DIGITAL IDENTITY

Technology Evolution · Regulatory Landscape · Forecasts · 2020-2025

Reprint for Experian

www.juniperresearch.com

JUNIPER RESEARCH

First Published Click here to enter publish date

Published by:
Juniper Research Limited,
9 Cedarwood,
Chineham Park,
Basingstoke,
RG24 8WD, UK
UK: Tel +44 (0) 1256 830001/475656
US: Tel +1 408 716 5483
UK : Fax +44 (0) 1256 830093
www.juniperresearch.com
info@juniperresearch.com

Printed in United Kingdom

Report Authors

Nick Maynard & Susan Morrow

Foreword

Juniper Research Limited

Juniper Research is a European based provider of business intelligence. We specialise in providing high quality data and fully-researched analysis to manufacturers, financiers, developers and service/content providers across the communications sector.

Consultancy Services: Juniper Research is fully independent and able to provide unbiased and reliable assessments of markets, technologies and industry players. Our team is drawn from experienced senior managers with proven track records in each of their specialist fields.

Regional Definitions

North America:	Canada, US
Latin America:	Argentina, Aruba, Bahamas, Barbados, Belize, Bolivia, Brazil, Cayman Islands, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, French Guiana, Grenada, Guadeloupe, Guatemala, Guyana, Haiti, Honduras, Jamaica, Martinique, Mexico, Netherlands Antilles, Nicaragua, Panama, Paraguay, Peru, Puerto Rico, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Surinam, Trinidad and Tobago, Turks and Caicos Islands, Uruguay, Venezuela, Virgin Islands.
Western Europe:	Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland UK.
Central & Eastern Europe:	Albania, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Macedonia, Moldova, Poland, Romania, Russia, Serbia/Montenegro, Slovakia, Slovenia, Turkey, Ukraine.
Far East & China:	China, Hong Kong, Japan, Macao, South Korea, Taiwan.
Indian Subcontinent (ISC):	Bangladesh, India, Nepal, Pakistan, Sri Lanka.
Rest of Asia Pacific:	Australia, Brunei, Fiji, New Caledonia, New Zealand, Cambodia, Indonesia, Laos, Malaysia, Maldives, Mongolia, Myanmar, Philippines, Singapore, Thailand, Vietnam.
Africa & Middle East:	Afghanistan, Algeria, Angola, Armenia, Azerbaijan, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo, Cote d'Ivoire, Democratic Republic of Congo, Djibouti, Egypt, Equatorial Guinea, Ethiopia, Gabon, Gambia, Georgia, Ghana, Guinea, Guinea-Bissau, Iran, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Lebanon, Lesotho, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Palestine, Qatar, Reunion, Rwanda, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Swaziland, Syria, Tajikistan, Tunisia, Turkmenistan, Uganda, United Arab Emirates, Uzbekistan, Yemen, Zambia, Zimbabwe

Contents

1. Digital Identity: Connecting to You

1.1 Introduction

The concept of digital identity and how it can be applied has been discussed for many years. These often-philosophical discussions are beginning to crystallise into the 2020s. The concept of digital identity is less about presenting a digital persona and more about sharing verified identifiable data. However, this is not to say that a digital version of 'you' does not have a place in the wide-scale, multi-use ecosystems being built today. With the versatility inherent in many modern identity systems, life events and portable identities take on new meaning.

Digital identity is about much more than creating an online account. Data drives transactions and, more and more, we are seeing a requirement to add weight to justify the use of identifying data. Beyond registration for an identity account, verified data sees a place in post-registration or even non-registered (third-party) verifiable, assured, transactions.

Digital identity systems or 'ID Networks,' are no longer an island; isolated from anything else going on around them. ID Networks are multi-faceted, multi-component ecosystems facilitated via APIs, open standards, and protocols. The players within the expanded ID Network ecosystem are focusing their efforts and fast becoming best-of-breed solutions; adding vital pieces to wider, whole, often extended, API-enabled ecosystems.

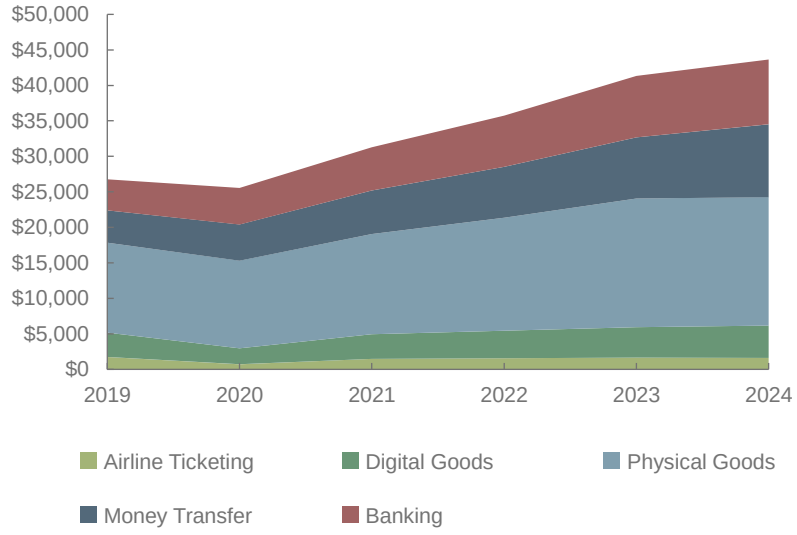
Within this, not layered, but deeply woven, are security and privacy. Digital identity is unique, in that it both needs security and privacy, and at the same time, when done well, enhances security and privacy.

Issues like synthetic identities and other identity-based fraudulent activities have a chance of being tackled by modern robust options in ID that draw in those best-of-breed ID Network components.

Juniper Research estimates that in 2024 over $43 billion will be lost due to online payment fraud (see figure 1.1).

As we carry on into an unknown future, disrupted by the pandemic, this interwoven nature of identity-security-privacy will play a vital part in making sure our internet, workplace, government services, and banking are safe havens.

Figure 1.1: Total Value of Fraudulent Transactions ($m), Split by eCommerce Segment, 2019-2024



Source: Juniper Research

This report will discuss new approaches in the ID space in detail, providing advice and best practice recommendations for their deployment, while also giving an overview of this rapidly growing market.

