Financial Data and Technology Association

http://www.fdata.global/north-america

THE CURRENT STATE OF DIGITAL IDENTITY

In parallel with open banking, digital identity is without question one of the most significant technology trends of the day. However, in a world on the brink of a Fourth Industrial Revolution driven by the convergence of digital, biological and physical innovation, digital identity – how humans are recognized and navigate through the sum of all of their online interactions in a secure and trusted way - has far greater implications and applications than just open banking or even finance. Fueled by an urgent and pressing need for seamless access to a constellation of services ranging from government departments to all sectors of the market, for the consumer, a secure digital identity resides at the heart of the technological universe.

Such is the importance of secure identification that is has become a core component in the design of global socio-economic policy, driven by the implications of empowerment in the arenas of financial inclusion (and thus, the reduction of poverty), health, education, the civil right right to vote and access to systems of social governance. Economic exclusion is just one element tied to the lack of legal identity and it is worthy of note that the United Nations Envision2030 Sustainable Development Goal 16 (Peace Justice and Strong Institutions) includes the provision of legal identity for the global population.

It is indeed the case that the fundamental proposition of open banking is based on the need for secure identity. However, none of the geographies that have live implementations or mature plans for such are subscribed to any single identity solution for the consumer as a prerequisite, federated or otherwise. Identity itself flourishes as a competitive marketplace, providing agile solutions that move with the innovative products and services created by FinTechs rather than the ecosystem being potentially hampered by a single narrow and static technology solution. Realistically, any reliance on a single solution carries risk and is antithetical to the competition and innovation designed to be inspired and cultivated by open banking.

Digital Identity in the United Kingdom

As arguably the most mature live implementation in the world, the UK took a prescriptive approach to open banking using the legal and regulatory framework of PSD2 to mandate the largest banks (the CMA9) to follow the UK Open Banking Standard, allowing

consumers to use a regulated third party to (with their permission) access their bank account using a secure interface (API). A critical component, a whitelist known as the Open Banking Directory, was created to ensure that banks and third party providers (TPPs) would know at all times which parties had access to what APIs. The whitelist provides three key functions: a trust framework that enables confirmation of an entity's regulated status, supporting real-time updates from a central source; an identity component with a searchable directory allowing for transparency as new actors join the market; dynamic registration and automation of the on-boarding process between TPPs and banks. The underpinning technology solution used for the directory was provided by Ping Identity, already a core vendor for many of the banks technology stacks in the CMA9.

The entirety of the Open Banking Directory was designed for interaction amongst regulated entities. Nothing similar was prescribed concerning identity for the individual UK consumer however; a pre-existing digital identity framework was clearly not necessary for the Open Banking implementation. The UK government's continuing efforts for a national identity assurance framework (Gov.UK Verify) have been long in development, a process begun in 2011 and launched in 2016. The system was designed to initially provide a single login across all government departments offering digital services. The verification process offered a choice of five companies (including Experian, Barclays, the Post Office, Digidentity and SecureIdentity) for the purpose of verifying an individual's identity to a level of assurance before providing access to a number of central government services. The identity verification process is carried out by these accredited private sector entities who aggregate identity evidence by comparing user data against a diverse set of publicly and privately held records.

Gov.UK Verify continues to experience a protracted roll-out with reduced funding, diminished scope and less than four million of the twenty-five million users projected by 2020. Government funding for this effort will cease in April, 2020 and the project will be passed in its entirety to the private sector. The Comptroller and Auditor General of the National Audit Office, Sir Amyas Morse, KCB, cited the challenge of working at the forefront of new technology and the ability of a single solution to maintain pace with rapidly evolving demands (NOA report of March, 2019, "*Investigation into Verify*"). In August, 2019 it was announced that Experian, Barclays and Secure Identity had notified the Government Digital Service of their intention to withdraw from the framework, leaving

Digidentity and the Post Office as the only remaining participants. As the Post Office is built around the Digidentity platform however, there are obvious questions around competition issues and whether Verify can continue with essentially one identity company effectively holding a monopoly.

