Jeremy Grant
Coordinator, The Better Identity Coalition

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 committee, thank you for the opportunity to discuss the future of identity in financial services with you today.

I am here today on behalf of the Better Identity Coalition[1] – an organization launched last year focused on bringing together leading firms from different sectors to develop a set of consensus, cross-sector policy recommendations that promote the adoption of better solutions for identity verification and authentication. The Coalition's founding members include recognized leaders from diverse sectors of the economy, including financial services, health care, technology, FinTech, payments, and security.

As our name would suggest, the Better Identity Coalition is not seeking to push the interests of any one technology or industry. Instead, our members are united by a common recognition that the way we handle identity today in the U.S. is broken – and by a common desire to see both the public and private sectors each take steps to make identity systems work better. Last year we published "Better Identity in America: A Blueprint for Policymakers" – laying out five key

[1] More on the Better Identity Coalition can be found at https://www.betteridentity.org

initiatives that government should launch around identity that are both meaningful in impact and practical to implement.

As background, I've worked for more than 20 years at the intersection of identity and cybersecurity. Over the course of my career, I've been a Senate staffer, led a business unit at a technology company architecting and building digital identity systems, and done stints at two investment banks helping investors understand the identity market – cutting through what works and what doesn't, and where they should put capital. In 2011, I was selected to lead the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative focused on improving security, privacy, choice and innovation online through better approaches to digital identity. In that role I worked with industry and government to tackle major challenges in identity, built out what is now the Trusted Identities Group at the National Institute of Standards and Technology (NIST), and also served as NIST's Senior Executive Advisor for Identity Management. I left government in 2015 and now lead the Technology Business Strategy practice at Venable, a law firm with the country's leading privacy and cybersecurity practice. In that role at Venable I serve as the Coordinator of the Better Identity Coalition.

Setting the stage

Let me say up front that I am grateful to the Committee for calling this hearing today. Identity is a topic that impacts every American, but it's only recently that identity has started to get proper attention from policymakers in the U.S. At a high level, the way we handle identity in America impacts our security, our privacy, and our liberty. And from an economic standpoint, particularly as we move high-value transactions into the digital world, identity can be the great

enabler – providing a foundation for digital transactions and online experiences that are more secure, more enjoyable for the user, and ideally, more respectful of their privacy.

But when we don't get identity right, we enable a set of great attack points for criminals and other adversaries looking to execute attacks in cyberspace. And unfortunately, we have not been doing well here. A whopping 81% of hacking attacks were executed by taking advantage of weak or stolen passwords, according to Verizon's annual Data Breach Investigation Report. 81% is an enormous number – it means that it's an anomaly when a breach happens and identity does not provide the attack vector.

And outside of passwords, we've seen adversaries seek to steal massive data-sets of Americans, in large part, so that they have an easier time compromising the questions used in "identity verification" tools like Knowledge-Based Authentication or Verification solutions (KBA/KBV). This was illustrated quite vividly by the hack of the IRS's "Get my Transcript" application in 2015 – where more than 700,000 Americans had sensitive tax data compromised.

A key takeaway for this Committee to understand today is that attackers have caught up with many of the "first-generation tools" we have used to protect and verify and authenticate identity. Recent breaches may have driven this point home, but the reality is that these tools have been vulnerable for quite some time. There are many reasons for this – and certainly blame to allocate – but the most important question is: "<u>What should government and industry do about it now?</u>"

That's a key point – government and industry. If there is one message this Committee should take away from today's hearing, it's that industry has said they cannot solve this alone. We are at a juncture where the government will need to step up and play a bigger role to help address critical vulnerabilities in our "digital identity fabric."

Why Identity is so important to Financial Services

While identity is important to every sector of the economy, it's especially critical to the financial services industry – where it is essential to delivering four key outcomes:

1. The first is security. When the legendary bank robber Willie Sutton was asked "Why do you rob banks?" he answered "Because that's where the money is." These days, modern day Willie Suttons don't bother to show up at banks with guns – it's much easier for a robber to steal money by exploiting weaknesses in a bank or business that has mediocre identity and access controls. Financial services firms must embrace robust identity solutions that can block these attacks.

