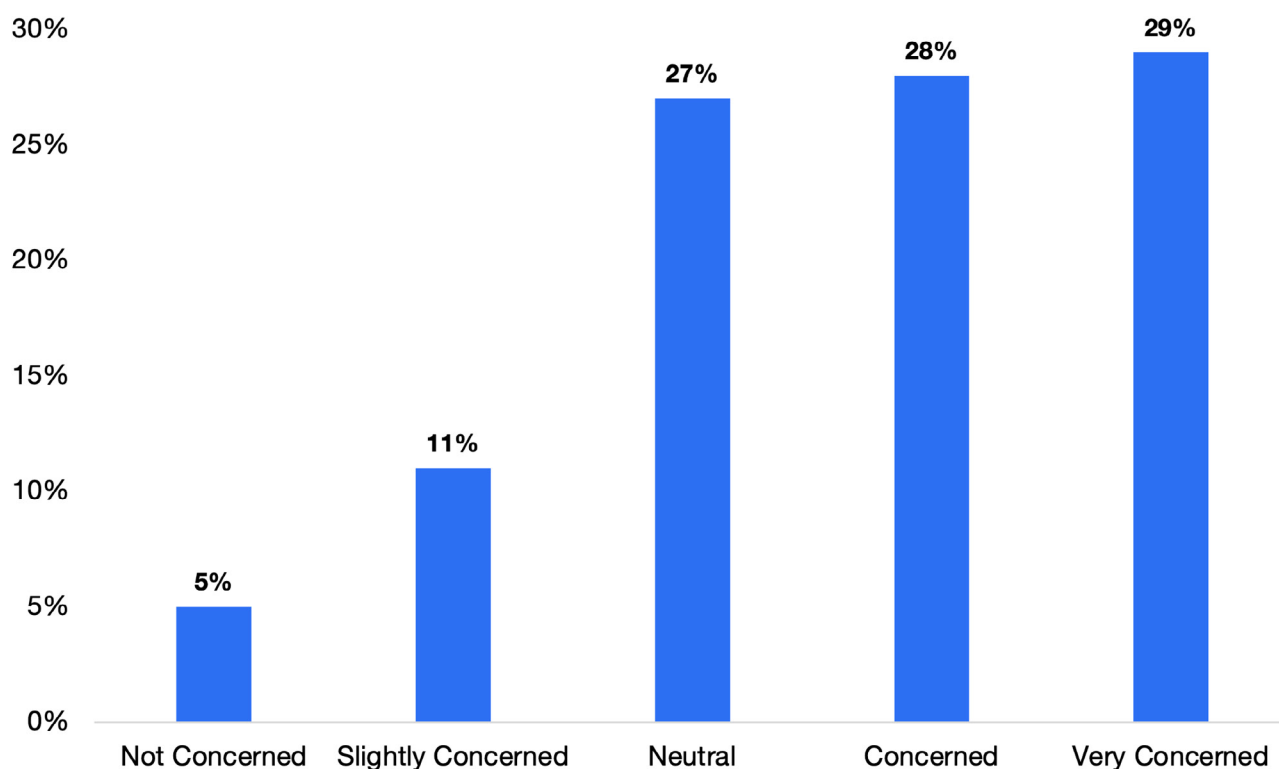
One significant area of concern for consumers pertains to identity theft, and this is understandable. 2020 presented a golden opportunity for fraudsters to further hone their craft, with a pandemic driving digital adoption, an abundance of naive digital consumers to defraud, and deep troves of government funding schemes to exploit. According to the Federal Trade Commission, there were nearly 2.2 million identity fraud reports in 2020, totaling over \$3.3 billion in losses.¹⁵

Consumers articulated their concerns about identity theft – 46% responded that they were concerned or very concerned about identity theft happening to them, with just 15% being unconcerned or very unconcerned (Exhibit 20).

Exhibit 20

Consumers generally express concern that identity theft is a real threat

Question: How concerned are you that identity theft will happen to you?



Source: Liminal Consumer Identity Survey

These concerns are well-founded – there is approximately a one in ten chance that identity theft will happen to consumers.

