Jeremy Grant
Coordinator, The Better Identity Coalition
and
Managing Director, Technology Business Strategy, Venable LLP

U.S. House Committee on Ways & Means
Subcommittee on Social Security

““Securing Americans’ Identities: The Future of the Social Security Number”

May 17, 2018

Chairman Johnson, Ranking Member Larson and members of the committee, thank you for the opportunity to discuss the future of the Social Security Number (SSN) with you today.

I am here today on behalf of the Better Identity Coalition[1] – a new organization launched earlier this 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, telecommunications, 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.

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

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

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. The SSN is a key component of America's identity infrastructure, and the sometimes conflicting roles that the SSN plays – which I will outline today – are a topic that impacts every American. 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. Last year, 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 private and state-sponsored adversaries seek to steal massive data-sets of Americans, including their SSNs. With these stores of data, they have an easier time compromising the questions used in "identity verification" tools like Knowledge-Based Authentication or Verification solutions (KBA/KBV). We've seen an uptick in breaches that exploit these tools as a result.

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 identity – and one's knowledge of his or her SSN has been a key component of these tools. The recent Equifax breach 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: "What should government and industry do about it now?"

I believe 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." To that end, it is important to talk not only about the future of the SSN, but also the role of the Social Security Administration (SSA).

The role of the SSA – and the future of the SSN

Up front, I would submit that 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.

1. 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.

2. 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.

3. 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.

I believe there are five areas where change is needed – and where this change can contribute to material improvements in the confidentiality, reliability and integrity of America's identity ecosystem, while also improving privacy and eliminating barriers to digital commerce.

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 months. Rather, government should take steps to change how we use it.

There's been a ton of discussion on this topic over the last few months 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 2018 — 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. 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 2018 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, and 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 to securely log the consumer in, without a password or any other shared secret.

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 Department of Veterans Affairs recently enabled Veterans logging into the Vets.gov website to protect their accounts with FIDO as well.

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

1) First, agencies should look to 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.

4. 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. However, in some cases, they are running up against laws and regulations that require companies to collect and retain the SSN.

   Among the legal requirements here:

   - 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.

5. Finally, any discussion of the future of the SSN also ought to include a discussion on the future of the SSA. The issue here goes beyond the future use of a 9-digit number to encompass a broader topic: what role should the government play in the future of the identity ecosystem?

While identity may not be a part of the SSA's mission statement, there is no question that SSA is in the identity business. It's time to acknowledge that fact – and then take a step back to contemplate what that means.

One of the biggest challenges the U.S. faces when it comes to digital identity is that the country has a number of authoritative government identity systems – the SSN included – which consumers, agencies and businesses have been able to leverage for <u>in-person</u> transactions. However, these systems are largely rooted in the physical world – based on cards and paper – at a time when commerce is moving to the online world.

Industry has tried to fill the gap with tools like so-called 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. But as I noted earlier, adversaries have caught up with these systems, and other first-generation tools that America has used for remote identity proofing and verification.

Against this backdrop, governments at both the Federal and State level should look to modernize their legacy identity systems 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 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.

To that end, the recent action by this Committee – and the full House – to advance H.R. 5192, the Protecting Children from Identity Theft Act, was a welcome development. The legislation would allow consumers to electronically request that the SSA validate whether SSA has a name, SSN and date of birth on file that matches the one they provide to a financial institution for certain kinds of account openings covered under the Fair Credit Reporting Act (FCRA).

The lack of such a service makes it much easier today for criminals to set up fraudulent accounts with "synthetic identities" using a fake name and a real SSN – often the SSN of a child.

Note that this new bill is not targeting SSN's use as an authenticator, only as an identifier; the goal is to enable consumers to request that SSA verify to a financial institution that a particular person with their name, date of birth and SSN actually exists. Enabling SSA to validate this information will lower the cost of digital transactions and close off a loophole that is commonly exploited by criminals to steal identities and fund illicit activities.

The bill is a great start, and I hope to see it become law this year. That said, it does not go far enough:

1) First, because as a consumer, I'd like to be able to ask SSA to help prove I am really me for a variety of different purposes online, not just opening a bank account.

2) Second, because it limits SSA to only validating three core attributes – Name, date of birth and SSN – when SSA also may have the ability to assist consumers by validating other attributes in SSA's systems.

Note that this concept was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity[2], 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 establish parameters and trust models for validating and using those industry attributes."*

Government should act on this recommendation, with a particular focus on having the Federal government 1) identify how SSA and other agencies can offer these services; 2) lead development of a framework of standards and operating rules to make sure this is done in a secure, privacy-enhancing way, and; 3) fund work to get it started.

As part of that effort, the SSA should be directed to outline what other attributes they may be in a position to validate.

In closing, while our current use of the SSN poses some challenges, they are not insurmountable. On the contrary, we have before us a series of ideas on the future of the SSN 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 SSN – and SSA's role in the identity ecosystem – for the future, and look forward to your questions.

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