2. The second is the integrity of the financial system – particularly in blocking those who wish to make use of the financial system for money laundering, terrorist financing, and other nefarious acts.

3. The third is enabling great customer experiences. Many high-value transactions are still stuck in the paper world, thanks in part to the challenges with figuring out who is who online. If we're going to bring them online – and streamline the experience consumers and businesses go through in transactions – we need to sort out the identity layer.

4. And the fourth – emerging in importance in recent years – is enabling open banking: where consumers are allowed to ask their bank to share their data with other firms such as account aggregation services, or enable third parties to make payments from their account. Open banking is creating a need for more sophisticated identity solutions, as banks and fintech firms alike seek to enable consumers to authorize access to certain data

or permissions in their accounts on a granular level, and enable consumers to revoke access at any time. And getting identity right is key to making sure that the U.S. leads the way in the next generation of banking solutions.

Against this backdrop, there are three major challenges that every company in financial services must deal with:

1. The first is figuring out whether someone is who they claim to be at account opening. Not surprisingly, this is one of the areas where we have the most work to do. Losses from "New Account Fraud" increased 13% over the last year to $3.4 billion[2].

2. The second – closely tied to the first – is synthetic identity fraud. This is when fraudsters combine a fake name with a real SSN and "trick" the financial system into thinking that an applicant's identity is real when in fact it's a "Digital Frankenstein" made up of a mix of legitimate and fake identity components.

   According to a recent report from the Federal Reserve, synthetic identity fraud accounts for $6 billion in fraud each year, and some estimates suggest that number is as high as $8 billion.[3]

   The playbook for fraudsters has been a simple one: find a child's SSN – which our credit scoring systems – which double as our ID verification systems – have never seen, since

[2] See Javelin Research's Report "2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt" at https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

[3] See https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

minors don't have credit – and pair it with a fake name to trick these systems into thinking that it's a legitimate identity. Over time, the fraudster then opens more and more accounts with this synthetic identity, racking up unpaid bills. Beyond the dollars lost, when a child turns 18 and tries to get her own credit established, she finds that her SSN is tied to a credit history that's a complete disaster – and now has to deal with the consequences.

3. And third is authentication. Once an account has been created – how you create systems that can securely log customers in to that account, in a world where passwords just don't cut it anymore?

Of these three challenges - within financial services, all of the challenges are not the same. If there is one takeaway I can offer about the state of the identity market in 2019, it is this: Authentication is getting easier, but Identity Proofing is getting harder.

Authentication is getting easier, but Identity Proofing is getting harder

Let me unpack that first part: Authentication is getting easier. By that, I mean that while passwords are broken, the ability of consumers and businesses to access tools that they can use in addition to – or in lieu of – passwords is greater than it's ever been. And with multi-stakeholder industry initiatives like the FIDO Alliance creating next-generation authentication standards that are getting baked into most devices, browsers and operating systems, it is becoming easier than ever to deliver on the vision of better security, privacy and convenience. This year, both Google and Microsoft announced that their Android and Windows platforms are FIDO certified, making it easier than ever for firms in financial services and other sectors to deliver passwordless

experiences. The development and adoption of the FIDO standards is, in my view, the most significant development in the authentication marketplace in the last 20 years.

And when these tools are paired with analytics solutions that use Artificial Intelligence and Machine Learning (AI/ML) to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords.

But while Authentication is getting easier – Identity Proofing is getting harder. By that, I mean the ability of consumers during initial account creation to prove that they are who they really claim to be is harder than ever – in part because attackers have caught up to the tools we have depended on for identity proofing and verification.

This means that it is harder than ever for businesses – as more transactions move online – to verify someone's identity when someone is creating an account or applying for a new service. Better tools are needed here. But unlike with passwords – where the market has responded with tools like FIDO authentication and behavior analytics to fix the problem – the market has not yet sorted things out here. And one thing that has become clear in discussion with industry is that the private sector cannot solve this problem on its own.

