**Testimony of Jeremy Grant – Coordinator, Better Identity Coalition**

**House Homeland Security Committee Subcommittee on Transportation and Maritime Security Hearing on *"Identity Management Innovation: Looking Beyond REAL ID"***

**December 5th, 2023**

Chairman Gimenez, Ranking Member Thanedar, and members of the committee, thank you for the opportunity to testify today.

I am here on behalf of the Better Identity Coalition – an organization focused on working with policymakers to improve the way Americans establish, protect and verify their identities when they're online.

Our members include leaders in sectors like financial services, health, technology, FinTech, payments, and security. Our 26 members are united by a common recognition that the way we handle digital 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.

Identity does not always get much attention, but is an important topic, in that 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But outdated identity systems enable a set of great attack points for criminals and other adversaries, such as hostile nation-states that are seeking to steal data and money and compromise American systems. And as these threats grow – and new systems are put in place to try to guard against them – they often create new burdens for consumers, businesses, and government agencies who need to accurately verify identity to enable high value transactions to be delivered online.

Five years ago, the Better Identity Coalition released a "Blueprint" for policymakers on how to improve digital identity infrastructure in America. The Blueprint highlighted the ways that

government can help deliver more secure, inclusive, privacy-preserving digital solutions – by closing the gap between the nationally recognized, authoritative credentials that work in the physical world – like driver's licenses, passports, and birth certificates – and the lack of any digital counterpart to those physical credentials that can be used when Americans need to prove who they are online.

Why is government action needed here? Well, at the end of the day, government is the only authoritative issuer of identity in the US. 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 government-issued credentials built to support digital transactions – is being actively exploited by adversaries to steal identities, money, and sensitive data, and defraud consumers, governments, and businesses alike.

And while industry has come up with some decent tools to try to get around this identity gap, adversaries have caught up with many of them.

Moreover, with the rise of artificial intelligence (AI) now enabling new types of attacks on digital identity (such as cheap and highly convincing deepfakes that can fool remote identity verification tools), the security and economic risks are more acute than ever. It is imperative that the US develop a strategy to ensure we have digital identity infrastructure that can mitigate and stay ahead of these threats.

Indeed most of our peer countries have either created robust digital identity infrastructure or has launched a national initiative to do so. Each year that passes without a comprehensive initiative to prioritize more robust, privacy-preserving digital identity infrastructure puts Americans at greater risk than the rest of the world and threatens our international competitiveness.

Going forward, government will need to take a more active role in working with industry to deliver next-generation remote identity proofing solutions. This is not about a national ID – and we do not recommend that one be created. We already have a number of nationally recognized, authoritative government identity systems – the driver's license, the passport, the SSN. But because of the "identity gap" these systems are stuck in the paper world, while commerce is increasingly moving online.

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

Digital driver's licenses – also known as "mobile" driver's licenses or mDLs – featured prominently in our Blueprint. This is by virtue of the fact that driver's licenses and state ID cards are by far the photo ID that is most commonly obtained by people in the US, and are thus the documents that are most commonly used to prove one's identity today in the physical world.

The single best way to prevent identity theft and identity-related cybercrime is to give Americans tools that they can use to protect themselves from identity thieves. mDLs have much to offer here, as they can enable Americans to reuse a high assurance credential they already have – their driver's license or state ID card – when they need to prove who they are online for high assurance transactions. And because the REAL ID Act of 2005 established a Federal standard for a robust, in person identity proofing process for states to follow, consumers can derive significant benefit if REAL ID compliant driver's licenses are enhanced to support digital transactions.

By binding proof of identity to a digitally signed mDL app housed securely in a smartphone, a mDL can help Americans be better protected against identity thieves. And if designed properly, a mDL can offer not just better security, but also better privacy and increased convenience when Americans need to prove who they are online.

We're thrilled to see this subcommittee focusing in on the issue of digital identity and what is needed beyond the REAL ID Act.

I expect a good deal of this hearing will focus in on the role that TSA is playing with regard to mobile driver's licenses and REAL ID. And I think it is important to say that I admire the work TSA is doing here, at least in regard to the subset of issues around identity that are a part of TSA's mission.

The more important question for this hearing to explore, in my view, is whether TSA alone should be in the lead? In that the things that TSA cares about with regard to digital identity are a relatively small set of issues relative to the broader set of issues at hand.

There are five key points we would like to emphasize today:

1. **First, when it comes to mobile driver's licenses, the government is prioritizing the wrong use cases.**

   There are essentially two core use cases for digital versions of state driver's licenses and ID cards:

- The first is in-person use cases, such as clearing a TSA security checkpoint, or proving age at a bar to buy alcohol. This is where you are presenting a digital version of the plastic card in your wallet that is instead stored on your phone.

- The second is remote or online use cases, where you need to prove who you are online, say, to open a bank account or apply for government services.

Of these two use cases, there are certainly some tangible benefits to the in-person applications – I discuss those later in my testimony – but viewed against the backdrop of a wave of identity-related cybercrime that is costing Americans hundreds of billions of dollars each year, the in-person applications look like a "nice to have."