Moving to Personal Identity Ecosystems

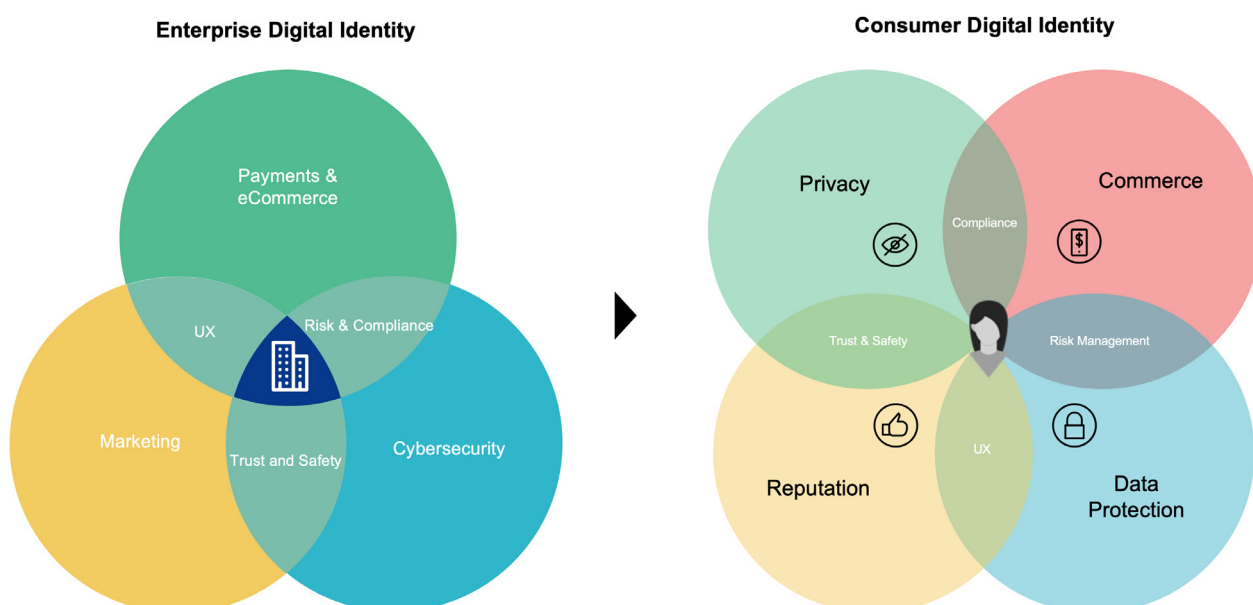
Today's consumer is burdened with managing dozens of one-to-one relationships with service providers and, as a result, resorts to their own unique strategy of cybersecurity hygiene -- one that is likely to err on the side of convenience over security, despite probable good intentions to do the right thing.

This is through no fault of their own -- breach fatigue, an inability to directly correlate insecure actions with cybersecurity consequences, and an industry that has adopted a culture of obfuscation when it comes to the usage and distribution of PII, has got us to this point. Consumer identity management has been allowed to get out of control, and now there is a significant cybersecurity debt burden that needs to be reclaimed.

From an identity architecture standpoint, the one-to-one relationship of consumer to account needs to be redesigned. These singular relationships are made by service providers on behalf of customers, yet, with a cumbersome verification and authentication process for each, user friction is exacerbated. If there were a layer between the consumer and the institution the whole process could be simplified.

Exhibit 21

Evolution of digital entity for the enterprise to consumer digital identity



Source: Liminal Advisory Services

Unlocking the current one to one marketplace will require the development of Personal Identity Ecosystems (PIEs) as the connective tissue between consumers and service providers, streamlining four consumer identity traits that are fundamentally important to them (Exhibit 21):

Privacy: the consumer's ability and right to own, control, restrict, remove and protect their digital identity. These are fundamental traits at the core of digital identity wallets and self sovereign identity initiatives.

Commerce: the consumer's ability to leverage services to initiate online transactions and payments.

Reputation: the consumer's ability to manage their online presence and information about them.

Data protection: the consumer's ability and right to protect their data, systems, devices and digital identity from fraudsters and thieves

These traits are foundational to building trust in the burgeoning digital identity landscape. A critical first step will be the development of digital identity wallets, as trusted and robust means of storing and disseminating identity credentials.

Developing Digital Identity Wallets

While digital wallets have been available for many years as a means of storing virtual payment cards, the analogy to traditional wallets largely ends there. To replicate a physical wallet, there would need to be a means for secure storage of other credentials such as a driver's license and healthcare/vaccination records, and travel documentation such as permanent resident cards and passports. A digital wallet with these capabilities would provide conclusive evidence of identity attributes including the owner's age, country of residence, and medical history, theoretically enabling use cases such as proof of residency and access to age-restricted products and services, as well as actions requiring high assurance like travel and proving eligibility to vote.