At the end of the day, government is the only authoritative issuer of identity in the United States. But the identity systems government administers are largely stuck in the paper world, whereas commerce has increasingly moved online. This "identity gap" – a complete absence of credentials suited for digital transactions – is being actively exploited by adversaries to steal identities, money and sensitive data, and defraud consumers and businesses alike.

Better Identity: How to Get There

The Better Identity Coalition lays out five key recommendations for how government and the private sector can improve the identity ecosystem.

1. *Prioritize the development of next-generation remote identity proofing and verification systems*

   As I noted earlier, adversaries have caught up with the systems America has used for remote identity proofing and verification. Many of these systems were developed to fill the "identity gap" in the U.S. caused by the lack of any formal national identity system – for example, Knowledge-Based Verification (KBV) systems that attempt to verify identity online by asking an applicant several questions that, in theory, only he or she should be able to answer. Now that adversaries, through multiple breaches, have obtained enough data to defeat many KBV systems; the answers that were once secret are now commonly known. Next generation solutions are needed that are not only more resilient, but also more convenient for consumers.

   Industry is innovating here, and AI-enabled solutions are one of the tools that can help. But they are not enough. The single best way to address the weaknesses of KBV and other first-generation identity verification tools is for the government to fill the "identity gap" that led to their creation.

   While the United States does not have a national ID – and we do not recommend that one be created – the U.S. does have a number of authoritative government identity systems.

These systems are largely stuck in the paper world; none of them can be easily used – or validated – online.

This means that consumers are hamstrung if they need to prove their identity – or certain attributes about themselves – online, in that they are unable to use the credentials sitting in their pockets and wallets. It increases risk for both consumers and the parties they seek to transact with.

To fix this, America's paper-based systems should be modernized around a privacy-protecting, consumer-centric model that allows consumers to ask the government agency that issued a credential to stand behind it in the online world – by validating the information from the credential.

The creation of "Government Attribute Validation Services" can help to transform legacy identity verification processes and help consumers and businesses alike improve trust online.

Such services could be offered by an agency itself, or through accredited, privately run "gateway service providers" that would administer these services and facilitate connections between consumers, online services providers, and governments.

The Social Security Administration (SSA) and state governments – the latter in their role as issuers of driver's licenses and identity cards – are the best positioned entities to offer these services to consumers.

Note that the SSA is in the midst of building just the sort of Attribute Validation Service that we called for, the Electronic Consent Based Social Security Number Verification (eCBSV) Service. SSA is doing so in response to Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act, which was signed into law last year thanks, in part, to this Committee's work.

The eCBSV system will allow financial institutions and their service providers to electronically get a "Yes/No" answer as to whether an individual's SSN, name, and date of birth combination matches Social Security records.

We're thrilled to see SSA move forward here.

First, because eCBSV will change the game in the fight against synthetic identity fraud, which costs the country $6-$8 billion annually. The fact that fraudsters have been targeting the SSNs of children to commit this fraud is especially galling – eCBSV will give the country a tool to fight back.

And second, because what SSA is doing here provides a template for other agencies.

To that end, we were elated to see the White House Office of Management and Budget (OMB) embrace our recommendation for government to play a bigger role in identity proofing with the issuance in May of OMB Memorandum 19-17, entitled "Enabling

Mission Delivery through Improved Identity, Credential, and Access Management."

Page 8 of the memo[4] states:

> *"Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing· events, as selected by OMB and permissible by law, shall establish privacy-enhanced data validation APIs for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent.*
>
> *"These selected agencies, in coordination with OMB, shall establish standard processes and terms of use for public and private sector identity proofing services that want to consume the APIs."*

In the wake of this White House policy memo, the table is set for a new wave of tools that not only help fight identity theft and fraud, but also give consumers new ways to more easily do business online.

We were also thrilled to see the Treasury Department echo our idea of leveraging the identity proofing process tied to state driver's licenses in the report they put out last summer on "Nonbank Financials, Fintech, and Innovation." Per their report[5]:

> *"Treasury encourages public and private stakeholders to explore ways to leverage the REAL ID Act driver's license regime — particularly, robust state*

[4] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[5] https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

REAL ID license identity proofing processes — to provide trustworthy digital identity products and services for the financial sector."