In the UK's private sector, a healthy profusion of providers exists in the marketplace. For businesses, the ID Co. provides a suite of services marketed as DirectID "Bank Data Unleashed" that includes account validation, income verification and product categorization, enriching bank data with use cases covering KYC, risk, collections, fraud and frictionless onboarding. For the consumer, Yoti (Your Own Trusted Identity) provides age verification, identity, login credentials and other key components for the use of digital services, and in the UK alone, now has over five million users on its platform. With aspirations for global growth, Yoti this year raised $9.7 million of new equity investment for further product development and expansion of operations in India, a potential market of 1.3 billion people.

Digital Identity in India

Yoti's entrance into India's digital identity space speaks to the capacity for competition in a jurisdiction with a well-established and celebrated federated identity framework. Established in 2009 by the government of India under the jurisdiction of the Ministry of Electronics and Information Technology, Aadhaar is the world's largest biometric identity system. From the Hindi, meaning "foundation", Aadhaar comprises a unique twelve-digit number that may be obtained voluntarily by participants. While the number is considered proof of residency it is not however, proof of citizenship. Demographic information such as date of birth and address is combined with biometric details such as fingerprints and iris scan with the data being held by the Unique Identification Authority of India (UIDAI). The multiple benefits of an Aadhaar identity card include the ease of access to bank accounts, e-verification of income tax returns and a simplified eKYC process. In recent years, the efficacy and scope of Aadhaar have been the subject of several rulings by the Supreme Court of India. In a push for harmonization across the ecosystem, the central government advocated for Aadhaar to be mandatory for an array of services including opening bank accounts and access to mobile platforms, an argument that met with significant resistance fueled by privacy concerns. In September, 2018 a judgement was rendered against that notion. While providing many benefits to the consumer and

technological ease of access, the single solution can clearly become exclusionary, counterproductive and divisive.

In parallel with Aadhaar, Indian innovation has continued to explore alternative identity solutions, perhaps the most notable of which is the Modular Open Source Identity Platform (MOSIP). With ex-Aadhaar members on its board, MOSIP, funded in part by the Bill and Melinda Gates Foundation, is an open source platform upon which national foundational identity systems can be built for effective delivery of a variety of public and private services. MOSIP provides core modules and access to an ecosystem of commercial partners responsible for customization and integration tailored to the requirements of governments and private organizations.

Digital Identity in Estonia

Estonia has provided an excellent case study for a federated identity system. Several European countries have made efforts for digital identity cards but typically these have been defeated by the blockers of high implementation costs, privacy (with regard to both government spying and data breaches) and efficacy in an ever-expanding world of multi-sector connectivity. Estonia's mandatory identity card is used for regular identification, a travel document within most of Europe and for establishing an identity within an electronic environment and providing a digital signature. The use cases extend to healthcare, public transit, voting and online banking with over six hundred e-services for citizens and nearly three thousand for businesses. In 2014, the government made the identity cards available to non-residents in order to facilitate the growth of international competitiveness of the Estonian state, making it the first country to have a truly global digital identity. Applicants simply have to provide the same documentation and biometric data, receiving a physical card or virtual equivalent that can be stored on a mobile device's SIM card. Possession of this virtual identity allows for fast-to-market launches for business as well as access to a variety of web-based services. The ambition for the population of digital Estonians is 10 million by 2025, far in excess of the current physical population of 1.3 million.

This visionary federated implementation is not however without its vulnerability and risks. In 2017, it was discovered that the new chip from Gemalto, introduced to the new version of identity cards in 2014, had a serious security flaw. Although no actual breach was

determined to have occurred, the remedy involved multiple patches and suspension of access for the 760,000 affected cardholders. Despite a larger crisis having been averted, the residual cost to the reputation of the Estonian e-state persists as do the legal proceedings of the €152 million lawsuit brought against Gemalto. It is also worth noting that the same chip was supplied for use in cards issued by the French and German governments.

Digital Identity in Australia and New Zealand

Australia's recent launch of Open Banking proceeded with due consideration of the importance of a secure digital identity but without the need for any particular pre-existing framework. The author of the 2017 Australian government's *Review into Open Banking*, Scott Farrell, had a vision for a digital identity backbone but stopped short of a clear definition or implementation. The Consumer Data Right issued by the Treasury in May, 2018 clearly describes the rights of the consumer to access and share data from the first three sectors to which the right will apply (banking, energy and telecommunications), but there is no embodiment of a digital identity framework. The scope expressed in these two key documents is clearly much larger than banking and more a view for an open data society in which anybody from the individual consumer up to large companies have the ultimate right to share and move data.