From a private sector standpoint, there are a plethora of apps in the market offering digital wallet capabilities. Big Tech companies and longstanding financial institutions are investing heavily in establishing interoperable, high assurance digital identity solutions. Apple, for instance, is focusing on incorporating digital driver's licenses into its Apple Wallet; the company has the advantage of an existing user base of significant size and ubiquity, as well as a reputation for protecting user privacy. Another notable private competitor is Mastercard, which is supporting a number of digital identity initiatives across the world, particularly in

APAC countries, which are rapidly developing digital identity infrastructure to account for their large populations.

From the public sector, there are also a number of initiatives already underway. Public agencies around the world are implementing initiatives for digital identities, driving the potential for government-developed identity wallets. Many recent initiatives are focused on transitioning from physical, document-based identity infrastructures to digital systems. These platforms rely on identity proofing, especially for relying parties that require higher levels of assurance. In the US, state governments are exploring the viability of digital drivers' licenses, which will allow citizens to hold a digital license on their smartphone and then share their age, photo, address, or any other piece of information standard on a license. In the EU, countries continue to create identity wallets for access to public services; to date, there are more than 20 countries with electronic identities (eIDs).¹⁶

Even in countries with established eIDs and digital services, governments are continuing to innovate. For example, Estonia is in the process of procuring a new Mobile ID solution by 2022, and a group of private organisations in Finland are planning to introduce a new digital credential and ecosystem, SisulD.¹⁷ To combat the disparate security mechanisms, differing philosophies, and limited cross-border usability of the various eID schemes, the EU Commission released a digital identity proposal in June 2021 that would create a cross-border framework and identity wallets to issue trusted and secure digital identities for all EU citizens, residents, and businesses.¹⁸ In Singapore, SingPass is a government-provided digital identity that allows citizens to access public services and private businesses with their smartphones.

Market Drivers for Digital Wallet Adoption

Consumer Appetite

To gauge appetite for digital identity wallet functions, consumers were asked to rate on a 1-5 scale (1 = very unlikely, 5 = very likely) their likelihood of performing a number of activities on their smartphones if they were able to do so. These included:

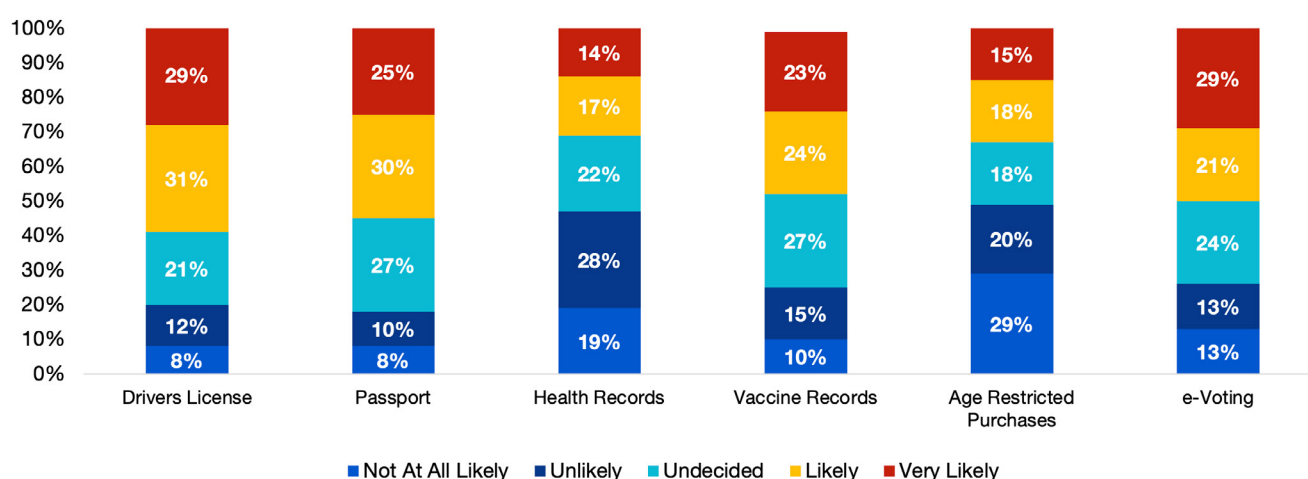
- **Storing a digital copy of their driver's license**
- **Storing a digital copy of their passport**
- **Storing their healthcare records**
- **Storing their vaccination history**
- **Purchasing age-restricted goods/services (alcohol, tobacco, firearms, marijuana)**
- **Voting in a national election**

Storage of driver's license and passport were considered the most likely activities that consumers would perform – 60% of consumers were likely or very likely to store their driver's license on their phone, and 55% were likely or very likely to store their passports. However, the ability to vote in a national election via smartphone was also seen as an attractive capability, with half of survey respondents expressing that they would be likely or very likely to do so if this was possible. Respondents were also relatively comfortable with storing vaccination records on their mobile devices – 47% of respondents were likely or very likely to do so (Exhibit 22).