1.2 Definitions & Scope

Juniper Research considers digital identity to be a digital representation of an entity; this can be one or more individual pieces of identifying data, an event, or a 'signal' such as an assurance indicator and similar, yet to be determined, items defined by the industry; this latter statement is important as ideas such as decentralised identities, IoT identities, robotic IDs, etc. take shape. This data can be used as authorisation signals, grant rights, access or privilege, on the basis of that representation.

1.2.1 Identity Tasks

ID Networks, even decentralised IDs, may be reliant on multiple components, each doing a job within the larger engine of identity. Which of the myriad requirements are applied, and at what point in a user journey, depends on the use case and remit of the ID system. Wider adoption of ID networks requires omnichannel support – facilitated by the re-use of ID verification and authentication to add assurance to transactions. The result is a rich ecosystem of contributing components. Typical tasks in an ID Network include:

- Authentication – A proof of an assertion (i.e., identity data). This is typically done through credentials such as usernames, passwords, PINs or biometrics, single or multiple factors in that authentication process. In addition, rules-based/risk-based authentication has a place in making ID-enabled transactions more granular.
- Authorisation – Association and assertion of rights with a given identity/role/transaction. This is typically done through assigning roles, independent of a given end user. But this can be done at a transaction or device level.
- Verification – Check of an identity or piece of identity data (e.g., an identity document such as a passport).
- Anti-fraud – Increasingly, anti-fraud checks are being used during registration or transactions that have an identity element.
- Attribute Enrichment – If required, additional attributes can be requested from external or internal sources. These may require further verification.
- Rules of Engagement – A rule applied to an identity event (e.g., under condition X, user Y can perform action Z).

1.2.2 Forms of Digital Identity

Juniper Research classifies digital identity under three categories:

- Centralised – Digital identity credentials are held in a single place, and each credential is used for a single purpose.
- Federated – Digital identity credentials are held in a single place, and applied to multiple contexts; allowing a single set of credentials to act for multiple systems.
- Decentralised – Digital identity credentials are typically created and managed directly by the credential owner, and stored in a decentralised manner, e.g., on a mobile device. In our previous report, we placed this

section under ‘self-sovereign identity’ or SSI. Typically, SSI is blockchain enabled; this year, we decided to expand the section to encompass both blockchain and non-blockchain decentralised solutions.

Note: All three categories can be used within a wider ID network.

1.2.3 Digital Identity Technologies

The report will cover the following forms of digital identity verification and authentication technology:

- Verification Services: Services that check an identifier (e.g., identity document checking services, credit reference agency, etc).
- Authentication: Proof of credential(s) to access an identity acccount. For example, biometrics, passwordless, MFA, SSO, adaptive, self-service recovery, etc.
- UI/UX: The way a user interacts with an identity-enabled service, including support for self-service.
- Anti-fraud Services: Performs checks on indiviudal/ transaction to prevent fraudulent activity (e.g., sanction list checks).
- Payments (including Open Banking): Incorporation of payment services for transactions, but also for assurance of identifying data.
- Identity Provisioning and Management: Services that manage, govern, and provision identities, they also handle requests for identity requests.
- Data Orchestration/Hubs: The ‘plumbing’ of the wider ID networks. They offer a number of facilitation functions, such as protocol translation, orchestration of various ecosystem components (e.g., data brokerage).
- Decentralised ID Providers: Offer a decentralised method of managing an identity (e.g., SSI, wallet-based ID, etc).
- Enterprise ID and Non-employee Directories: A way of managing external and internal employees, contractors, freelancers, third parties, fourth parties, etc.

2. Digital Identity Verification

2.1 Market Trends Affecting Digital Identity

The current needs of the digital identity market arise broadly from the condition of the online environment. These will be discussed in this section; detailing how each is shaping the future of digital identity.

2.1.1 The COVID-19 Pandemic, Remote Working, and Access Control

No report on digital identity management in 2020 would be complete without reference to the impact of the COVID-19 pandemic. Companies all over the world have been forced to turn to home working to stay productive. This has created challenges for enterprise IT teams, particularly in the areas of cybersecurity. Cybercriminals have taken advantage of not just extended, but fuzzy, networks where Shadow IT is common. Shadow IT is where systems are deployed by departments other than the central IT department, to work around challenges with centralised systems. This is combined with the now massive variety of devices and networks that users are working on, driven by an explosion in remote working. The advent of the malicious 'remote insider' only adds complexity to the needs of traditional enterprise Identity & Access Management (IAM) systems.

Providing robust and effective access control in an environment that is outside the direct control of the enterprise requires a change in approach. The August 2020 NIST Special Publication 800-207 update on implementing a Zero Trust Architecture (ZTA) defines a process to create an effective ZTA with an emphasis on monitoring, NIST states that[i]:

'When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and best practices, a ZTA can protect against common threats and improve an organisation's security posture by using a managed risk approach.'

On the subject of remote employees NIST says:

'Remote enterprise subjects and assets cannot fully trust their local network connection. Remote subjects should assume that the local (i.e., non-enterprise-owned) network is hostile. Assets should assume that all traffic is being monitored and potentially modified.'

The situation in regard to online consumer accounts has reached a tipping point. Credential management has gone beyond onerous. Dashlane estimates that, on average, a US adult has around 150 online accounts. It is becoming extremely difficult to manage the credentials, usually, a password, required to access these accounts. Coupled with this, many people reuse credentials to avoid remembering multiple passwords. The result is an onslaught of credential stuffing attacks, where fraudsters use stolen credentials to hack into online accounts, there were 88 billion such attacks recorded in 2019.[ii]

This issue is not just a consumer problem. The phenomenon of work from home, coupled with Shadow IT and bring your own device (BYOD), means that the issue of credential stuffing could potentially leak over into enterprise access: users re-using cloud login credentials for personal accounts for convenience.

Federated identity provision, seen in its simplest form, provides the reuse of social provider login federation, as well as in enterprise Software-as-a-Service (SaaS) provision. This is a useful device for

improving usability. Single Sign On (SSO) is sometimes associated with federated login for even easier resource access. Tokenisation is used via standard identity protocols, Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorisation (OAuth).

Federation of identity, or 'identity reuse' can provide a mechanism to reduce the burden of credential management and recall. However, federation has some implicit problems, namely which existing identity providers to support. The use of standard protocols such as OIDC allows easier onboarding of federated ID support. However, some existing ID systems, such as decentralised wallets (see later) may use proprietary standards.

