SECURE KEY

Andre Boysen
Chief Identity Officer, SecureKey Technologies

U.S. House Financial Services Committee
Task Force on Artificial Intelligence

"The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"

September 12, 2019

Chairman Foster, Ranking Member Hill and members of the Financial Services Committee and Task Force on Artificial Intelligence, thank you for the opportunity to discuss the future of digital identity in financial services with you today.

I am Andre Boysen, Chief Identity Officer at SecureKey Technologies. I look forward to sharing our experiences in building a privacy-based digital identity verification network for Canadian consumers, in the hopes that my testimony will help inform this committee and task force as to what possibilities robust digital identity schemes can offer to citizens, governments and the services with which they choose to interact.

SecureKey is a Canadian company that is a world leader in providing technology solutions that enable citizens to efficiently access high-value digital services, while guaranteeing the security and privacy of their personal information. We do this by building highly secure networks that span and merge the strengths of the public and private sectors.

SecureKey's expertise lies in building tools that realize the possibilities of digital identity in the modern digital economy. To build identity verification tools, we focus on the intersection of the citizen, public and private sectors, privacy and consent, rather than leveraging AI and big data.

As we know, the digital age has ushered in a host of new services, business models and opportunities to participate in the world. Not long ago, it would be unimaginable to order a shared ride from a device in your pocket, or to access sensitive government services from your home. Today, we take these things for granted and often get irritated when we come across a task that can't be done online.

It's not just about citizen expectations. Companies, governments and other organizations have strong incentives to move services and transactions online to realize cost savings, enhance client experiences and increase business surety. An organization's ability to do this hinges on a single question: "Can I trust the person, or digital identity, at the other end of the transaction?"

This digital identity challenge is equally problematic on both sides.

To recognize clients and provide trusted access to services online, organizations typically deploy a mix of analogue and digital measures to confirm identity and mitigate risk. As we have seen, however, these solutions tend to be complex and not fully effective. As such, confidence in them has suffered.

On the other side, citizens are asked to navigate a myriad of identification methods and challenges to satisfy the identity proofing requirements of the organizations they seek services from, without knowing where the information is going, and in the face of a steady stream of news about data breaches and online impersonators.

These concerns are well-founded.

Fraudsters are collecting information to know as much, and sometimes more, about the citizens they are impersonating. Standard physical cards are easily counterfeited, and it is often impossible to check their validity with the issuing sources. Even biometric methods, which have often been touted as the solution to digital fraud, are increasingly being targeted by hackers, elevating the risk that biometric data may be compromised.

These factors are driving complexity up, trust in the system down, and adversely affecting privacy; exactly the opposite of what needs to happen.

Our siloed system is too hard for consumers to use and too expensive to be sustained.

Consider the reality of Twitter and Facebook's chief executive officers, Jack Dorsey and Mark Zuckerberg. These two individuals know how the system works, understand digital identity best practices and have all the resources in the world at their fingertips. Yet, even *they* have problems controlling and managing fraudulent access to their own digital identities. If they cannot manage in the current digital identity landscape, how can an everyday citizen be expected to navigate the pitfalls?

The problem we face is not simply a matter of finding the best technology, the right skills, or enough money to fix it; rather, everyone with a stake in the system needs to focus on solving the digital identity problem that underpins all digital services, bringing data and identity information back under the control of the citizen.

To solve the digital identity challenge, we must find ways to combine the prime factors of identity. These are the unique things we know, like shared secrets; the unique things we have, like existing trusted relationships, mobile devices or government-issued identification; and, the unique things we are, like our fingerprints or facial scans.

By combining these factors, we can resolve identity and give organizations confidence that their clients are who they say they are. All experience to date proves that single methods are not up to the task. This means that trusted networks and models are needed. All participants must be involved in the solution, including, and perhaps especially, citizens, whose control over their own data and privacy, will underpin its security.

Only by combining the best aspects of each system can we solve the digital identity problem and rebuild the trust that is equally required by both organization and citizen. The Canadian model is a public-private-partnership between banks, telcos, governments and other trusted partners. Each participant has a unique contribution to make to the ecosystem, and they each also desire services from other participants in the network. It is give to get.