Exhibit 22

Likelihood for consumers to adopt smartphone-enabled consumer digital identity services

Question: Irrespective of current local or federal laws, how likely would you be to access or perform each of these activities on a smartphone?



Source: Liminal Consumer Identity Survey

These findings augur well for the future of digital identity wallets. Consumers are largely comfortable with the prospect of digital equivalents to their driver's license, passport, and vaccination records stored on a smartphone, and are even prepared to go as far as trusting digital wallets for democracy. Notably, they are less comfortable with the storage of healthcare records and making age-restricted purchases – both private sector activities. This could indicate an adoption advantage for public sector digital wallet initiatives over private-sector equivalents.

That early initiatives for digital wallet functions are focusing on mobile drivers licenses is also telling – service providers realize that trust needs to be built with lower risk functions that consumers are already familiar with before moving to higher risk functions that are more prone to disinformation and political polarization. Carrying a driver's license in a wallet is commonplace, storing healthcare records and voting are not. Apple, for instance, is focusing on digital driver's licenses as the first step beyond payment and loyalty card storage in the ApplePay Wallet.

Age Verification Regulation

An area that is the subject of increased attention, and a potential catalyst for digital wallet growth, is age verification. With children spending more time online in the home, there are growing concerns relating to access to age-restricted content and services.

One specific regulatory requirement from the UK is having a significant impact on how service providers are handling age verification – the Age Appropriate Design Code (AADC).¹⁹ While it is not actually a new law, but simply a clarification on how GDPR is to be enforced, it does extend the regulators' reach beyond the basic protection of children's personal data into how children's digital experiences are designed. AADC makes clear that companies can't be in compliance with GDPR if they use personal data in ways that don't have the best interests of their potential child users in mind. It extends privacy protections to:

- Children up to 18 years old
- Not only services aimed at children, but those likely to be used by them;
- The passive collection of data by connected devices (such as voice assistants or toys);
- 'Inferred data', such as that created by ad targeting platforms
- Any company with operations in the UK, any non-EEA company with users in the UK, and – post-Brexit – any EEA company with users in the UK

Non-compliance is punitive – if an organization is not compliant with AADC, it is likely to be considered in breach of the European General Data Protection Regulation (GDPR) and exposed to fines of up to €20 million, or 4% of annual worldwide turnover, whichever is higher. While AADC is regional, it is expected to be received as a template for other developing regulatory standards around age verification, as was the case with Europe's General Data Protection Regulation (GDPR) and data privacy.

COVID-19 Vaccination Proof

As the COVID-19 pandemic has demonstrated, there is a clear and present need for trusted proof that an individual is free from infection and/or has received accredited vaccination. Businesses and public sector entities are exploring methods to enable safe and secure physical access. Many countries worldwide authorized the adoption of contactless biometric solutions at airports and border crossings and began piloting digital immunity passports. In partnership with Hawaii's Safe Travels program, CLEAR is enabling travelers to use their CLEAR Health Pass to confirm vaccination or negative test results to skip quarantine

measures.²⁰ The private sector is leveraging digital credentials to ensure public safety as well – some businesses are accepting or requiring digital proof of vaccination for access. In New York state, the Excelsior Pass is digital proof of COVID-19 vaccination or negative test results that is accepted by participating businesses and agencies.²¹ In Europe, EU citizens can use their verified Digital COVID-19 Certificate as proof of vaccination, negative test result, or COVID-19 recovery in all EU countries.²²