The W3C project, 'Decentralised Identifiers (DIDs) v1.0' is updating this situation by developing the DID standard so that:

'DID methods can also be developed for identifiers registered in federated or centralised identity management systems. Indeed, almost all types of identifier systems can add support for DIDs. This creates an interoperability bridge between the worlds of centralised, federated, and decentralised identifiers.' [iii]

The development of 'hubs' or an orchestration layer, to handle protocol translation, onboarding and offboarding of relying parties and services, and federated identity providers (IDPs), offer a more versatile and manageable way to create federated identity networks.

However, federation in and of itself is not the answer to securing access. The whole system requires other components to verify and check access events. For example, verification of additional attributes may be required. Other checks such as machine-learning based User and Entity Behavioural Analytics (UEBA), Anti-money laundering (AML) checks can also be used to augment identity networks that utilise federation.

2.1.2 API-sation of Identity

Cloud-based identity was hailed as the next big leap into more accessible identity systems. This is not untrue. However, a movement towards a more connected network of identity components is crystallising. This is driven by widely available services and functionality through Application Programming Interfaces (APIs). Opening up functionality via an API provides the mechanism needed to easily connect up important building blocks in identity services. The result is the development of a number of hubs and 'identity (data) orchestration engines' that sit at the heart of identity services. These hubs and engines act to bring disparate components together to facilitate use cases. Some of the more mature orchestration engines offer a mechanism to connect disparate APIs to create ecosystems/ID Networks, based on industry needs/use cases. Identity (data) orchestration is typically controlled using rules that modify behaviour based on the relying party needs. The data orchestration engines can find a fit with a number of use cases in retail, banking, healthcare, and government, as they can draw in from existing functions including federation, open banking, verification services, behavioural monitoring, anti-fraud checking services, etc. The identity (data) orchestration engines are typically capable of performing protocol translation so they can handle many types of existing identity providers to facilitate identity re-use. ID Networks have the potential to draw proprietary solutions, such as ID wallets, into a wider system. 'Bridges' or 'hubs' are being offered by a number of vendors as a method to orchestrate both traditional identity providers and DiD-based self-sovereign wallets. This ability to provide user choice and federation of ID

no matter what source is likely to be a unification authority in a complicated ecosystem that requires emphasis on user-choice.

'The API economy has driven advancement in this space in simplifying the transmission of data. And while there are still technological hurdles to integrate new fraud detection and authentication solutions, the challenge becomes more about how to leverage those solutions in a coherent manner. Aligning risk scores from a diverse set of niche solution providers can cause significant confusion for the business that is attempting to efficiently serve an increasingly demanding customer base, with low friction and low risk. Having APIs to help with the transmission of data still doesn't solve for the need to ensure that the data is valid, authentic, or that the person requesting that the data be shared is authorised to make that request. These become the new concerns in an ecosystem approach to data sharing and transmission.' - David Britton, VP of Industry Solutions, Identity & Fraud Management at Experian[1]

2.1.3 Governments Leading?

A wide variety of countries have tried, failed, or are planning to bring, digital identity to citizens. This will be discussed more fully in section 3, but its effect on the market will be noted here.

The move to a digital government is largely dependent on a mechanism of identifying yourself in an assured manner. The government also has control over a number of identity documents, such as passports. The two should be symbiotic. However, the devil is always in the detail.

Online government services are often the main touchpoint for consumers wishing to connect to local and national governments. These services can be crucial in delivering benefits and tax options. The level of assurance required to transact online with government services is a key requirement of these systems.

In the UK, this same requirement became a blocker for the smooth running of digital government identity. The UK Verify service was a vanguard service that shaped the ideology of digital government. The identities were provisioned by a number of UK brands, including the Post Office, Royal Mail, Experian, and Barclays Bank. The system was based on a SAML 2.0 'hub,' in this case acting as a conduit to the citizen; allowing them to pick a brand to provision their government ID. The level of assurance started off as low (LOA1); allowing a small number of these brands to quickly onboard for the scheme. A second procurement was put out to market but these new IDPs were required to start at an increased level (LOA2), eventually, retro fitting to an LOA1, as the project progressed. Issues with match rates plagued the project, as to achieve an LOA2, users had to be taken through fairly onerous steps to prove their identity; providing identity documents and being asked identifying questions from a number of Credit File Agencies and aggregators at the backend of each IDP. Match rates were low, typically below 50%. Most IDPs left the scheme due to government funding issues; leaving only the Post Office and Digidentity to run the IDPs (note: The Post Office IDP technology is provided by Digitdentity). Match rates for 2020 are around 45% of users successfully being issued an identity.[iv] Of the expected 25 million UK citizen signups, by February 2019, only 3.6 million people had successfully signed up for Verify.[v]

A number of different approaches to digital identity for Government-to-Citizen (G2C) transactions are shaking out. Australia has launched the

[1] Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian in September 2020

MyGovID which is a smartphone-based ID that is based on a granular point system (you can gather up to 100 points to prove your identity).

Card or wallet-based IDs remain popular in a number of countries in the EU, including Estonia, who are innovators in the space.

The Canadian government is active and innovative in the digital identity space. Digital ID & Authentication Council of Canada (DIACC), headed up by Joni Brenan, ex Kantara Initiative, is working toward an interoperable relationship between the public and private sector to build a Canadian digital identification and authentication framework.[vi]

Figure 2.1: Specimen Estonian eID Card

Source: Republic of Estonia Police & Border Guard Board

The US continues to battle with citizen acceptance of a federal identity scheme. This will play out in the coming years.

Citizen identity has the potential to create bridges between consumer and citizen identity. Schemes around borders and airports such as WorldReach's 'Know Your Traveller' app has allowed the successful processing of most of the 3.1 million applications to the UK Home Office EU Settlement Scheme (EUSS).

Government use cases continue to drive certain aspects of the identity market and test the waters around high assurance IDs and consumer usability.

2.1.4 Anti-fraud and Seamless Online Transactions

By 2024, Juniper Research forecasts that fraud detection and prevention software spend will reach $10 billion; showing the importance of leveraging identity for fraud management.