This is because the numbers on the cybersecurity side are staggering, and they are impacting many different sectors:

- FinCEN recently revealed that $212 billion in transactions flagged in 2021 Suspicious Activity Reports (SARs) filed by banks were tied to some form of breakdown in the identity verification process.[1]

- The Government Accountability Office (GAO) reported that between $100-$135 billion in pandemic Unemployment Insurance (UI) benefits was lost to fraud during the pandemic. Funds were stolen both by organized criminals and state-sponsored actors, with compromised identities being used to enable the bulk of the theft.[2]

- The Identity Theft Resource Center (ITRC) – a non-profit which helps victims of identity theft – has stated that 2023 is shaping up to be the worst year ever for identity theft and data breaches.

Why are there so many problems here? As I stated earlier, attackers have caught up with many of the "first-generation tools" we have used to protect, verify and authenticate identity online, to the point that it is an anomaly when a major breach happens and some

[1] https://www.nextgov.com/digital-government/2023/09/212b-suspicious-activity-reports-fincenin-2021-concerned-identity-officials-report/390279/

[2] https://www.gao.gov/assets/gao-23-106696.pdf

sort of identity compromise is not the attack vector. There are many reasons for this – but the most important question is: What should government do about it now?

With nearly $350 billion in identity-related cybercrime documented in just two sectors – banking and government benefits – the deficiencies in digital identity infrastructure that enable most of this crime should be getting a ton of attention.

Instead – inexplicably, in my opinion – the US government has been prioritizing the in-person use cases for mDLs while giving little attention to the online use cases that could address this massive wave of identity-related cybercrime.

This is not to say that the in-person use cases have no value; on the contrary, there are notable improvements to security, privacy, and convenience that can be delivered by a properly designed mDL that is used for in-person use cases. The ability, for example, to let someone share elements of their ID such as age or state of residence on a granular basis – without revealing all of the information printed on their ID – can improve privacy. Likewise, having digitally signed data in a mDL app can offer security and anti-counterfeiting benefits above and beyond the security features that are built into plastic cards. However, when weighed against our most pressing problems in digital identity, these in-person use cases should not be the lead priority.

There is some background here worth sharing:

- The initial pilots of mDLs were funded by the National Institute of Standards and Technology (NIST) between 2012-2015, as part of the National Strategy for Trusted Identities in Cyberspace initiative. It's worth sharing here that I ran that program, and served as NIST's Senior Executive Advisor for Identity Management. The pilots were focused on the ways that a mDL could be used to help people when they had to prove who they were online for a high value service like banking or government benefits.

- However when Congress passed the REAL ID Modernization Act in 2020 to reflect the emergence in the market of mDLs, Congress did not specify which use cases were a priority. The law just more generally directed DHS to update regulations for REAL ID driver's licenses to support digital mDLs. Rather than focus on the applications of mDLs that can prevent identity theft and identity-related cybercrime, DHS instead delegated implementation of the law to TSA, who has largely focused on in-person use cases such as using a mDL to clear a TSA checkpoint.

One question to consider is if TSA alone should be in charge – especially when DHS originally led the REAL ID regulations out of its policy office back in 2005? We assume DHS made this decision because the "core use case" for REAL ID that impacts most Americans is whether they can use their driver's license to clear a TSA checkpoint.

However, that's a small subset of the use cases where digital identity matters, and many of these use cases are well outside of TSA's jurisdiction – among those, the online identity use cases that are not getting much attention.

2. **Second, our understanding is that the reason DHS and the states have both been focused on in-person use cases is because work is still ongoing in the International Standards Organization (known as ISO) to craft a standard for the online use cases of mDLs.**

   This is a terrible reason for the government to avoid focusing on a solving a problem that leads to hundreds of billions of dollars in identity-related cybercrime and millions of victims of identity theft. Indeed, it is hard to think of another security crisis where the government's response has been to say "let's hold off on solving it until the International Standards Organization gets things figured out."

   If ISO is moving too slowly, the United States should take the lead on creating its own standard, and work to advance it in ISO rather than sit back and hope that ISO eventually figures it out.

   While DHS does not create standards, DHS – or even better, the White House or Congress – should request that NIST lead a timeboxed, one-year effort to create the standards and guidance needed to accelerate the deployment of secure, privacy-protecting mDL apps that Americans can use to protect and assert their identity online.

   There is precedent for this here – indeed a number of ISO security standards are more or less based on work that NIST led first. For example, in 2013, when the Obama Administration determined that cybersecurity risks had reached a point that government action was urgently needed, President Obama signed an Executive Order that gave NIST one year to create a Cyber Security Framework (CSF). NIST released the CSF in 2014, and it has since become recognized across the globe as the preeminent framework for organizations to use to manage cyber risk. So much so that ISO then used it as the basis of a "formal international standard," leveraging the CSF content as the basis of both ISO 27103 and 27110. None of this would have happened without a recognition from the US government that government action was needed here to jumpstart progress.

Note that NIST has launched a small project here out of its National Cybersecurity Center of Excellence (NCCoE) focused on developing a reference implementation of the digital identity standard in partnership with industry. Some of the Better Identity Coalition's members are participating with NIST in this project; NIST has noted that outcomes of this project may result in contributions to the ISO standard currently being crafted. It's a good project that will help to move the ball forward – but bluntly, it's too small and too slow an effort relative to what is really needed here to accelerate the rollout of robust digital identity infrastructure.

