Jeremy Grant
Managing Director, Technology Business Strategy, Venable LLP

U.S. House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

"Identity Verification in a Post-Breach World"

November 30, 2017

Vice Chairman Griffith, Ranking Member DeGette and members of the committee, thank you for the opportunity to discuss identity with you today.

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. Note that my testimony today represents my views alone; they are not the views of my firm.

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. 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. As my colleague Troy Hunt will discuss today, there are billions of compromised usernames and passwords out in the marketplace – his site "Have I Been Pwned" is a great resource to know if your account has been compromised. We need to kill the password.

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 identity. 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."

What has been done to date

Before I get into what government should do, I'd like to talk for a minute about what government has done – particularly over the last few years with the National Strategy for Trusted Identities in Cyberspace (NSTIC) – because there are some notable takeaways from the program that may help to inform where government and industry should focus in 2017 and beyond.

As background, the creation of NSTIC was driven, in part, by a key recommendation from the 2008 Commission on Cybersecurity for the 44th Presidency, which flagged the high prevalence of cyberattacks where identity provided an attack vector and called on the next Administration to take steps to address these issues.

Digital identity is a tricky issue, in that many countries address it through creation of a national ID system – something that we do not have in America for a number of good reasons. However, just because we do not have a national ID does not mean that we do not need a national identity strategy – identity is too challenging an issue, particularly in cyberspace, to solve without some government involvement, and too important to our economy to ignore. The approach the Obama Administration took was to recognize these issues, and craft a uniquely American strategy to tackle digital identity.

When it launched in 2011, NSTIC called for the government to collaborate with the private sector on development of an "identity ecosystem" – essentially a marketplace where all Americans could, in a few years, choose from a variety of different types of digital credentials that they could use everywhere they go online in lieu of passwords, and that would be more secure, convenient and better for privacy.

The role of the government in NSTIC was largely focused on two areas: First, how can government take steps to catalyze the market for NSTIC-aligned identity solutions? And second, are there barriers to better identity solutions that government needs to help remove in order to ensure that a robust identity ecosystem can flourish?

To do this, we focused on four areas:

1. Funding pilots – both to seed the marketplace with new, NSTIC-aligned solutions, as well as to learn what works well and what doesn't. Some of the most promising solutions to the identity verification challenges we are discussing in this hearing today emerged from these pilots; many of them featured participation from both government entities and the private sector.

2. Working on better standards – to help to measure the effectiveness of different identity technologies, and to make it easier for every stakeholder in the identity ecosystem to make use of these new solutions in the marketplace.

3. Getting US Government applications to embrace better identity solutions – which was helpful not only for purposes of enabling new high-value digital services, but also demonstrating to industry that the government was serious about this topic.

4. Focusing on governance – looking to bring together different stakeholders from the private sector to create a framework of standards and operating rules for the identity ecosystem. Part of that meant sorting out questions such as: What does it mean to be aligned with NSTIC? How would this be measured? And certified?

But above all these activities – the most important thing NSTIC did was having the President sign it. Because by throwing down a marker, the President got everybody's attention.

Companies that loved it came in to ask how they could get our help in making their next generation of identity products align with NSTIC and its vision of better security, privacy and convenience – that was a win for all Americans!

Companies that hated it – and to be clear, there were a few – still had to pay attention to it, and account for it in their product planning and roadmap. Because their customers would ask what they were doing to comply with it.

Six years after the strategy was published, the identity market has made significant progress. In some areas, more than others, however. If there is one takeaway I can offer about the state of the identity market post-NSTIC, 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. 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.

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 some of the tools we have depended on for identity proofing and verification. One example of the ways they have caught up are the terabytes of data that have been stolen through major breaches such as Equifax, which have captured Congress' attention this fall – and, I assume, led to the Committee calling this hearing.

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 ways to fix the problem – the market has not yet sorted things out here.

The good news is that some of the most promising approaches to better identity proofing emerged from pilots that the government funded through the NSTIC program. The bad news: funding for those pilots has been cut in the 2018 budget, while the challenges in the marketplace are greater than ever.

The history of what has happened to date is important for context setting. But as I stated earlier, the most important question is: "What should government and industry do about it now?"

What should government and industry do about it now?