Transaction decoupling from identity can offer an alternative way of delivering identity-driven services without the identity component. Consumers want to perform online tasks (e.g., buy goods, send money, and so on). They do not necessarily want or need a full-blown digital identity to do this. API-based orchestration of data could provide an answer. By removing the identity piece and replacing it with on-the-fly presentation of specific required data, transactions could be made more secure from both ends of the transaction:

- An existing identity account such as a bank can be re-used
- The service gets the data needed to perform the transaction (for example, by calling an Open Banking API)
- The user may need to supply some additional attributes depending on the transaction and service needs, for example, an address, driver's licence

- These data have gone through a Know Your Customer (KYC)/Customer Due Diligence (CDD) process at the bank
- These data can be checked using a third-party verification service (e.g., government checks, CRA, etc.)
- AML checks can be performed on-the-fly
- Nothing needs to be stored
- Data can be tokenised

The driver of online fraud is pushing the market towards fewer online accounts and more data orchestration with checks facilitated by API-enablement of services. This should help improve security and usability.

2.1.5 Consumer Expectations: Ease of Use and Omnichannel Identity

As always in the world of technology, consumer uptake drives any scheme. Usability is a hot topic, especially in relation to diversity challenges in mass-adopted identity systems. All approaches to identity have an underlying need to build a great Customer Experience (CX). Diversity in identity groups like Women in Identity (WID) are pushing for more consideration of diverse groups coverage by ID schemes; WID pushes for ethnic minorities, women, disabled users, etc. to be considered during the design stage. This makes sense when you consider that bias often adversely affects technologies such as facial recognition. Additionally, issues for disabled users in complex verification journeys can lose that customer base. Having an omni-channel approach is a key driver for ID system uptake.

2.2 Current Digital Identity Landscape

The following sub-areas of the digital identity landscape give a flavour of where ID offerings are maturing in the space. One common theme shaking out is a digital identity solution that is progressive and versatile; driven by data and facilitated by technology including APIs, machine learning, and advanced verification services. Customer expectations are also a driver. Simplification of identity services and identity-driven transactions are likely to be the catalyst for success in terms of which identity solution wins out. However, there is a high probability that a more pragmatic approach utilising best-of-breed options incorporated into a fuller ID Network or ecosystem will offer the requirement for many use cases.

2.2.1 Identity Wallets

An ID in a user's pocket is a compelling idea. The use of smartphones to carry out day-to-day life activities has proven highly successful. We use our smartphones for music, contacts, notes, emails, banking, messages, so why not identity? The market for mobile ID/identity wallets has evolved over recent years to bring a number of solutions to the market. A Thales study found that 87% of respondents were 'highly interested' in using a Digital ID Wallet.[vii]

Identity wallets are a form of decentralised identity. Some are based on proprietary protocols, some on standards. Some identity wallets are based on self-sovereign identity (SSI) architecture and are therefore built on a backbone of a blockchain. Some are centralised but with the ethos of user-controlled decentralised actions using a mobile wallet. Evernym's decentralised wallet, Connect.me, uses the Sovrin blockchain.

Connect.me manages all of an individual's verified (and non-verified) identity data from a mobile device. Connect.me supports the privacy-enhanced sharing of these data via a zero-knowledge proof methodology (ZKP).

The digitalisation of ID documents is growing at fast pace, especially with the introduction of new ID wallets which can be point solutions, such as a mobile driver licences, or which can aggregate various documents (digital identity, driver licence, health care credentials, etc.) in a single app.

Another example of mobile identity is CULedger's MyCUID which creates a KYC checked, decentralised digital credential based on Evernym's Sovrin decentralised ledger.

Others such as Infobip use mobile ID as a way to improve the user experience of using a digital identity. The Infobip solution verifies a user's phone number and, in doing so, protects customers against SIM Swap attacks. This is done in an unobtrusive manner – a key requisite of ID solutions, with friction often being a barrier to uptake.

The verified attributes that a digital wallet can present on request are those same attributes that other digital identity systems present. The relying party is in charge of deciding if those attributes are assured to a level that is acceptable for the transaction.

Juniper Research's View: Smartphone identity is part of a wider ecosystem play. One of the drawbacks of a smartphone-based identity wallet is that it is, by definition, not omnichannel. Increasingly, accessibility is a consideration in the design of mass-adopted identity systems. While mobile devices are ubiquitous, with over 6.9 billion handsets in use in 2020, based on Juniper Research data, not every situation when presenting an identity/transacting is done using a smartphone.[viii] Juniper Research expects that wallet IDs will be valuable in point use cases, like digital driver's licences, and also when used in combination with ID Networks/ecosystems. They are likely to be co-opted into ID networks within a re-use model to give users choice in presenting identity credentials to relying parties.

2.2.2 Identity Networks

Multiple driving forces are coming together to flesh out the requirements of identity use cases. Platforms such as Customer Identity and Access Management (CIAM) are morphing into powerful, API-enabled ecosystems, sometimes called 'ID Networks.' These so-called ID Networks are designed to have a more fluid approach to sharing identity data – some offering 'decoupled,' transaction-led ID interactions for enhanced flexibility and use models.

Identity Networks are based on the idea of 'connecting the dots' around use cases. Being API-based, the networks draw in the functionality of many of the identity technologies mentioned in the report. A typical system will be based on a controlling component, an identity (data) orchestration engine (IdOE) which is a multi-functional API. This acts as a central piece to manage the requirements of a service. The service will be based on rules of engagement. These rules reflect the needs at specific junctures in a user journey. For example:

- The user may be required to have identity attributes verified – The IdOE will call a verification service to perform this function.
- The user may be required to choose an existing identity account to federate login – The IdOE will offer a set of optional identity providers.

The IdOE will handle protocol translations to allow for a wide choice of federated IDPs.

- The user may be required to add attributes to a new or existing identity account or during a transaction (e.g., banking details) – The IdOE will handle this and verify these additional attributes if requested. This may include checks that cover AML, sanction lists, and behavioural monitoring.
- The user may be required to provide consents across various parts of the user journey pipeline – The IdOE would handle the collection of consents; sharing consent event data (e.g., log file) with a consent manager

For example, the direct integration of Open Banking APIs and/or Open Banking aggregators (e.g., Truelayer) can be used to provide KYC assured identity attributes to an eCommerce relying party. The same integration could offer identity decoupling, providing assured federated login and/or assured banking data to process a transaction.

Another example, which is likely to drive adoption in the UK is the mandatory checking of age. The Information Commissioners Office (ICO) has published an 'Age Appropriate Design Code' which came into force in September 2020. The code sets standards about how digital services interact with minors, strongly encouraging the use of age verification. In a multi-functional service, adding on age verification checks can be costly and complicated. ID Networks have the potential to use rules to add these checks in under certain triggers.[ix]

ID Networks utilise any of the available identity-related technologies on the market. ID Networks are not about individual technologies but about how to pull services together that are best-of-breed to create identity services. They can provide the omnichannel support needed by modern systems, especially those of mass-adoption, such as government attribute networks.