3. **Third, TSA alone should not be in the lead here.**

I do want to complement the TSA team working on this, in that they get that there is a bigger set of issues at play beyond the use cases directly relevant to TSA's mission, and they have been working with NIST and other government stakeholders. TSA's proposed draft regulations here also include some elements dealing with the security of how a mDL is provisioned for in-person use cases that can be leveraged to also ensure a secure provisioning process for online use cases – they seem to be looking beyond the use cases that are in their scope.

That said, TSA's mission does not involve ensuring a safe and privacy preserving foundation for digital transactions in banking or health or government services, or other places where Americans might have a need for digital ID.

Nor does it include issues around identity inclusion, such as how to help people who might not have a driver's license or other government credential today – and who may not be able to easily get one. This is an important point to flag: Roughly ten percent of adults do not have a driver's license or state ID, and in many cases, people lack critical identity documents like birth certificates and Social Security cards needed to get one. This disproportionately impacts the most marginalized communities, including people of color, the elderly, the poor, as well as survivors of domestic violence and those reentering society after time in prison. As we talk about investing in new digital identity tools, it is important to make sure our most vulnerable neighbors are not left behind.

And so while I admire much of the work TSA is doing here – particularly how their team has taken some very forward-looking steps in their proposed draft regulations on mDLs to look ahead to solving some of these other issues, there is a bigger structural issue where TSA is limited in how much they can accomplish.

We desperately need to elevate protecting people from ID theft and identity-related cybercrime so that it is a national priority, not a transportation security priority.

4. **This brings up my fourth key point, which is that digital identity is a critical infrastructure issue and needs to be treated as such.**

   DHS said as much in 2019 when it declared identity as one of 55 "National Critical Functions" – defined as those services "so vital to the US that their disruption, corruption, or dysfunction would have a debilitating effect on security…"

   But compared to other critical functions, identity has gotten scant investment and attention. And it's a bit puzzling that DHS, after calling out digital identity as a critical function, has opted to focus so narrowly here as it implements the REAL ID Modernization Act of 2020.

5. **Finally, on that note, the White House could and should play a bigger role here, by launching a "whole of government" effort to address critical vulnerabilities in our "digital identity fabric."**

   The Administration actually had great language on digital identity in its March 2023 National Cybersecurity Strategy; Strategic Objective 4.5 of the Strategy called for the government to "Support Development of a Digital Identity Ecosystem" and stated:

   > *"Today, the lack of secure, privacy-preserving, consent-based digital identity solutions allows fraud to flourish, perpetuates exclusion and inequity, and adds inefficiency to our financial activities and daily life. Identity theft is on the rise, with data breaches impacting nearly 300 million victims in 2021 and malicious actors fraudulently obtaining billions of dollars in COVID-19 pandemic relief funds intended for small businesses and individuals in need. This malicious activity affects us all, creating significant losses for businesses and producing harmful impacts on public benefit programs and those Americans who use them. Operating independently, neither the private nor public sectors have been able to solve this problem."*

   Of note, the National Cybersecurity Strategy noted the role that mDLs could play, encouraging "a focus on privacy, security, civil liberties, equity, accessibility, and interoperability."

   We agree that all of these are important, and, indeed, essential. It is critical as mDLs are emerging that government defines what "good" looks like with regard to these credentials,

and puts a plan in place to make sure that we get there – and that we avoid bad outcomes that might arise if the architecture for mDLs is not properly designed to maximize benefits and minimize any potential harms.