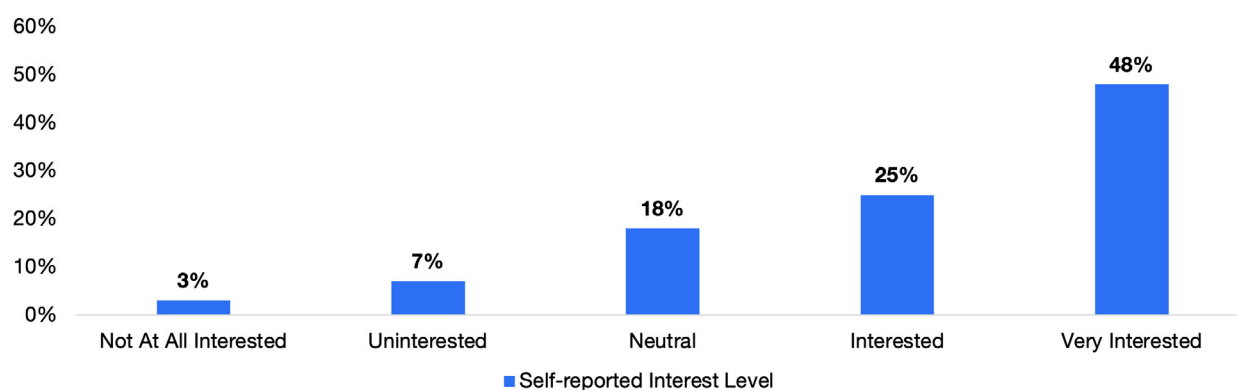
Self-Sovereign Identity

Consumers want greater control over their digital identities – three-quarters are interested or very interested in having the ability to control which companies get to see and share their digital identity, and to revoke access at any time (Exhibit 23).

Exhibit 23

Consumers demonstrate interest in having more autonomy over their digital identity

Question: How interested are you in having the ability to control which companies get to see and share your digital identity, including the ability to revoke access at any time?



Source: Liminal Consumer Identity Survey

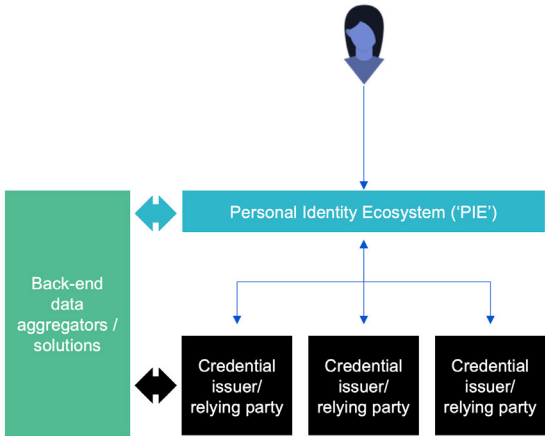

This desire for consumer control of where PII is shared may become a reality with Self-Sovereign Identity. Self-sovereign identity (SSI) is a decentralized system that provides consumers with the ability to own, maintain, and share their identity credentials with relying parties. The decentralized, interoperable, privacy-preserving credentials limit the business risk of maintaining vulnerable data lakes while also providing individuals with additional control over their personally identifiable information. SSI has struggled to gain traction due to lack of adoption by both users and organizations, and also due to the technical complexities associated with blockchain. However, the foundational philosophy and principles of SSI are a significant driver for the development of identity wallets by both private and public entities in order to provide greater control and transparency for consumers.

Building Personal Identity Ecosystems

Educating consumers, adopting greater data transparency, and focusing on streamlining verification and authentication user experiences will alleviate surface issues, but these are all symptoms of a deeper sickness – today’s identity ecosystem is built on one-to-one identity relationships between consumers and service providers, and that is no longer sustainable.

Personal Identity Ecosystems (PIEs) build on the attributes of digital identity wallets and self-sovereign identity to enable collectives that will facilitate the enablement of one to many and many to many relationships between consumers and service providers.

Exhibit 24
Opportunity for companies to disrupt the status quo by simplifying the relationship between consumers and their digital identities

Potential Future State	Description	Example Use Cases/Companies
	<p>Consumers engage with consumer services through a single front-end interface</p> <p>Consumers capture and manage identity attributes in one consumer-side, unique repository (e.g., an 'identity wallet')</p> <p>Businesses/organizations rely upon data provided directly by the consumer and furnish credentials directly to the consumer's front-end 'layer'</p>	<ul style="list-style-type: none">BankingeCommerceTravelGaming <p>Potential PIE Players</p>  <ul style="list-style-type: none">Retail companiesGovernment servicesConsumer cloud service accountsOther consumer services