I believe there are five areas where government can and should engage, and in doing so, 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 weeks. 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 weeks as industry and government leaders, along with security and privacy experts, have called for the country to come up with something to replace the SSN in the wake of the Equifax breach.

   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 and other data brokers, who have used the SSN as one way to aggregate 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 that 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 2017 — 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, government should start to push companies to stop 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.

However — and this is key — just because SSNs should no longer be used as authenticators does not mean that we need to replace them as identifiers. Instead, let's start treating them like the widely-available numbers that they are.

While it might be tempting to create a new, revocable identifier in response to the overuse (relative to its intended purpose) of the SSN, 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.

Rather than create a new identifier, the focus ought to be on crafting better identity vetting and authentication solutions that are not dependent on the SSN, and are resilient against modern vectors of attack. That tees up my next four recommendations:

2. Along with the SSN, we also need to recognize how useless passwords have become as authenticators. 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 in 2017 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.

   The reality is that very few compromises of passwords are executed by "brute force" attacks to crack the password. Instead, attackers either spear-phish someone into entering their password into a phishing site. Or they break into companies that store millions of user-name and password combinations and just steal them outright. In either case, it does

not matter whether a password has four characters or 24. Even the most complex password is still a "shared secret" that is easily compromised in 2017.

Beyond passwords: the problems with shared secrets extend well beyond passwords to also make other forms of first-generation multi-factor authentication (MFA) vulnerable. For example, "one time password" (OTP) technology – which generates a time-limited login code that is good for only 30 seconds – used to provide excellent protection against many attacks on passwords. But in 2017 the attackers have caught up – that 30 seconds is enough to phish or compromise an OTP. It is still a shared secret that both the user and the service provider know – and that creates routes for compromise.

The same issues apply to authentication codes delivered by text message, for example, using SMS. In addition to being phishable, malware can redirect text messages away from the intended device, including MFA codes. We have also seen attacks on the mobile network itself – attacking the SS7 protocol – to intercept MFA codes. And we're increasingly seeing mobile phone account hijacking (aka "SIM swap") attacks – taking over someone's phone account via social engineering, with the goal of stealing these codes.

The bottom line: these days, most attackers can successfully phish MFA based on shared secrets just about as easily as they can a password. The government needs to make it a priority to move the market to modern, unphishable authentication.

3. 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 efforts like the FIDO Alliance 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 a 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 standards. The power of FIDO 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. Major firms like Aetna, PayPal, Google, Microsoft, Bank of

America, Intel, USAA and Samsung 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 – first by enabling FIDO standards to be used in more of its own online applications. And second, through the regulatory process, by ensuring 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. As I mentioned earlier: while authentication is getting easier, identity proofing is getting harder, as attackers have caught up to first-generation solutions like static Knowledge Based Verification (KBV). Adversaries have targeted massive data-sets of Americans, in part, so that they have an easier time compromising the questions used in "identity proofing" tools like KBV.

   A notable challenge here is that KBV has been the de-facto standard for years, and while industry understands it's time to move to something better, the market has not yet – in my view – developed the logical successor. One reason: industry cannot do this alone. They need the government's help.

   Providing this help may be the single most meaningful thing government can do to improve identity. Government can do so through a relatively simple approach: allowing consumers to ask agencies that have their personal information to vouch for them. Let me detail what I mean:

While we do not have a national ID, most Americans have at least one government-issued identity document:

- At birth, you are issued a birth certificate, from the city or county you are born in.
- Also at birth, you are issued a Social Security Number from the Federal government.
- At or around 16, state governments issue a driver's license or state ID card – which, thanks to the Real ID Act of 2005, now requires an incredibly rigorous identity proofing process.
- If you travel outside the US, you go to the US Postal Service to apply for a passport or passport card – which is then manufactured by the US Government Publishing Office and issued by the State Department.
- If you go overseas a lot – as I do – you may go to DHS to enroll in the Global Entry program – getting another ID card.

That's five government-issued credentials that I have today – but all of them are stuck in the physical world.

Meanwhile, this past February when I went to open up a new bank account – to take out a loan – I had to appear in person at the bank so that they could validate my identity. The highly sophisticated process entailed me showing them my driver's license so they could ascertain if it looked real.