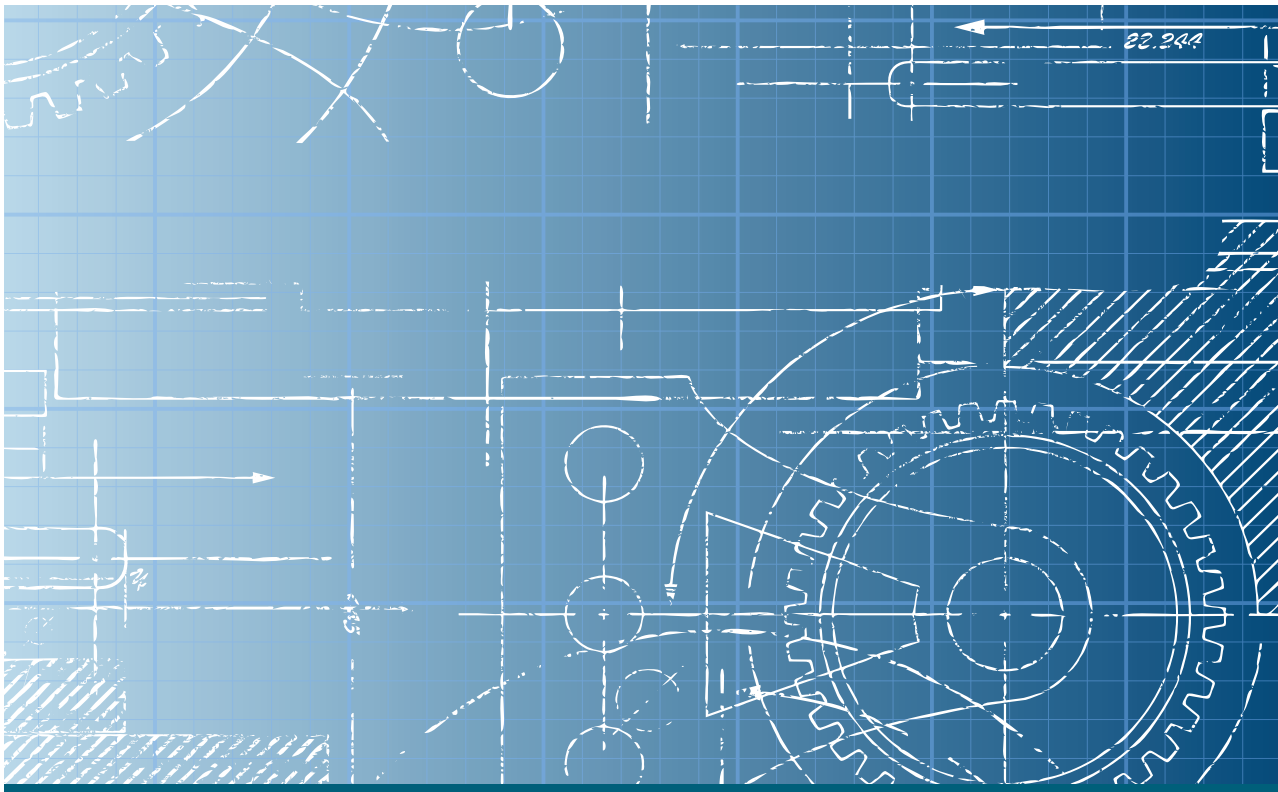
Unfortunately, when the implementation plan for National Cybersecurity Strategy was published in July, it inexplicably skipped over the identity section entirely – jumping from Strategic Objective 4.4. to 4.6, as if the identity objective was never in the Strategy. The Administration has said that identity might be addressed in future versions of the implementation plan, but for now this work has been sidelined. That means there is no vision of what "good" looks like to guide different agencies working on these issues, nor is there any plan to address some of the difficult inclusion issues I discussed earlier to make sure that we are not leaving anybody behind as we invest in better digital identity.

In the wake of White House inaction, Congress can help to drive progress. Last year a bipartisan bill that is based on our Policy Blueprint – the Improving Digital Identity Act – cleared the House Oversight Committee and the Senate Homeland Security and Governmental Affairs Committee (HSGAC), but came up just short of passage. That bill has been reintroduced in the Senate and passed the HSGAC in March , and is currently awaiting further action. As currently drafted, it falls under the jurisdiction of the House Oversight Committee and not the Homeland Security Committee, but the bill was sponsored by Democrats and Republicans on this committee – former Ranking Member John Katko and former Congressman Jim Langevin were original authors of the bill – and we'd love to explore ways this committee might be able to drive action forward.

Thank you for the opportunity to testify today. Note that I have submitted a copy of the Coalition's Policy Blueprint[3] for the record to augment this testimony; I look forward to answering your questions.

[3] The Blueprint can be found at https://www.betteridentity.org/s/Better_Identity_CoalitionBlueprint-July2018.pdf.

# Better Identity in America: A Blueprint for Policymakers



THE BETTER IDENTITY COALITION

July 2018

## ABOUT THE BETTER IDENTITY COALITION

The Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication.

The Coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity.

Founding members of the Better Identity Coalition are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, telecommunications, fintech, payments, and security. These companies include Aetna, Bank of America, IDEMIA, JPMorgan Chase, Kabbage, Mastercard, Onfido, PNC Bank, Symantec, U.S. Bank, Visa and Wells Fargo.

As government contemplates new policies to improve the quality of digital identity in the United States, the Better Identity Coalition is bringing together leading companies to help develop innovative ideas that improve security, privacy, and convenience for all Americans.

More on the Coalition can be found at https://www.betteridentity.org/ or by contacting info@betteridentity.org.

# TABLE OF CONTENTS

"Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network..."

"The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks."

- National Institute of Standards and Technology (NIST)

## EXECUTIVE SUMMARY

**Digital commerce in America is at a crossroads. Today, the variety of services available online is greater than ever before, offering consumers, businesses, governments and other entities the power to engage in all sorts of transactions from a device in the palm of their hand.**

But conversely, the ability to offer high-value transactions and services online is being tested more than ever, due in large part to the challenges of proving identity online. The lack of an easy, secure, reliable way for entities to verify identities or attributes of people they are dealing with online creates friction in commerce, leads to increased fraud and theft, degrades privacy, and hinders the availability of many services online. While the market has responded with an array of products that aim to address the identity challenge for specific use cases, the tools available today are uneven in accuracy and reliability, and are increasingly coming under attack.

$16.8 billion was lost in the United States due to identity fraud in 2017 – a year in which the Identity Theft Resource Center reported a 44.7% increase in the number of data breaches. In total, nearly 179 million records containing personal information were exposed in these breaches – a 389% increase in the number of records exposed.