Culturally, driven by the familiar concerns surrounding privacy and risk, Australians are generally predisposed against a national identity system or centralized credential. Digital identity is built around an assortment of documents including the state-issued driving license and passport and predictably a variety of approaches to digital identity exist. Similar to the UK, the Australian government are contemplating a federated identity proposal for access to government services such as social security and income tax verification. The effort embraced the hope that eventually industry would adopt the system, however the private sector indicated that it was not fit for purpose outside of the government sector. The Australian postal service has an age verification product with aspirations for this to become a broader digital identity solution in the future. The payments network body are independently working on a solution as a response to solving "card not present" fraud. The big four Australian banks having arguably the most security do have the ability to verify identity for services with FinTechs via a redirect model, but

there is no active collaboration between the banks themselves thus potentially limiting consumer choice.

In New Zealand, a seventy-member consortium of banks, Fintechs, large and small companies and consumer groups is leading a national effort to help the country's transformation as a digital nation. Digital Identity NZ describes itself as a purpose driven, inclusive, membership funded organization, whose members have a shared passion for the opportunities that digital identity can offer, supporting a sustainable, inclusive and trustworthy digital future for all New Zealanders. Among the core principles are identifying scenarios where a person-centric digital identity helps solve key problems and improves people's lives, giving input to the governments Digital Identity Trust Framework, and agreeing on a recommended open protocol model that supports interoperable solutions.

Digital Identity in the United States of America

As in the UK, there are a range of digital identity and verification services offered by the private sector in addition to a federal initiative. The market opportunities for identity provision in the private sector have also attracted the attention of non-US companies such as the UK's ID. Co. The US is clearly within their scope for international expansion as evidenced in their strategic plans revealed shortly after securing $2 million in seed funding in May of 2019. As part of the evolving federal initiative, in April, 2017 login.gov replaced connect.gov that had launched at the end of 2014. (Interestingly, Ping Identity was one of the first software platforms to provide Federal Identity, Credential and Access Management (FICAM) compliant credentials to enable private sector organizations to connect securely to government agencies, a primary goal of connect.gov).

A single sign-on solution for government websites, login.gov enables users to access services from multiple government agencies with the same username and password. By offering the public a single, secure private access to online federal services, login.gov eliminates the need to remember credentials for numerous systems and reduces the cost of developing or buying duplicative authentication solutions for the agencies themselves. With two-factor authentication, login.gov leverages the best, most current security protocols (as defined by the National Institute of Standards and Technology's 800-63

Identity Assurance Method Level 1 and Authentication Assurance Level 2). A stated mission is to offer the most secure and modern authentication to the entire US public.

As the US identity conversation actively continues it would be remiss to not mention the work to date contributed by the Better Identity Coalition (BIC), the founding members of which represent leading companies across multiple sectors of the economy, including financial services, fintech, payments, technology, healthcare, telecommunications and security. BIC, an initiative of the Center for Cybersecurity and Law, released its policy recommendations for improving the privacy and security of digital identity solutions in a July, 2018 report entitled *Better Identity in America: A Blueprint for Policymakers*. While certainly not intended as a comprehensive solution for every challenge in the identity space, the guidance provided a well-contemplated set of principles and initiatives designed to be both impactful and practical to implement.

The five key pillars of the report are:

- Prioritize the development of next generation remote identity proofing and verification systems
- Change the way America uses Social Security numbers
- Promote and prioritize strong authentication
- Pursue international coordination and standardization of identity systems
- Educate consumers and businesses about better identity solutions

In general, excluding Estonia and to a lesser extent, India, it would be reasonable to state that most such efforts on the part of governments are in the early stages of rollout, with many standards still being defined and solutions being designed for very narrow and specific use cases.

Towards Canadian Digital Identity Frameworks

There have been several notable advances in Canada with regard to the question of digital identity for Canadian citizens:

- The *Budget Implementation Act* of March, 2018 contained amendments to the business and powers provisions of federally regulated institutions (FRFIs) under *the Bank Act*, *Insurance Companies Act* and *Trust and Loans Companies Act*. These

amendments included enabling an FRFI to provide identification, authentication or verification services.