Juniper Research's View: This is one to watch and an important evolution in the ID space. Identity ecosystems have been discussed in the space for over a decade. However, it has taken an alignment of technology trends to bring this thought to fruition. API-enabled services, industry partnerships, consumer expectations, and regulations including AML/Combating the Financing of Terrorism (CFT) are all pushing the need for more fluid and versatile identity solutions forward. Open Banking (part of Payment Services Directive 2 or PSD2) offers a new way to connect users, KYC checked identity accounts, and relying party (RP) services. Most banks have already completed KYC/CDD to a high level' and RPs can utilise this to provide assured identity for their own purposes, including transactional assurance. Vendors of ID Networks include Avoco Secure and SecureKey. Companies who offer this must be able to connect to required contributing services through long-term relationships with the vendors who make up the network.

2.2.3 Decoupling Identity and Transactions

Digital identity as a concept may have caused the industry to stall at times. Trying to build an all-purpose digital equivalent of a human being can be complicated; the process can be arduous for the consumer, as it requires deep verification and is costly. This is borne out by the experiences of government and banking. A subset use case that is based on some functionality of an identity network is to decouple identity from transactions: a service built to supply the necessary assurance and other

data (e.g., financial) during a transaction. Data would not be stored, the IdOE would be responsible for acting as a conduit for the data requirements during the transaction.

Decoupled ID systems can be centralised or decentralised and offer a flexible way for users to transact.

Juniper Research's View: This specific use case may be a useful one to create simple demonstrators and prototypes for this type of technology. It is also a good candidate for companies wanting some of the flexibility inherent in ID networks without building a larger ecosystem. Alternatively, this can be used by existing services that support consumer accounts – the service can then use an API call to provide proof during a transaction, in a similar way to PSD2 requirements, but for non-financial data (e.g., proof of age).

2.2.4 Zero Trust, Authentication, UEBA, and Anti-fraud

NIST recently (August 2020) published NIST Special Publication 800-207 on Zero Trust Architecture.[x] This paper sets out best practises for establishing a Zero Trust Architecture (ZTA). Although ZTA models are a few years old now, the COVID-19 pandemic and home working has brought the concept sharply into focus. ZTA focus on devices, people, and assets – the three closely mapped and intrinsically linked. The idea of 'never trust, always verify' is particularly pertinent in a climate where credential theft is at an all-time high. During the pandemic lockdown there was a considerable increase in Dark Web (dot onion) sites; in March 2020 there were around 75,000 sites; by mid-May 2020 there were over 250,000 unique dot onion sites. This sharp spike corresponds with the increased phishing campaigns that were sent out during the lockdown period.[xi] Adding into the mix, according to a BitGlass 2020 report, 63% of companies are concerned about data leaks via personal devices.

ZTA offers a way to add more dynamic controls over the access of data and other resources. In a company context, ZTA is applicable to not only employees, but non-employees (e.g., contractors, as well as third and fourth parties).

A takeaway from the NIST report sets out the importance of using this stance in cybersecurity threat mitigation and data protection:

'When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and best practices, a ZTA can protect against common threats and improve an organisation's security posture by using a managed risk approach.'

One of the areas that the report focuses on is the act of monitoring. A number of things are coalescing in the digital identity industry. One of these is anti-fraud. Monitoring solutions are becoming smart with machine-learning based algorithms offering dynamic and proactive analysis of not only human but entity behaviour. The solutions are typically referred to as User and Entity Behavioural Analysis (UEBA).

'Experian recognise that there is a convergence of fraud prevention and consumer identity – the lines are blurring – and we believe that Experian, already having the experience in both, is at the forefront of this. We can provide the necessary insights to inform better decisions for the CIAM platforms on both the identity risk and the authentication risk.' - David

Britton, VP of Industry Solutions, Identity & Fraud Management at Experian[2]

Juniper Research's View: Zero Trust Architectures and associated enabling technologies like UEBA are likely to be increasingly used, as remote working continues to be an important part of the flexible working solutions of the 2020s. Achieving the dictates of a ZTA will likely foster new identity consultancies that offer advice and help in creating effective ZTAs. These consultancies have a natural home with MSSP vendors. Juniper Research would not be surprised if MSSP's built ZTA practices.

2.2.5 Single Sign On and Integrated Solutions

Single Sign On (SSO) is a useful option for both consumers and employees/non-employees. SSO is most commonly handled through standard identity protocols such as OpenID Connect (OIDC) OAuth 2 and SAML 2.

SSO provides a mechanism for cross-domain access that simplifies the user experience. For security, it must be backed up using robust authentication, such as multi-factor and risk-based authentication. The system is built upon an ecosystem comprising of Identity Providers (IDPs) and Service Providers/Relying Parties (SP/RP). Business agreements and shared credentials between the parties underpin the ecosystem.

Juniper Research's View: SSO is a useful tool in a business context for allowing employees to access resources on multiple domains. SSO has become more complicated by the home working movement during the COVID-19 pandemic. SSO requires a more robust approach to ensure that security is not impacted by home networks. A Zero Trust Approach with UEBA and employee monitoring can augment SSO.

In terms of consumer and SSO, Juniper Research believes that, as ID Networks become widespread, this will enable a more robust version of SSO for consumers to take off.

2.2.6 A Word on Decentralised vs. Centralised Identity

Over the last year, there has been much discussion on social platforms and in working groups to forward the area of decentralised (most notably Self Sovereign identity or SSI). The Sovrin Network, a not-for-profit providing an underlying decentralised ledger for SSI, has repositioned itself under a banner known as Trust over IP (ToIP). This acts as SSI's trust framework and is used to promote the use of an SSI. In addition, the SSI movement has worked diligently under the roof of the World Wide Web Consortium (W3C) to create a standard, Decentralised Identifiers (DIDs). The sharing, management, and control of digital all use a security standard called Zero Knowledge Proofs (ZPKs).