As the number of impacted Americans grows, the privacy implications of existing identity tools – specifically the ways in which the inadequacy of some identity systems has placed consumers at risk – have made clear that consumers need better identity solutions that empower them to decide what information they share, when they share it, and in what context.

No incident highlighted the limitations of our current identity infrastructure more than last year's Equifax breach; the theft of sensitive personal data from more than 147 million people – including "secret" data that had been used by consumers and businesses to verify identities online – made clear that some of our legacy systems were no longer good enough. In the wake of the breach, a "policy window" has emerged, where government and industry have both expressed an interest in solving these problems, and, in some cases putting forth new ideas for how to do so.

The promise of new solutions here is exciting, as better identity solutions could not only address concerns with security and fraud, but also improve privacy and enable new types of trusted services to be offered to a wider swath of Americans online.

Consensus on a policy framework to enable better identity solutions has been difficult to establish, however, given the complexity of the issues at hand, as well as the extensive – but inadequate – legacy infrastructure in place today.

The members of the Better Identity Coalition came together to create a set of consensus, cross-sector, technology-agnostic policy recommendations for improving identity in America. Our recommendations – presented in this paper – do not purport to solve every challenge in the identity space. Rather, we have focused on a handful of common-sense initiatives that are practical to implement and will be meaningful in their impact; the Policy Blueprint we put forth in this document is squarely focused on making identity systems work better.

**Our Blueprint for Policymakers contains five key initiatives – some with multiple components:**

1. **Prioritize the development of next-generation remote identity proofing and verification systems.** The single biggest takeaway from recent breaches is that adversaries have caught up with the systems America has used for remote identity proofing and verification. The following four actions can help to accelerate the emergence of better identity proofing solutions in the marketplace:

   a. Governments should offer new digital services to validate attributes – modernizing legacy paper-based identity systems around a privacy-protecting, consumer-centric digital model that allows consumers to ask the 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 – are the best positioned entities to offer these services to consumers.

   b. The Federal government should create a five-year, $200 million-per-year grant program to provide seed funding to states enabling DMVs to modernize and become digital identity providers.

   c. Develop a forward-looking investment strategy for R&D and standards work in identity.

   d. Address policy and regulatory barriers that inhibit private sector entities from innovating around identity – and create incentives that promote adoption of innovations.

2. **Change the way America uses the Social Security Number (SSN).** Proposals to replace the SSN or ban some entities from using it are not feasible to implement, nor would they actually address the underlying challenges America has with the SSN. Instead government should:

   a. Frame every proposal about the future of the SSN on the basis of whether it looks to impact the use of the SSN as an authenticator, an identifier, or both.

   b. Stop using the SSN as an authenticator.

   c. Preserve use of the SSN as an identifier – but look to reduce its use wherever feasible.

   d. Consider changing laws and regulations that require companies to collect and retain the SSN.

   e. Avoid trying to replace the SSN – given that it would cost billions of dollars and create confusion for millions of Americans, while offering very little in terms of security benefits.

3. **Promote and prioritize the use of strong authentication.** Inherent in any policy change that removes use of the SSN as an authenticator is a way to replace it with something better. Government should continue work already underway in promoting strong authentication and update legacy policies that create barriers to its adoption.

4. **International coordination and harmonization.** The United States should pursue coordination with other countries – including in Europe with the eIDAS initiative and globally though the Financial Action Task Force (FATF) – with the goal of harmonizing requirements, standards and frameworks where feasible and compatible with American values.

5. **Educate consumers and businesses about better identity.** 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.

Note that there are no "moonshot" items in this Blueprint. This is by design: history has shown that lofty identity initiatives which aim to solve every problem struggle to get traction, given their complexity and difficulty. Instead, we have focused on a set of proposals that are both significant in impact and achievable – should government choose to act on them – in the next 2-3 years.

## I. INTRODUCTION

**There is no longer a question of if the United States has to act to improve identity – only how. Consensus on a policy framework to enable better identity solutions has been difficult to establish, however, given the complexity of the issues at hand, as well as the extensive – but inadequate – legacy infrastructure in place today.**

While concerns about security and fraud have elevated this issue, the issues at play also touch on privacy and consumer empowerment, as well as development of better trust models that can enable government and businesses to offer new types of high-value services to a wider swath of Americans online. When done right, identity can be "the great enabler" – helping to drive innovation and new, better ways of delivering services, while improving privacy, security and user experiences.

The members of the Better Identity Coalition came together to create a set of consensus, cross-sector policy recommendations for improving identity in America. Our recommendations – presented in this paper – do not purport to solve every challenge in the identity space. Rather, we have focused on a handful of common-sense initiatives that are practical to implement and will be meaningful in their impact; the Policy Blueprint we put forth in this document is squarely focused on making identity systems work better.

"The Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021."

- 2016 Report from the Bipartisan Commission on Enhancing National Cybersecurity

### History of identity in the United States (or "Where we are and how we got there")

There is no Federal law that requires Americans to obtain an identity card or any other identity credential. To be clear, for all purposes nearly every American needs to get a credential, since some sort of government-issued identity document is required to open a bank account, get a job, pay taxes, receive government benefits, drive a car, board a plane or purchase alcohol.[1] However, if someone does not need to do any of those things, there is no law that requires them to get an ID.