Source: Liminal Advisory Services

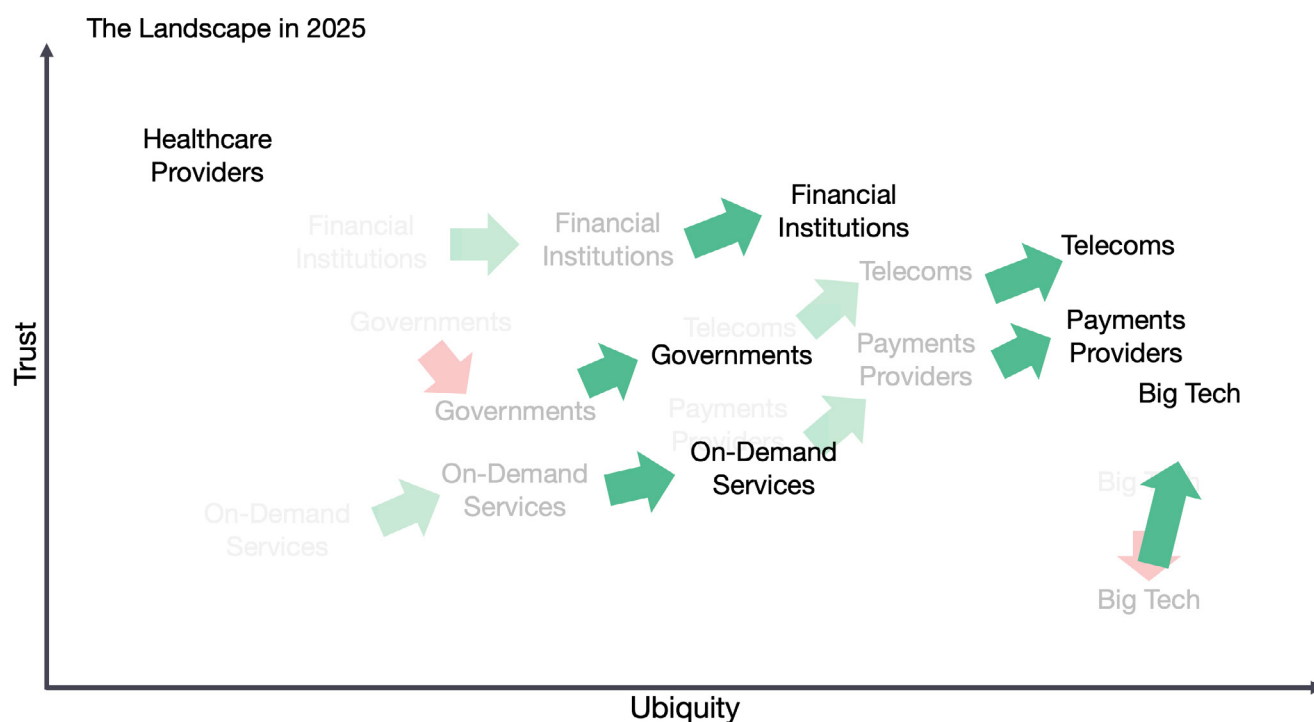
What is significant here is that companies upon which consumers already rely for cybersecurity and identity protection have no advantage over companies that have previously had little involvement in the identity space. Providers of antivirus and identity theft protection fulfill a role in mitigating cyber risk, but the attributes that will make PIEs successful are likely to be strong consumer adoption, a CX-first attitude, and, most importantly, consumer trust.

This last attribute is hard to quantify – trust is a highly subjective term. Further, the attribute of trust is fragile – one single bad incident could ruin consumer trust permanently.

While there are numerous candidates to become PIEs, the attributes that are most likely to engender consumer adoption are industries that are currently onboarding users for high assurance and/or regulated use cases (Exhibit 25). These include financial institutions, payment providers, telcos, and big tech. As highlighted, there are already notable PIE plays from big tech companies such as Apple and Microsoft, to payment card networks such as Mastercard, to government and regional eID providers such as the European Union.

Exhibit 25

In the future, industries onboarding users for high assurance / regulated use cases have the biggest opportunity to play a critical role in new digital-first markets