- Shortly thereafter in May of 2018, the Canadian Bankers Association published a white paper entitled *Canada's Digital ID Future – A Federated Approach* in which the CBA argued the case for a federated digital identification framework, in part referencing the experience of other countries including Estonia. To avoid a central repository possessing holistic views of individuals identities, a citizen's attributes and electronic identity would be stored on the framework across linked but distinct systems. This in turn would enable authentication via a combination of distinct linked data points such as biometric data, a driving license and banking credentials. This approach relies on seamless communication between the constituent systems.
- In May of 2019, Canada and Estonia entered into a Memorandum of Understanding (MOU) around the theme of Digital Government and Economy. The non-legally binding MOU seeks to facilitate cooperation in the areas of digital identity, digital economy and related government policy arenas. The two countries have committed to organizing joint events, exchanges between experts and public officials and the sharing of operational lessons learned in the digital ecosystem. This cooperation extends to other key forums including the Open Government Partnership and the Digital 7 Intergovernmental Working Group.
- Not dissimilar to the inclusive, positive and collaborative spirit of the New Zealand consortium and the US BICs report, Canada's Digital ID and Authentication Council leverages well-crafted fundamental principles for entrants into the identity space as to the desired scope and utility in the provision of digital identity.

As one option in the Canadian market, the SecureKey Verified.Me proposition rests on a collaboration between the five largest financial institutions and Experian. Consumers holding accounts with institutions within that consortium would certainly benefit from the provision of digital identity services and access to open banking. An interesting aspect of the SecureKey business model is the monetization of the data: with a cost of $5 per pull of data, $4 goes back to the originating bank so a key driver for SecureKey is clearly the commercial benefit driven by high volume. Yet, today, Verified.me has only two limited use cases on its platform: Equifax and Sun Life Financial.

One of the other rapidly evolving providers of digital identity in the Canadian market, Owl, hold the thesis that the data set used by financial institutions to authenticate identity is limited. The multiple data points used by banks for digital identity such as driver's license, health card and social insurance details also reside in a fragmentary way across different government domains. Owl sees an opportunity in aggregating data with a business model leveraging access to tens of thousands of live, real-time sources for external data. By comparison, this coverage reaches beyond the data of the big five banks and credit bureaus as found in the SecureKey Verified.Me product. The external sources are more likely to capture historically accurate data, accounting for the possibility that today's consumer may have had more recent interactions with, for example, a FinTech than one of the big five banks. As an automated process, Owl dispenses with any manual checks that occur in the bank environment that also place potential burden on the consumer. With privacy as a fundamental pillar of its design, Owl's platform is built on a zero-knowledge protocol with no stored data and end-to-end encryption.

It would be an important consideration for the SecureKey ecosystem to be open to the participation of other institutions and FinTech firms to ensure a healthy competitive landscape that had the capacity to offer broader solutions. An isolated monopoly would seem antithetical to the nature of the consumer and market benefits offered by open banking products and services. Any notion of a federated identity framework would have to encompass more than just an identity for open banking; if not it would become one of several that consumers would need to navigate other sectors in the digital world. Alternatively, it would need the potential and agility to expand out to other sectors, so banks could not control the only solution.

A partnership between the private and public sectors could potentially provide an environment to ensure that digital identity solutions would be flexible, multi-faceted and innovative. Many current solutions leverage financial institutions as a trusted source for identity that can be federated for other companies to use. In the long term however that structure does not address the population of underbanked citizens, one of the key demographics that stands to benefit from an identity-contingent framework such as open banking. A further consideration is the ongoing challenge with synthetic identities being used to establish accounts for the purposes of fraud; banks themselves therefore may not have the most accurate data.

http://www.fdata.global/north-america

When examining the Estonian model in particular, there are clearly lines of reasoning to support the notion of the government as the ultimate source of truth for identity information. In this structure, the government would provide APIs that allow other entities to directly verify identity or enable third party identity proofing services that are supported with government data.

While there is a perceived risk on the part of financial institutions in letting other actors interact with their systems in an open banking regime, a monopoly that essentially allows the banks to control verification and in effect add a layer of bank certification is too narrow a solution. Without question, there is a role for government to play in ensuring that there is a competitive landscape not tied to any single solution wherein open banking would reside in a closed ecosystem. Furthermore, banks, who stand to face heightened competition within an Open Banking regime, should not be the sole custodians of that solution.

Richard Prior
Global Head of Policy and Research
Financial Data and Technology Association