America's policy here stands in contrast to that of other countries that have a mandatory national ID. While the United States has long rejected efforts to create a national ID, the lack of such an ID does not mean that the United States does not have a government-backed identity system. Instead, a patchwork system has emerged of identifiers and credentials issued by a variety of different Federal, state and local entities. This patchwork has worked relatively well for in-person transactions where it was important to verify someone's identity; service providers could simply ask to see someone's credentials. However, the model has fallen apart online.

Nothing quite captured the extent of this challenge in the digital age like Pete Steiner's famous 1993 New Yorker cartoon; in 2018, it still perfectly describes our challenges with addressing identity online.


*"On the Internet, nobody knows you're a dog."*

While in some cases anonymity or pseudonymity online (being a "dog") is appropriate or desirable, there are many cases where individuals and businesses want or need to be able to definitively prove identity online. In these cases, our legacy systems have struggled; Americans remain dependent on paper – and plastic-based identity credentials, none of which were designed to be easily used – or validated – online.

The Federal government has tried three times over the last 16 years to leverage private sector solutions to fill the gap. Specifically, in an effort to not have the government be a digital identity provider, government instead launched initiatives based on public-private partnerships such as the Electronic Authentication Partnership (EAP), the Trust Framework Solutions (TFS) program, and the National Strategy for Trusted Identities in Cyberspace (NSTIC), focused on trying to get the private sector to create solutions that could solve the identity conundrum.

Outside of formal partnerships, the government has endorsed – by virtue of deploying it to manage access to the government's own resources – Knowledge-Based Verification (KBV) solutions as an alternative to government creating solutions to support digital identity requirements.

These past public-private initiatives have helped – a bit – but they have also made clear that there is no true substitute for the unique role that government plays as the authoritative source of conferring legal identity.

Moreover, in hindsight, they look like attempts to ignore the elephant in the room: that government alone confers identity authoritatively, and that government is thus in the single best position to address the challenges we have today and make identity better.

Not by issuing a national ID – but by allowing consumers to ask government that it stand behind the paper and plastic credentials it already issues in the physical world.

## Identity by the Numbers: The Cost of Outdated Identity Solutions

› **16.7 million** victims of identity fraud in 2017.[2]

› **$16.8 billion** stolen as a result of identity fraud in 2017.[3]

› **44.7%** - the increase in U.S. data breaches from 2016 to 2017.[4]

› **179 million** records containing personal information were exposed in 2017 breaches – a 389% increase over 2016.[5]

› **69%** of 2017 data breaches were identity theft incidents.[6]

› **30%** - the rate in which Online shopping fraud attacks rose in 2017, with criminals leveraging holes in e-Commerce identity services to perpetrate fraud.[7]

› **$6 billion** was lost to "synthetic" identity fraud in 2016, where criminals "synthesize" real-looking fake identities by combining real data from multiple individuals. This fraud often targets the SSNs of children, given that they have valid SSNs that are not yet being used to obtain credit; the impact is that many of them turn 18 only to find that they have a ruined credit history.[8]

› **81% of 2016 breaches** that exploited identity as an attack vector – using weak or stolen passwords to access systems and steal data.[9]

› **69%** of online shopping carts are "abandoned," meaning that consumers fail to complete a purchase online after beginning the process; 37% of those abandonments had to do with consumer frustrations about the account creation process.[10]

› **$150** million is spent by the largest financial institutions each year to comply with Anti Money Laundering (AML), Know Your Customer (KYC), and other identity-related compliance requirements.[11]

› **81%** of Americans say they would stop using a service that allowed their profile information to be stolen and leaked online.[12]

"Today, the information necessary to compromise identity is readily available to those who wish to find it."

- Greg Walden, Chairman, House Energy and Commerce Committee

### Industry filled the gap – but now attackers have caught up

Industry responded to the challenges posed by a lack of digital identity solutions with a number of novel approaches crafted with digital commerce in mind, such as Knowledge-Based Verification (KBV). As the name implies, KBV relied on a subject's ability to answer questions that were presumably secret – and thus answerable only by the individual being asked the question – in order to verify that someone was who they claimed to be and not a proverbial "dog on the Internet."