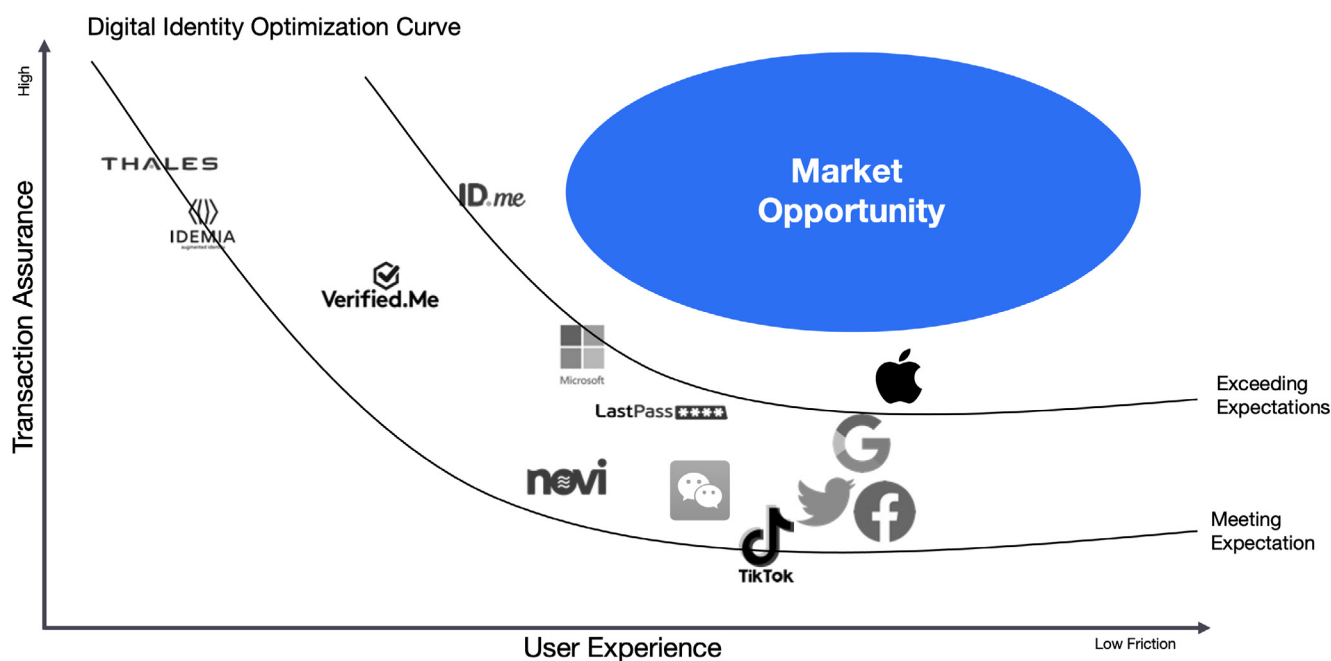


Source: Liminal Advisory Services

The market opportunity for PIEs is most apparent for organizations that can excel in meeting the sweet spot of high transaction assurance combined with low levels of user friction. To date, expectations have been met by companies that have focused on identity federation, such as social networks, and companies that have focused on verification and authentication, but the organizations that have exceeded expectations in both areas remain scarce.

Exhibit 26

Personal identity ecosystems with strong consumer brands are leveraging their position to increase transaction assurance by adding use cases, such as payments



Note – The chart depicts example industry players.

Source: Liminal Advisory Services

Getting from where we are today will not occur easily or quickly, but this evolution is necessary to resolve today's identity management challenges. With an increasing reliance on online services to meet changing patterns to life and work, digital identity management will play an increasingly important role at the hub of our daily lives.

A fundamental first step will be charting a course that will actively recalibrate the industry towards building and relying on trusted personal identity ecosystems, which will only be possible if consumers are shown the value of the fusion of physical identities and digital personas. Identity companies partnering with trusted brands are well positioned to be the provider of choice for identity federation in the future.

Appendix

Antivirus

- Antivirus software runs in the background and works as a gatekeeper to prevent, detect, and remove viruses and malware that put identity data at risk.
- Antivirus goes beyond protecting computers and extends across smartphones, tablets, and IoT devices to prevent social engineering techniques, advanced persistent threat (APT), and botnet Distributed Denial-of-Service (DDoS) attacks.

Consumer Identity Theft Protection

- Consumer identity theft protection solutions monitor personal data for anomalies (e.g., social security numbers, credit card accounts) and provide paths for identity restoration in the event of theft.
- Identity theft services include reimbursement options and legal support to help undo any damage incurred to credit, reputation, or fiscal standing due to identity theft. These are often sold as a component of a larger bundle of cybersecurity services such as antivirus, as well as insurance for physical items such as home and auto.

Identity Wallets

- Identity wallets are smartphone-enabled applications that manage digital identity credential sharing for in-person and online interactions.
- Identity wallets are used by consumers to control what personal information is shared, when, and with whom.
- Due to the fragmented competitive landscape and uncertain guidance about the validity of digital credentials, the identity wallet segment is still emerging and adoption is relatively limited, especially when compared to traditional identity documents such as driver's licenses and passports.
- However, with the continued proliferation of smartphone usage, particularly following the digitization caused by COVID-19, both private and public entities are focusing on becoming the predominant provider of a widely accepted and adopted identity wallet in a segment without a clear forerunner.

Password Managers

- Password managers help customers generate and store secure passwords so that individuals only have to memorize a single, master password. Password managers help enterprises set organization-wide password policies.
- Password managers encourage the use of unique and strong passwords, preventing

password leaks.

- Password managers currently struggle with adoption, facing hurdles such as low consumer awareness and lack of trust. The current deprecation of passwords may also present an obstacle for password managers, requiring password managers to innovate and adapt. Possible replacements for passwords include biometric authentication.