Industry voices have asked questions around the business application of SSI. One issue raised was the use of account delegation with an SSI. Sovrin has responded with a whitepaper looking at the feasibility of delegating SSI account access and use. The answer lies in creating 'digital guardians.'[xii] Other issues involve claims around complete control and privacy of personal data – for example, if an online retailer needs an address, this will have to be revealed for delivery. Another concern is over the use of a governing body within the framework of self-sovereign – is this fitting a square into a round hole?

[2] Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian in September 2020

Several governments are exploring the use of SSI, including the Canadian government and the Flemish Government, within the Programme for Innovation Procurement (PIP).

Centralised identity may become a more abstract description if decoupling of identity from transactions becomes more widespread. Centralised identifying data, however, such as passports, national identity numbers, and so on are likely to continue to be centrally managed by government bodies. How this central management of core identifying data fits with an SSI view of the world is not clear. The verified claims may sit on a decentralised platform, but they are still within centralised control. These debates continue in the space.

Juniper Research's View: Juniper takes a pragmatic view on Self Sovereign Identity in line with commentators such as the Canadian government's Tim Bouma, who has taken a deep interest in SSI, and states that 'while emerging technologies such as self-sovereign identity (SSI) might be the better way, allowances need to be made for the coexistence of different identity models.'[xiii]

Taken from an Electronic Frontier Foundation article on self-sovereign IDs:

'The privacy recommendations in the W3C and mDL specs must be treated as a floor and not a ceiling. We implore the digital identity community and technologists to consider the risks to privacy and social equity. It can be exciting for a privileged person to be able to freely carry one's information in a way that breaks down bureaucracy and streamline their life. But if such technology becomes a mandate, it could become a nightmare for many others.'[xiv]

Juniper Research believes that SSI will work in best-fit use cases where an individual using a self-managed identity model is appropriate. SSI also works well as part of a wider ID Network offering self-sovereign choices to individuals.

3. Digital Identity Competitive Landscape

3.1 Competitive Analysis Introduction

In this section, we examine and compare a number of vendors active in the digital identity space. We do not intend to provide comprehensive coverage of all the vendors operating in this market, but to introduce the reader to 14 vendors that are active and have recently been successful in this space. The vendors in this area are broadly comparable. All of those included offer solutions that enable the provision of digital identity. While the areas in which identity is available and used are different, all the vendors are active and high profile in the market. The individual vendors analysed and placed in our Leaderboard are:

- Acuant
- Callsign
- Civic Technologies
- Evernym
- Experian
- Thales
- Giesecke + Devrient
- HYPR
- IBM
- IDEMIA
- Mitek
- Okta
- Signicat
- WorldReach

3.2 Vendor Analysis & Juniper Leaderboard

Our approach in this assessment of digital identity vendors is to use a standard template to summarise vendor capability. This template concludes with our views of the key strengths and strategic development opportunities for each vendor. In this section, we provide our view of vendor positioning using our Leaderboard technique.

This technique, which applies quantitative scoring to qualitative information, enables us to assess each vendor's capability and capacity, as well as its product and position in the digital identity space. The resulting matrix exhibits our view of relative vendor positioning.

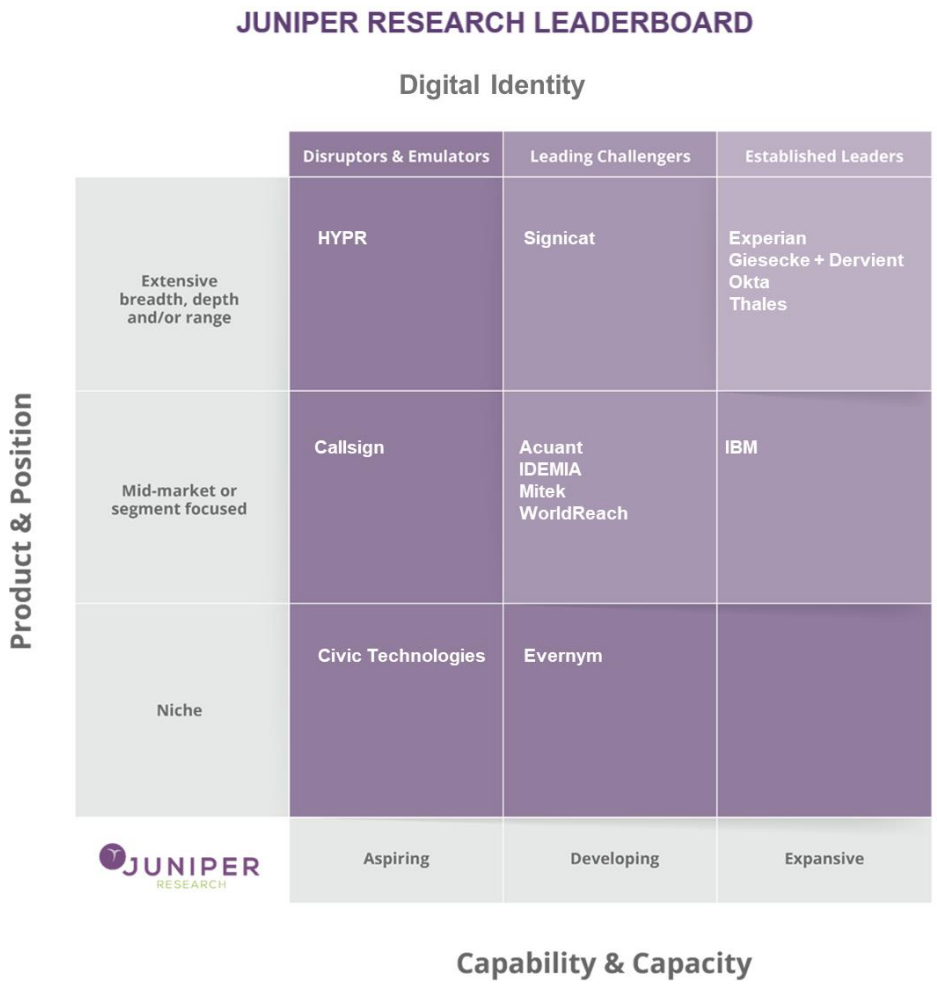
We have assessed each vendor's capabilities against the criteria in following table.