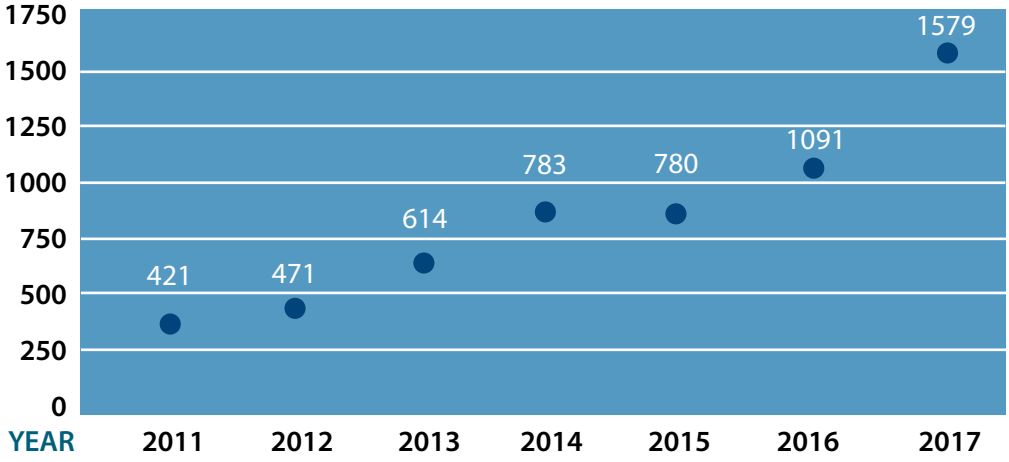
While these solutions were helpful for several years, they also became targets of attack for adversaries. Their goal has been simple: steal identity data in order to aggregate and analyze it – and then turn it against systems that used knowledge of personal data as a means of protection.

Indeed, the House Energy and Commerce Committee recently noted that one of the reasons large sets of personal data have been targeted over the last several years is that adversaries are able *"to combine multiple stolen data sets into one, thereby enabling them to obtain more complete "packages" of identity information"*[13] that can then be used to answer the questions served up by these "knowledge-based" identity systems.

This was illustrated quite vividly by the breach of the IRS's online "Get Transcript" application in 2015 – where more than 700,000 Americans had sensitive tax data compromised.[14] Here, IRS had a KBV solution in place, only to find that attackers were able to answer the questions the KBV system teed up using information stolen in previous breaches.

A number of Better Identity Coalition members also have seen stepped-up attacks on these knowledge-based systems and learned that merely answering the questions correctly cannot guarantee authenticity; one financial institution commented that if someone correctly answers a knowledge-based quiz too quickly, it is a signal that they might be dealing with an attack from a "bot" rather than a real human being.

#### NUMBER OF REPORTED DATA BREACHES




Source: Identity Theft Resource Center, https://www.idtheftcenter.org/images/breach/Overview20052017.pdf

Coalition members have also seen the rise of "synthetic" identity fraud, where fraudsters take advantages of weaknesses in our identity systems to create accounts under fictitious identities. In 2016, this fraud resulted in an estimated $6 billion of losses.[15]

The need for better identity solutions has been exacerbated by the wave of major breaches over the last five years. As House Energy and Commerce Committee Chairman Greg Walden noted in a hearing last year, *"Today, the information necessary to compromise identity is readily available to those who wish to find it."*[16]

Bottom line: adversaries have caught up with America's first-generation approaches to digital identity, in a way that inhibits commerce, fuels fraud and erodes trust. Identity solutions need to evolve and improve.

**Two Types of Identity Fraud**

- **Traditional Identity Theft:**
  Fraudster steals a victim's identity information to open a new account in their name

- **Synthetic Identity Fraud:**
  Fraudster establishes a fictitious identity to use for a new account – often by combining legitimate data elements (Name, SSN, DOB) from different identities with fraudulent elements

## II. BETTER IDENTITY IN AMERICA: A VISION OF THE FUTURE

While the identity ecosystem is fraught with problems, they are not ones that are unsolvable. On the contrary, many of the most glaring problems in digital identity are ones that can be addressed through active partnership between the public and private sector.

Before defining a plan of action, however, it is important to first lay out a high level vision of what "Better" means. Collectively, we believe that Better Identity in America means that the following outcomes have been achieved:

a. **Better Security – with Less Fraud and Identity Theft** – embracing the recommendation of the 2016 Commission on Enhancing National Cybersecurity that *"compromises of identity will be eliminated as a major attack vector by 2021."*[17]

b. **Better Convenience for Consumers** – allowing consumers to open new accounts with ease, without having to go through duplicative, burdensome enrollment processes.

c. **Better Confidence for Both Consumers and Service Providers** – that identities asserted online are reliable and trustworthy.

d. **Better Privacy** – shifting the predominant model for identity verification from one based on firms aggregating personal data without opt-in consent to one where consumers proactively request that their data be shared for the sole purpose of verifying identity.

## III. BETTER IDENTITY: HOW TO GET THERE

At the core of our recommendations is the belief that the private sector will not be able to solve America's identity challenges on its own. 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."

### Our Blueprint for Policymakers contains five key initiatives:

1. **Prioritize the development of next-generation remote identity proofing and verification systems**
2. **Change the way America uses the Social Security Number (SSN)**
3. **Promote and prioritize the use of strong authentication**
4. **Pursue international coordination and harmonization**
5. **Educate consumers and businesses about better identity**

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

As this paper has documented, 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. There are four steps that the government can take to improve identity proofing and verification:

#### > 1. Governments should offer new digital services to validate attributes.

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, 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.

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.

- SSA should 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 an organization for account opening.

- State DMVs should allow consumers to electronically request that the state which issued their driver's license validate whether the state has data on file (name, date of birth, address, driver's license number) that matches the one they provide to an organization for account opening.