Note that this concept was also embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity[6], who, in response to the wave of attacks leveraging compromised identities, stated "The government should serve as a source to validate identity attributes to address online identity challenges." Per the report:

"The next Administration should create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online.

"As part of this effort, the interagency task force should be directed to incentivize states to participate. States—by issuing drivers' licenses, birth certificates, and other identity documents—are already playing a vital role in the identity ecosystem; notably, they provide the most widely used source of identity proofing for individuals. Collaboration is key. Industry and government each have much to gain from strengthened online identity proofing. The federal government should support and augment existing private-sector efforts by working with industry to set out rules of the road, identify sources of attributes controlled by industry, and

[6] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

establish parameters and trust models for validating and using those industry attributes."

The Coalition is thrilled that government has begun to act on this recommendation – as evidenced by the OMB memo and the launch of the SSA initiative. But going forward, we think four more things are needed:

1) A formal government-wide initiative, led by the White House, dedicated to identifying which Federal agencies besides SSA are best suited to offering new consumer-centric identity services, as well as ensuring each agency has adequate resources to stand these services up.

2) Work at NIST to lead development of a framework of standards and operating rules to make sure these services are built in a way that sets a high bar for security and privacy.

3) The establishment of a formal "Identity Center of Excellence" in government that can develop a standardized architecture for these services which implements the framework, and assist selected agencies in getting these systems established.

4) A new grant program to provide funding to states to help them implement this architecture and framework in state DMVs – accelerating their transition to being digital identity providers.

These four initiatives could be accomplished by legislation or via an Executive Order – we don't have strong views as to which path is pursued, only that action is taken. We

would welcome the chance to work with the members of this committee on ways to drive these initiatives forward.

2. *Rethink America's use of the Social Security Number.*

Many of our woes in identity are linked to the rather bizarre way the United States has treated the Social Security Number over the last 80 years. I expect the history of the SSN is well known to this Committee, but I do think it's worth briefly pointing out some of the contradictions in policy around how it should be managed and used.

- First, the SSN is simultaneously presumed to be both secret and public. Secret because we tell individuals to guard their SSN closely. Public, because we also tell individuals to give it out to facilitate all sorts of interactions with industry and government. Secret because we tell those entities in both government and the private sector to ensure that if they store it – which the law often requires them to do – that it be protected. And public, because that's proven quite hard to do: to the point that the majority of Americans' SSNs have been compromised multiple times over the last several years amidst a wave of data breaches.

- Second the SSN is commonly used as both an identifier and an authenticator. As I will discuss today, years of breaches mean the SSN is of little value for authentication – but it is still quite valuable in the role it was first created for, as a unique identifier. Understanding this difference is key to crafting a solid strategy for the SSN's future.

- Third, the SSN system is managed by an agency not formally tasked with providing an essential element of the country's identity infrastructure. Yet the SSA finds itself in that role by default – and is increasingly being asked to do more.

These policy contradictions are not the result of anything malicious; on the contrary, they reflect years of trying to balance several important roles played by the SSN and the SSA. What's most important now is that the government 1) recognizes these contradictions, and 2) takes steps to put policies in place that are more consistent, and that put us on a path toward a system that enhances security, privacy and convenience for Americans.

That process starts by changing how we view the SSN and how we use it.

1. Up front, government should acknowledge that there is not a need to "replace" the Social Security Number (SSN) – at least not in the way that some have suggested in recent years. Rather, government should take steps to change how we use it.

   There's been a ton of discussion on this topic over the last two years as some industry and government leaders, along with security and privacy experts, have called for the country to come up with "something to replace the SSN."

   Unfortunately, the debate has been muddled by people failing to differentiate between whether the SSN is an identifier or an authenticator. Part of the confusion is that SSN has been used as both identifier and authenticator in recent years.