Which – in 2017 – seemed a bit ridiculous. I would have much preferred to simply log into the DC DMV with my FIDO security key and asked them to let my bank know who I was – in this case by sharing several attributes about me that the DMV had already validated. But that sort of system does not exist today in the United States.

If it did, it could solve many of our problems with identity verification in a post-breach world.

In 2017, consumers ought to be able to ask agencies that have their personal information to provide validated attributes about themselves to parties they seek to do business with. The Social Security Administration at the Federal level and Departments of Motor Vehicles (DMV) at the state level have the most to offer here.

- The Social Security Administration could make a significant dent in identity fraud by setting up a simple service to electronically verify that there really is a "Jeremy Grant" with a SSN and date of birth that corresponds to my name. 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 SSA offers a paper-based version of this service today – the Consent Based Social Security Number Verification (CBSV) Service – but requires that the requester provides a physical signature on paper from the applicant. In era where most everything is digital, this requirement, for all purposes, precludes this service from being used for real-time identity proofing. It's time to change that. Note that the CBSV is not tied to SSN's use as an authenticator, only as an identifier – it is used only to verify that a person actually

exists. Making the system digital could lower the cost of digital transactions and close off a loophole that is commonly exploited by criminals to steal identities and fund illicit activities.

- And in the states, the DMVs could help to pave the way for easier account openings that are more convenient and more secure. State DMVs already put people through a rigorous, in-person identity proofing process today – consumers should be able to leverage the fact that they went through this costly, time-consuming process to avoid having to go through similar hassles for other transactions.

Note that this concept was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity, 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 last December's report[1]:

> *"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*

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

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."

To date, I do not believe that the Trump Administration has acted on this recommendation. But I believe they should, with a particular focus on having the Federal government 1) lead development of a framework of standards and operating rules to make sure this is done in a secure, privacy-enhancing way and 2) fund work to get it started.

Note that some work was done in the previous Administration on this – the NSTIC program funded DMV-focused pilots in states including Virginia, North Carolina, Georgia, Colorado, Idaho, Maryland and Washington DC. The learnings from these pilots[2] should be leveraged to jumpstart the Commission's recommendation, with a particular focus on making sure such a system places the consumer and his or her rights and needs at the center of any new service. Since these services involve consumers' personal information – let's architect systems that are designed to put the consumer in control!

Toward that end, NSTIC also worked with industry to set up a privately-led Identity Ecosystem Steering Group (IDESG)[3] tasked with creating a framework of standards, requirements and best practices for modern, user-centric identity systems. This framework has been used in the state NSTIC pilots, and can serve as a guidepost for any future government offering here.

[2] See https://www.nist.gov/itl/tig/pilots
[3] More details at https://www.idesg.org/

5. Finally, government needs to support continued work on identity research and standards.

When I look at the positive impacts of NSTIC, one of the top items has been the emergence of a robust Trusted Identities Group in NIST's Information Technology Lab (ITL), focused on working with government and industry to develop better standards, guidelines and best practices for next-generation identity solutions. The publication of NIST's updated "Digital Identity Guidelines" this past summer is one example of the great work that NIST has done here[4] – it's a document that has been nearly universally praised around the world in taking a forward-thinking approach to digital identity.

Unfortunately, the FY 2018 budget proposed to cut funding for research and standards work in NIST's Trusted Identities Group, singling out NIST's work on biometrics for commercial and government applications.

From my perspective, this is an awful decision. Biometrics – if applied properly – offer one of the most promising tools to improving identity solutions. But the technologies on the market today vary widely in accuracy and reliability. Moreover, some ways in which biometrics can be deployed can enhance security and privacy, while other models present material security and privacy risks. If we're worried about "Identity Verification in a Post-Breach World," government should be increasing the government's budget for research as well as development of better standards and best practices in this area, not cut it back. The FY18 budget cut funding for what is literally the one office in government

[4] See https://pages.nist.gov/800-63-3/

that is tasked with working with industry on tools that can improve the reliability, security and privacy of biometrics and other next-generation authentication technologies.

In closing, America faces challenges at the intersection of identity and cybersecurity – but we also have some actionable ideas that we can implement to address these challenges. I am grateful for the Committee's invitation to offer my recommendations on how government can improve identity verification, and look forward to your questions.