Table 3.1: Digital Identity Vendor Capability Assessment Factors

Category	Factor	Description
Corporate	Experience in Sector	A measure of the length of time the company has had digital identity products.
	Financial Performance & Size in Segment	In assessing this factor we have considered the absolute size of the vendor, as measured by the identity-related revenue of the company.
	Operations	This factor considers primarily the overall extent of geographical penetration of the vendor based on numbers of countries, regions, customers and offices to measure global reach.
	Marketing & Branding Strength	The strength of the vendor's brand and marketing capability.
	Partnerships, Mergers & Acquisitions	The level of digital identity-related partnerships, mergers or acquisitions undertaken by the vendor in question.
Product & Position	Identification Coverage	This factor assesses the number of forms of identification products that the vendor has currently available, and the sophistication of those offerings.
	Authentication Coverage	This factor assesses the capability of the vendor to provide wider authentication features, and the sophistication of those offerings.
	Customers & Deployments	Scale of deployments of the company's digital identity solutions, both in terms of number of users and geographic availability.
	Compatibility & Interoperability	This factor evaluates the number of operating systems, identity protocols and integrations the company's products have. This considers both overall compatibility at an OS and hardware level and distribution partnerships with other companies.
	Certification & Compliance	This factor analyses the level of compliance with a variety of identity standards the company can provide.

Source: Juniper Research

Figure 3.2: Juniper Research Leaderboard for Digital Identity



Experian has a large client base and several innovative methods of verifying identity using both its own and its partners' technologies. The company has a deep understanding of the nuanced nature of modern ID verification. Their application of passive verification within a wider ID context will position them in many use cases, including government.

Source: Juniper Research

i. Limitations & Interpretation

Our assessment is based on a combination of quantitative measures where they are available (such as revenue and number of employees) that will indicate relative strength, together with a qualitative judgement based on available market and vendor information, as published and gleaned during our extensive set of one-to-one CxO-level interviews right across the market. We have used publicly available information to arrive at a broad, indicative positioning of vendors in this market, on a 'reasonable efforts' basis. However, we would also caution that our analysis is almost by nature based on incomplete information and, therefore, for some elements of this analysis we have had to be more judgemental than others. For example, with some vendors, less detailed financial information is typically available if they are not publicly listed companies, although we have detailed data on the scale of venture capital investment.

We also remind readers that the list of vendors considered is not exhaustive for the entire market but rather selective. Juniper Research endeavours to provide accurate information. Whilst information or comment is believed to be correct at the time of publication, Juniper Research cannot accept any responsibility for its completeness or accuracy; the analysis is presented on a 'reasonable efforts' basis.

The Juniper Research Leaderboard above compares the positioning of digital identity vendors based on Juniper Research's scoring of each company against the above criteria that Juniper Research has defined. The Leaderboard is designed to compare how the vendors position themselves in the market based on these criteria; relative placement in one particular unit of the Leaderboard does not imply that any one vendor is necessarily better placed than others. For example, one vendor's objectives will be different from the next and the vendor may be very successfully fulfilling them without being placed in the top right box of the Leaderboard, which is the traditional location for the leading players.

Therefore, for avoidance of doubt in interpreting the Juniper Research Leaderboard, we are not suggesting that any single cell implies in any way that a group of vendors is more advantageously positioned than another group, just differently positioned. We additionally would draw the reader's attention to the fact that vendors are listed alphabetically in a unit of the Leaderboard and not ranked in any way in the cell in question.

The Leaderboard is also valid at a point in time: September 2020. It does not indicate how we expect positioning to change in future, or indeed in which direction we believe that the vendors are moving. We caution against companies taking any decisions based on this analysis; it is merely intended as an analytical summary by Juniper Research as an independent third party.

Finally, we would point out that the Leaderboard is based on a global view consolidated across the digital identity space; any Leaderboard produced for one specific region or segment would, by definition, show different vendor positioning. Indeed, not every vendor would appear on such a Leaderboard.

Table 3.3: Digital Identity Leaderboard Scoring Heatmap

	Corporate Capability & Capacity					Product & Position				
	Experience in Sector	Financial Performance & Size in Segment	Operations	Marketing & Branding Strength	Partnerships, Mergers & Acquisitions	Identification Coverage	Authentication Coverage	Customers & Deployments	Compatibility & Interoperability	Certification & Compliance
Experian	●	●	●	●	●	●	●	●	●	●

HIGH ●●●●● LOW

Source: Juniper Research

3.3 Experian Company Profile

Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian, September 2020

i. Corporate

Experian is a global information services company which provides data and analytical tools to client companies around the world. It is a publicly listed company and trades on the EXPN (London Stock Exchange). It had revenue of $5.18 billion for the fiscal year ended in March 2020. Key executives at the company include Brian Cassin (CEO); Kerry Williams (COO); and Steve Wagner (Global Managing Director, Experian Decision Analytics).

Perhaps best known as one of the biggest credit reporting agencies, the company's main business divisions include Data, Decisioning (both B2B) and Consumer Services (B2C).

The company's fraud solutions have historically been reported under its Decision Analytics segment (now part of a new Decisioning segment). Evidence from its latest annual report suggests that the company's FDP offering became an increasingly important part of its portfolio, with demand for fraud prevention noted as a driver for segment growth across business regions.

The company has a long tradition of providing identity proofing services and around 22-28% of revenue of the Decision Analytics division is attributed to identity checking and verification.

Table 3.4: Experian Financial Snapshot ($m) FY, 2018-2020

	FY 2018	FY 2019	FY 2020
Revenue	$4,662	$4,861	$5,179
Profit before tax	$815	$957	$942
Decisioning Revenue Share (%)	14.3%	25.6%	23.9%

Source: Experian

In April 2014, Experian acquired 41st Parameter for $324 million, a provider of device identification technology for web fraud detection, to strengthen its risk-based identity authentication capabilities. The acquisition was part of Experian's goal to provide the most complete set of fraud detection and identity authentication capabilities in the market.

ii. Geographic Spread

Experian's headquarters are in Ireland. It has further offices in 45 countries across the globe in 6 continents. Experian employ around 17,800 staff.

iii. Key Clients & Strategic Partnerships

- Experian continues to acquire around data and analytics. In 2019, Experian completed eight acquisitions including those of Compuscan (CSH Group (Pty) Limited) a leading provider of credit information and decision analytics across sub-Saharan Africa for $263 million.