At its core, the SSN was created as an identifier. It is a 9-digit code, issued by the Social Security Administration at birth, that is used to help the government know "which Jeremy Grant" they should associate wage and tax data with, and to help administer the delivery of Social Security benefits. Over time, use of the SSN has expanded beyond the purposes for which it was intended, with thousands of private sector entities collecting the SSN as part of the account opening experience — and by credit reporting firms, data brokers, and other private firms, who have used the SSN as one way to aggregate and match data about a person.

These expanded uses of the SSN are all as an identifier. But where things have really changed is the practice of using the SSN as an authenticator. Every time a party asks for the last four digits of that number, for example, the premise is that the SSN is a secret — and thus possession of the SSN could be used to authenticate a person.

There was a time when SSN as authenticator made sense: someone's SSN was not widely known or publicly available, so it was safe to presume that it was a secret. But in 2019 — after several years of massive data breaches where millions of SSNs have been stolen — the notion that SSNs are a secret is a fallacy. The Equifax breach may have woken people up to this fact, but for several years now, SSNs have been widely available on the dark web for just a dollar or two.

The message is clear: data breaches have gotten bad enough that we should assume an attacker can get someone's SSN with only minimal effort. The

attackers have caught up to authentication systems that use SSN as a factor — it's time to move on to something better.

With this, we need to move beyond using the SSN as an authenticator. Beyond delivering immediate improvements to security, such a move would also lessen the value of SSNs to criminals and other adversaries.

2. Just because SSNs should no longer be used as authenticators does not mean that we need to replace them as identifiers. When architecting a system for security, identifiers don't have to be a secret – and many times it is desirable that they be known. Given that - rather than replace the SSN as an identifier, instead, let's start treating SSNs like the widely-available numbers that they are.

Doing this is the single best way to reduce the risks associated with use of the SSN as an identifier. If we shift everybody's mindset to one where everybody understands that SSNs are widely known – and design security systems that don't allow someone with just an SSN to use it to gain access to data or services – it effectively devalues the SSN as an attack point.

There have been a number of proposals suggesting that America should instead scrap the SSN and invest in creating a new, revocable identifier administered by the SSA.

I've yet to see any proposal that does not involve spending tens of billions of dollars and confusing hundreds of millions of Americans – with very little security benefit. The reality is that both government and industry would simply

map that new identifier back to the SSN and other data in their systems. Because the new and old identifiers would be connected, the security benefits would be close to nil.

Moreover, the possibility of chaos due to errors in mapping and matching these additional identifiers would be quite high, given that many government and commercial systems deliver less than 100 percent accuracy today; think about what might happen when a system fails to associate a new identifier with the right person.

Winston Churchill once said: "Democracy is the worst form of Government except for all those other forms that have been tried." So it is with the SSN – it's not a perfect identifier, but keeping it beats the alternatives.

Rather than create a new identifier, the focus ought to be on crafting better authentication solutions that are not dependent on the SSN, and are resilient against modern vectors of attack.

3. Back on the topic of identifiers: even if we assume that the SSN is publicly known, that doesn't mean that it needs to be used everywhere. Many of the members of the Better Identity Coalition would love to reduce where they use the SSN, due to the risks that collecting and retaining SSN may create relative to other identifiers. Our Blueprint documented how one of our members, Aetna, embraced a six-year, $60 million initiative to do just that – with great success. However, in some cases, they are running up against laws and regulations that

require companies to collect and retain the SSN. Our Policy Blueprint contains a 6-page appendix detailing some of these legal requirements. Among them:

- The Federal government requires employers to collect SSN each time they hire someone
- The Federal government requires financial institutions to collect the SSN as part of account opening or applying for a mortgage – and requires them to retain it for up to five years after the account is closed
- The Federal government requires college students to provide their SSN when applying for student loans
- The Federal government requires state governments to collect the SSN when Americans apply for a driver's licenses
- Health insurers are required by the government to collect the SSN of each person they insure
- Many states require blood donation services to collect and retain the SSN of blood donors
- The Coast Guard requires SSN to be collected as part of its Vessel Identification System

Much of industry's ability to reduce their reliance on the SSN will be dependent on the government changing its requirements for them to collect it.

Moreover, this list also demonstrates just how embedded the SSN is as an identifier in so many of our identity processes – and helps to frame the complexity and cost associated with any effort to replace it.