Self Sovereign Identity

- Self Sovereign Identity (SSI) is a lifetime portable identity for any person, organization, or thing that does not depend on any centralized authority and is irrevocable. In SSI, a user controls its own data, it controls when and how it is provided to others, and when it is shared, it is done in a trusted way. The transfer of trusted information is done with cryptographic certainty because of blockchain technology.
- SSI has been in the market since 2015. Still, it has not been able to gain wide adoption due to the increase in friction and technical difficulties – customers want seamless user experience, portability, and data privacy to gain traction in the market. Currently, solutions in space have yet to meet seamless user experience as it requires technical knowledge to get the identity wallet and verifiable credentials set up. Additionally, large entities or governments could adopt SSI solutions leading the way for widespread adoption. However, the user experience needs to be improved to incorporate any user with any technical background.

About Us

LIMINAL

Liminal is a boutique strategy advisory firm serving digital identity, fintech, and cybersecurity clients, and the private equity and venture capital community. Since 2016, we have offered objective, high impact strategic advice, and analytical services, helping to support clients in crucial business decisions at all stages of the product and business lifecycle. We've advised many of the world's most innovative business leaders, investors, and government officials on building, buying, and investing in the next generation of integrated digital identity platforms and technologies. As a result, our clients trust us to set strategic direction in light of radically evolving ecosystem dynamics, pursue new growth strategies, capitalize on M&A opportunities, and optimize deal flow. We see the solutions to these complex digital challenges not as a 'what' but as a 'how.' We don't just tell you about the destination, we show you how to get there.

Learn More at www.liminal.co

Endnotes

1. Schrage, M. "Why User Experience Always Has to Come First." Harvard Business Review, September 2016. <https://hbr.org/2016/09/why-user-experience-always-has-to-come-first>.
2. Liminal. "Digital Identity Landscape." September, 2021. <https://oneworldidentity.com/2021-digital-identity-landscape/>.
3. Bassett, Hylender, Langlois, Pinto, Widup. "Data Breach Investigations Report." Verizon, 2020. <https://enterprise.verizon.com/resources/reports/dbir/>.
4. One World Identity. "The Ten Commandments for Data Management: Personal Data Management Fundamentals." June 2018.
5. U.S. GAO. "Range of Consumer Risks Highlights Limitations of Identity Theft Services." GAO-19-230, March 2019. <https://www.gao.gov/assets/700/697985.pdf>.
6. Bassett, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S. "2020 Data Breach Investigation." Verizon, 2020, <https://enterprise.verizon.com/resources/reports/dbir/>.
7. TraceSecurity.org "81% of Company Data Breaches Due to Poor Passwords." TraceSecurity.org, August 14, 2018, <https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords>
8. Security.org "Digital Privacy Risks Increase As Americans Stay-at-Home." Security.org., April 6, 2020, <https://www.security.org/resources/digital-privacy-telecommuting/>.
9. Europa.EU. "Commission proposes a trusted and secure Digital Identity for all Europeans." June 3, 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.
10. Turner, Jack. "Average Person Has 100 Passwords." Tech.co, October 20, 2020. <https://tech.co/news/average-person-100-passwords>.
11. Liminal. "Winning the Financial Services Onboarding Battle by Repositioning eIDV ROI." July 13, 2021. <https://liminal.co/reports/winning-the-financial-services-onboarding-battle-by-repositioning-eidv-roi/>.
12. Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." New York Times, April 4, 2018. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.
13. Apple. "App Tracking Transparency." 2021. <https://support.apple.com/en-us/HT212025>
14. Google. "Advertising ID." Android, 2021. <https://support.google.com/googleplay/android-developer/answer/6048248#zippy=%2Chow-to-opt-out-of-personalized-ads>.
15. Federal Trade Commission. "Consumer Sentinel Network Data Book." February 2021. <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020>.
16. European Commission. "What is eID?" July 28, 2021. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID>.
17. European Commission. "Approaches to eID in EU Countries." April 22, 2021. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2021/04/14/Approaches+to+eID+in+EU+countries>.
18. European Commission. "Commission proposes a trusted and secure Digital Identity for all Europeans." June 3, 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.
19. Information Commissioner's Office. "Introduction to the Age Appropriate Design Code." 2021. <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.
20. Fox, Allison. "Traveling to Hawaii Just Got Easier Thanks to Clear." Travel and Leisure, July 9, 2021. <https://www.travelandleisure.com/travel-news/clear-health-pass-hawaii>.
21. New York State. "Excelsior Pass." <https://epass.ny.gov/home>.
22. European Commission. "EU Digital COVID Certificate." https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en.