- Experian has a wide range of partners, some of which are not publicly disclosed. Key publicly announced identity and fraud partnerships include BioCatch, Ekata, Emailage, Mitek, Daon, Acuant, Boku, GDC, and Onfido, as well as specific regional partners like Oiti and Nextcode in Brazil, and RapidID and IDfy in Asia.
- Experian has also partnered with Microsoft Azure Active Directory to allow Microsoft customers to benefit from Experian's identity verification, fraud prevention and authentication solutions to limit fraud losses and reduce unnecessary customer friction.
- The company partners with leading technology companies, for example, to create IP geolocation data.
- Customers include banks, eCommerce merchants and retail companies, telecommunications providers, travel providers, health providers, insurance companies, and public sector organisations.
- Since the launch of its CrossCore platform, the company has secured a growing list of commercial clients throughout North America, Latin America, Asia-Pacific, Europe, and Africa to take advantage of the platform, as well as 15 integration partnerships to expand its capability.

iv. High-level View of Offerings

Experian offers identity and fraud services for clients in more than 44 countries. Every year, Experian validates that 400 million people are who they say they are and help organizations effectively fight fraud while providing a hassle-free customer experience.

In May 2020, Experian released a new version of CrossCore. This version has been designed to make the management of complex orchestration simpler, faster, with a highly scalable performance. CrossCore is being used by more than 250 clients worldwide and is designed to help clients manage risk across the various touchpoints of the customer journey, from new account creation, through login/authentication risk and, ultimately, transactional activities.

The platform has been promoted as a 'smart plug-and-play platform,' given the ability for customers to connect their own solutions, Experian products and third-party vendor solutions. David Britton remarked that the platform is 'a single API for clients, where the client can submit the data into Experian and Experian handles the technical integration with third-party solutions, the financial contracting with those vendors on behalf of the client, manages the complex orchestration and risk assessment, after which CrossCore processes that data through an ML modelling infrastructure to generate highly accurate risk and trust assessments.' The platform's key features include:

- A single API with which clients can integrate, for real-time assessments of ID verification, authentication, and fraud risk for the user journey (account origination, login/account maintenance, non-monetary activities, and transactional activities).
- Sophisticated workflow orchestration, where CrossCore can invoke calls to various services (Experian's solutions, bank solutions or third-party vendors) based on conditional logic.
- Partner integration: Experian's partnerships extend beyond technical integration, but include all contracting and due diligence with the vendor, such that the client only needs to amend their MSA with Experian to take advantage of the solutions.

- Advanced Decisioning: CrossCore is designed to leverage the complete raw output in Experian's network to perform advanced analytics via Experian's native machine learning infrastructure. Experian's approach includes a hybrid of unsupervised models (to generate features), supervised generic or custom models per use case, and a business rules infrastructure. This provides high levels of accuracy to the client; leading to significantly reduced friction and operational costs.

- Behind CrossCore, Experian's native solutions include Bureau-based ID Verification, Device intelligence (malware, jailbreak, and device emulation detection), dark web intelligence, access to consortium risk attributes, machine learning-based risk modelling, and case management/investigator tools.

The company reports that one of the strategic goals for the year ahead is to further develop the CrossCore platform through the ongoing addition of new partners, as well as continuing to evolve the solution's capabilities in terms of machine learning and biometric authentication.

Among the marquee solutions within the Experian portfolio, which are integrated into the CrossCore platform, are global solutions and regional-specific identity solutions like:

- Hunter – This is an industry-leading global application fraud prevention and data sharing platform which specialises in new account fraud and AML. It's used by more than 410 organisations in over 22 different countries across a variety of verticals. Hunter offers a high level of configurability to match and profile application data – with tools that enable quick decisions and analysis of connected fraud rings.

- FraudNet – This solution manages digital access and payments fraud detection and includes customised versions which have been developed to suit specific verticals such as eCommerce and banking. FraudNet is Experian's patented device intelligence solution that analyses hundreds of device attributes and prevents fraud on all digital channels. It uses a multi-layered, rule-driven identity linkage framework that bridges the gap between physical and digital identity. Any business that has a digital channel, a mobile app, or facilitates digital transactions will experience fraud and will benefit from implementing FraudNet.

- PreciseID in North America as well as ID Authenticate in the UK market; are used for Identity Verification and Identity Fraud detection, leveraging authenticated identity data from Experian's bureau to help clients fight identity theft fraud and maintain regulatory compliance for KYC.

- The Precise ID Model Suite combines identity analytics with advanced fraud risk models to distinguish various types of fraud – such as first-party, third-party or synthetic fraud. By differentiating fraud types, clients can determine the best treatment for each scenario which in-turn prevents fraud more efficiently and protects legitimate customers.

- Experian's Sure Profile™ is the first product in the market to share in the losses caused by synthetic identity. Sure Profile is first-of-its-kind credit profile that helps lenders detect synthetic identity fraud risk before making a credit decision. Experian determines authentic identities and stands behind the data by sharing in losses.

The breadth of these combined solutions allow Experian to detect events such as synthetic identity fraud and traditional identity fraud, combining device analytics to assess fraud patterns or bot activity. These elements integrate seamlessly with the CrossCore platform.

The fraud landscape is constantly changing and a one-size-fits-all approach does not do enough to stop today's sophisticated fraudsters. Experian uses a unique combination of data, analytics, and technology to create right-sized solutions that allow our clients to make confident decisions for every transaction. Experian's ultimate goal is to make the industry's identity and fraud solutions work better for everyone around the world.

For more information, visit https://www.experian.com/blogs/global-insights/.

4

Endnotes

[i] NIST Special Publication 800-207: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[ii] Akamai: https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-in-the-media-industry-report-2020.pdf

[iii] W3C, Decentralized Identifiers (DIDs) v1.0: https://www.w3.org/TR/did-core/

[iv] UK Gov Verify Match rates: https://www.gov.uk/performance/govuk-verify

[v] National Audit Office Investigation into Verify: https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf

[vi] DIACC: https://diacc.ca

[vii] Thales: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/digital-id-wallet

[viii] Statistica: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[ix] Information Commissioners Office (ICO) has published an 'Age Appropriate Design Code': https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

[x] NIST Special Publication 800-207: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

BitGlasss report: https://www.bitglass.com/press-releases/bitglass-2020-byod-report-remote-work-drives-byod-but-security-not-keeping-pace

[xi] TorMetrics: https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2020-02-16&end=2020-05-16

[xii] Sovrin, Digital Guardianship white paper: https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper2.pdf

[xiii] Tim Bouma blog April 5th 2020: https://medium.com/@trbouma/canada-enabling-self-sovereign-identity-efcfda2aa044

[xiv] Electronic Frontier Foundation: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10