3. *Promote and Prioritize the Use of Strong Authentication*

On the authentication topic – we need to recognize that the problems with using SSNs as an authenticator extend to using any "shared secret" for authentication. It doesn't matter if the so-called "secret" is the SSN or passwords – they both are terrible.

As I mentioned earlier, 81% of 2016 breaches were enabled by compromised passwords, which is about as clear a sign as you can ask for that things need to change. There is no such thing as a "strong" password or "secret" SSN in 2019 and we should stop trying to pretend otherwise. We need to move the country to stronger forms of authentication, based on multiple factors that are not vulnerable to these common attacks.

There is good news in this regard: parts of government and industry have recognized the problems with old authenticators like passwords and SSNs – as well as other forms of authentication using "shared secrets" – and worked together these past few years to make strong authentication more secure and easier to use. Multi-stakeholder groups like the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium (W3C) have developed standards for unphishable, next-generation multi-factor authentication (MFA) that are now being embedded in most devices, operating systems and browsers, in a way that enhances security, privacy and user experience. Government should recognize the significance of this market development that is enabling authentication to move beyond the password, and embrace it.

What makes this possible is the fact that the devices we use each day have evolved. Just a few years ago, MFA generally required people to carry some sort of stand-alone security device with them. This added costs and often degraded the user experience. Moreover, these devices were generally not interoperable across different applications.

Today, however, most devices – be they desktops, laptops or mobile devices – are shipping from the factory with a number of elements embedded in them that can deliver strong, multi-factor authentication that is both more secure than legacy MFA technology and also much easier to use.

What are these elements?

1) Multiple biometric sensors – most every device these days comes with fingerprint sensors, cameras that can capture face and sometimes iris, and microphones for voice.

2) Special tamper-resistant chips in the device that serve as a hardware based root of trust – such as the Trusted Execution Environment (TEE) in Android devices, the Secure Enclave (SE) in Apple devices, or the Trusted Platform Module (TPM) in Windows devices. These elements are isolated from the rest of the device to protect it from malware, and can be used to 1) locally match biometrics on the device, which then 2) unlocks a private cryptographic key which can be used for authentication.

Together, these two elements enable the ability to deliver authentication that is materially more secure than older authentication technologies, and also easier to use. Because rather

than require the consumer to carry something separate to authenticate, these solutions are simply baked into their devices, requiring them to do nothing more than place a finger on a sensor or take a selfie.

The rest of the authentication (the other factors) automatically happens "behind the scenes" – meaning that the consumer doesn't have to do the work. A biometric matched on the device then unlocks a second factor – an asymmetric, private cryptographic key, that can then be used in conjunction with a public cryptographic key to securely log the consumer in, without a password or any other shared secret. The private key is stored in – and never leaves – the hardware device that the user controls.

While the actual composition of these two elements – both biometric sensors and security chips – varies across manufacturers, most of the companies involved in making these devices and elements have been working together to create the FIDO and related W3C Web Authentication standards. The power of these standards is that they enable all of these elements all to be used – interoperably – in a common digital ecosystem, regardless of device, operating system or browser. Which means that it's become really easy for banks, retailers, governments and other organizations to take advantage of these technologies to deliver better authentication to customers. Firms such as Aetna, PayPal, Google, Microsoft, Cigna, Intel, T-Mobile, Samsung, and several major banks are among those enabling consumers to lock down their login with FIDO authentication; the General Services Administration (GSA) recently enabled Americans logging into government websites with the Login.gov solution to protect their accounts with FIDO as well.

Note that FIDO also is the essential standard in Security Keys: external, portable hardware-based authenticators that can be used across multiple devices over interfaces including USB, NFC and Bluetooth. These Security Keys are widely used in devices and environments where built-in authentication is not available, as well as in environments where an external authenticator might be preferred to one that is built in.

Government can play a role in accelerating the pace of adoption of strong authentication through three key actions:

1) First, agencies should look to follow GSA's lead and make use of the FIDO and W3C Web Authentication standards in more of its own online applications. This will set an example for the private sector to follow – and ensure that citizen-facing applications are more secure and convenient to use. The SSA should be among the first here, given the importance of its MySSA online portal.