For example, governments are the initial issuers of individual identities, including birth registries, immigration documents, and permits and licences. Governments also can link their records to a living person, by issuing a driver's license or a passport. But governments are not as adept as the commercial sector at knowing if that person is actually at the end of a given digital transaction.

This brings us to financial institutions, who complete billions of authentications per year. Compared to other organizations, citizens only rarely interact with governments during their daily lives. They may renew a license or passport every five years but will log into their bank account several times a week, which gives a higher level of trust and immediacy to that interaction. Then think about mobile devices, which are always within reach, and which are both identifiable within a cellular network and are tied to subscriber accounts.

All parts have something valuable to offer within a successful network.

Imagine a scenario where a citizen can choose to share information securely within a network made up of organizations that they trust already. This citizen would need to access the network using their trusted online banking login and, because he or she is using a device that the telecommunications operator knows and can validate, reliable information – like their age of majority – can be shared to an online seller for a regulated sale, like alcohol, for example. The citizen has complete control over the interaction to share with knowledgeable consent.

In this scenario, the online seller does not need to know the actual issuer of the information, only that it comes from a trusted source. The seller doesn't need to know the citizen's actual birthday, only that the trusted source confirms that they are above the age of majority. Moreover, companies or organizations using the network would have no access or visibility to the data transiting the network. We call this Triple Blind Privacy®.

This scenario is not part of the distant future. All of the pieces are already in place to allow the providers of data to enable a system that has authoritative information, that provides receivers of information with confidence in the transaction, and for the citizen to fully trust the system as they control their own data in a privacy-enhanced way. This type of arrangement is the cutting edge and is happening now in Canada, with our Verified.Me digital identity verification network.

Verified.Me is a service offered by SecureKey Technologies Inc. The Verified.Me service was developed in cooperation with seven of Canada's major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD. It is a first-of-its-kind and blockchain-based network that takes an ecosystem approach to solve the problems associated with digital identity today. Working closely to develop the network with Canada's financial institutions was a natural foundation, as ours is a highly banked population and the number of financial institutions is far more concentrated.

With the information and resources already available, we had the opportunity to solve the digital identity problem and develop a replicable model for the world. These include cooperative jurisdictions, technologically advanced telecommunications, and world-leadership in developing new approaches, such as Global Privacy and Security by Design developed by Dr. Ann Cavoukian; the U.S. Department of Homeland Security Science and Technology Directorate; IBM Blockchain; the Linux Foundation's open source Hyperledger projects; and the Pan Canadian Trust Framework, championed by the Digital Identity and Authentication Council of Canada.

We had, and continue to have, the opportunity to build services that can provide identity validation claims from multiple parties in a single transaction, while ensuring complete privacy and control for the citizen. Key factors for any solution to be successful will be citizen acceptance, trust and the potential to reach a large user base quickly.

The responsibility to guarantee and protect privacy, and to provide a sense of security to citizens, are fundamental factors in the success of any solution. It is critical that any approach to solve the problem with digital identity connects together the trusted parts of the digital economy such as finance, telecommunications, government, and commerce. Only this will provide citizens with confidence they demand, to use the providers that they already trust and to have access to the information that they want to securely share.

The cyber risk around digital identity is high. Any solution that does not involve both the private and public sectors will be of limited success. It will perpetuate the siloed approach that is currently under strain and will not have the security or public trust to enable the digital economy of tomorrow.

Fortunately, there are options and many brilliant minds around the world who are dedicated to solving this problem on behalf on the everyday citizens everywhere. We have the privilege of being the custodians of citizens' digital futures. As such, we have the obligation to act responsibly and with the highest degree of collaboration, commitment to open standards and world-leading privacy and consent technologies. I am thankful for the opportunity to share my expertise in this public forum today, and I welcome your questions.

Thank you,

Andre Boysen
Chief Identity Officer
SecureKey Technologies Inc.