2) Second, through the regulatory process, government should ensure that regulated industries are keeping up with the latest threats to first-generation authentication – and implementing the latest standards and technologies to address these threats.

3) Third, when crafting new rules or guidance on privacy and security, it is important to make sure that language is not written so broadly that it might preclude use of promising technologies for risk-based authentication. As I noted earlier, when tools like FIDO are paired with analytics solutions that use Artificial Intelligence and Machine Learning

(AI/ML) to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords. However, the use of these promising analytics tools might be threatened if their use is inadvertently precluded by new privacy legislation or regulation.

In Europe, they seem to have gotten this balance right. While Europe's General Data Protection Regulation (GDPR) limits the collection of data in many circumstances, it also highlights that when it comes to protecting security and preventing fraud, there are cases where an entity may have a "legitimate interest" in processing personal data – including in cases where such data can be used to deliver secure authentication or verification capabilities. This "carve out" has allowed the use of data-based security and consumer protection solutions to flourish. In fact, the European Banking Authority (EBA) is specifically encouraging banks and fintechs to use these technologies to secure open banking and payments.

In contrast, California's recently passed California Consumer Privacy Act (CCPA) has more ambiguous language that some experts have interpreted as allowing consumers to opt out of having their data used to protect against malicious, deceptive, fraudulent, or illegal activity. This could inhibit the deployment of new, innovative authentication and verification technologies and place consumers at risk – and provides an example of

the potential consequences of overly prescriptive or poorly drafted policies or frameworks.

California's state legislature is considering some tweaks to CCPA that might address these concerns, but it is unclear if they will be adopted.

4. *International Coordination and Harmonization*

Consumers and businesses operate in environments beyond American borders, and other countries are also contemplating new approaches to making identity better. The United States should look for ways to coordinate with other countries and harmonize requirements, standards and frameworks where feasible and compatible with American values.

Coordination and harmonization is particularly relevant in the financial services industry, where a shift to digital banking and the emergence of "fintech" startups is disrupting traditional business practices – and challenging requirements for managing risks associated with the Customer Identification Program (CIP) requirements of the Bank Secrecy Act (BSA), as well as related Know Your Customer (KYC) and Anti-Money Laundering (AML) rules.

In the U.S., the push for "Open Banking" – where consumers are allowed to ask their bank to share their data with other firms such as account aggregation services or enable third parties to make payments from their account – is creating a need for more sophisticated identity solutions, as banks and fintech firms alike seek to enable consumers to authorize access to certain data or permissions in their accounts on a

granular level, and enable consumers to revoke access at any time. Robust identity solutions are at the heart of these applications, given the need to ensure that those authorization requests are coming from the right person, as well as comply with KYC rules for any new account opening.

Here, we think the U.S. should look to leverage ongoing work in the Financial Action Task Force (FATF) to ensure recognition of American identity solutions for digital financial services abroad, as well as explore the possibility of allowing U.S. financial institutions to leverage high-assurance digital credentials from other countries for foreigners looking to establish accounts in the U.S. The FATF is heavily focused on anti-money laundering and terrorist financing issues – particularly the role of better identity solutions in making it easier to address these critical concerns. The benefits of coordination and harmonization here could extend beyond financial services to encompass a wide array of digital commerce.

5. *Consumer and Business Education*

Finally, as part of improving the identity ecosystem, Americans must be aware of new identity solutions and how to best use them. Government should partner with industry to educate both consumers and businesses, with an eye toward promoting modern approaches and best practices. The National Cyber Security Alliance (NCSA) – which has a strong record of driving public/private partnerships to educate the public on cybersecurity – should be leveraged to promote better identity outcomes.

In closing, while the current state of digital identity poses some challenges to the financial service industry, they are not insurmountable. On the contrary, we have before us a series of ideas on the future of identity that can be used to address these challenges – and that are actionable today. I am grateful for the Committee's invitation to offer recommendations on how government can improve the identity ecosystem, and look forward to your questions.