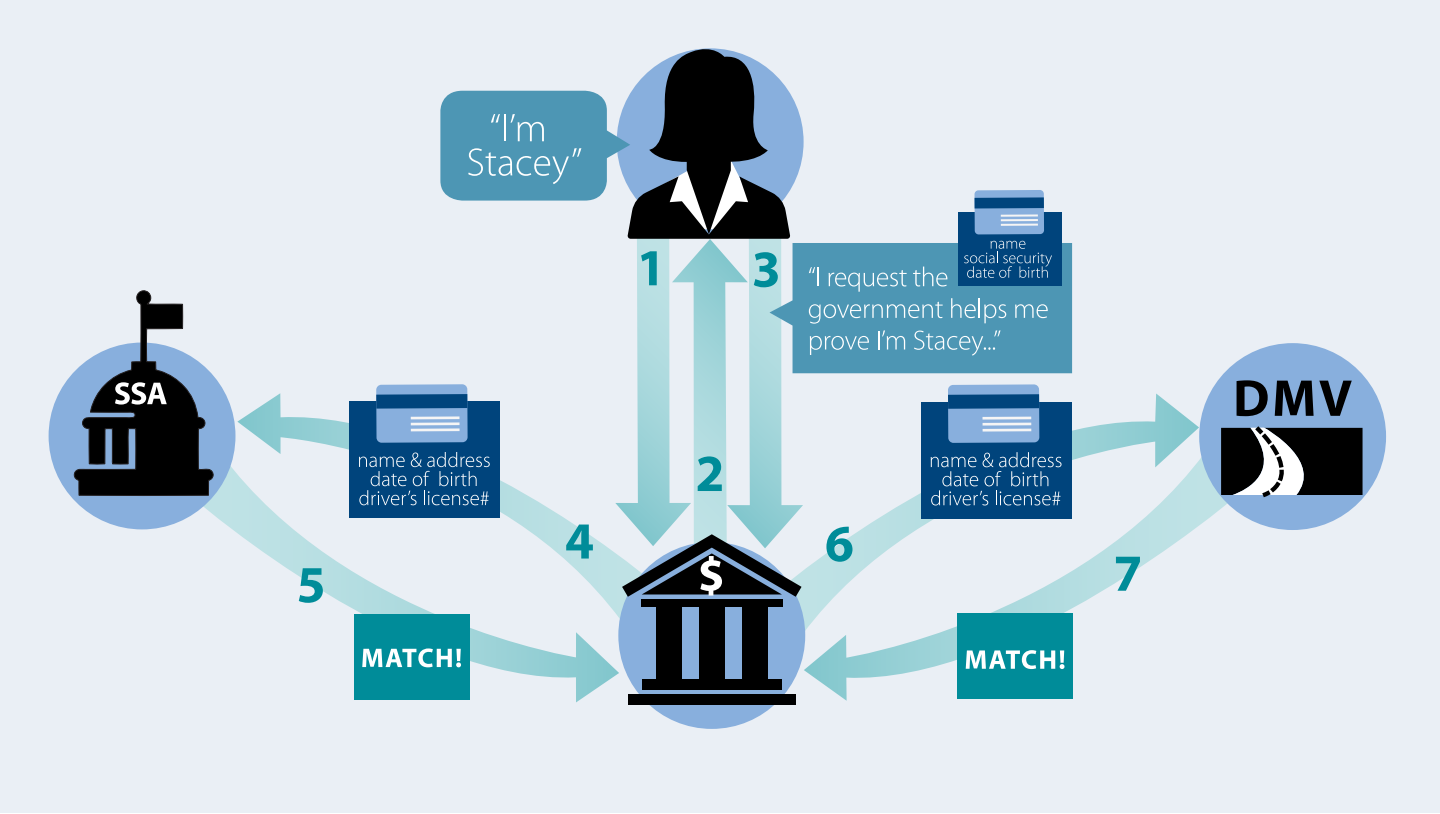
- State DMVs should offer consumer-facing services via new "mobile driver's license" (mDL) apps that allow consumers to easily leverage their physical driver's license card in the mobile world.

Each of these services could be supported by fees from commercial parties, who already pay today for reliable services that can eliminate fraud and streamline account opening and recovery processes.

Government – as the entity that conveys identity authoritatively – needs to play a larger role in the ecosystem if we are to deliver improved systems.

## Here is how this idea could work in practice for Stacey - a consumer opening a bank account online:

### SCENARIO 1: ONLINE ACCOUNT OPENING: GOVERNMENT AS A VALIDATOR OF ATTRIBUTES




1. Stacey would submit the information the bank requires for an application – much as she does today.
2. The bank would seek to validate that 1) the information she provided actually belongs to a real person, and 2) that the person applying for the account is actually Stacey.
3. Stacey would electronically request – through her bank – that SSA validate whether there really is an individual with her name, SSN and date of birth.
4. The bank would then ping SSA with this request – submitting these three attributes.
5. SSA will send a "yes/no" answer as to whether there is a match. Note that SSA is not sharing any of Stacey's personal information – they are only telling the bank whether that person actually exists in their records.

> ***Impact:*** *The bank now knows that the information provided by the applicant corresponds to a real person, with a legitimate SSN for tax reporting purposes. Synthetic identity theft attacks are averted.*

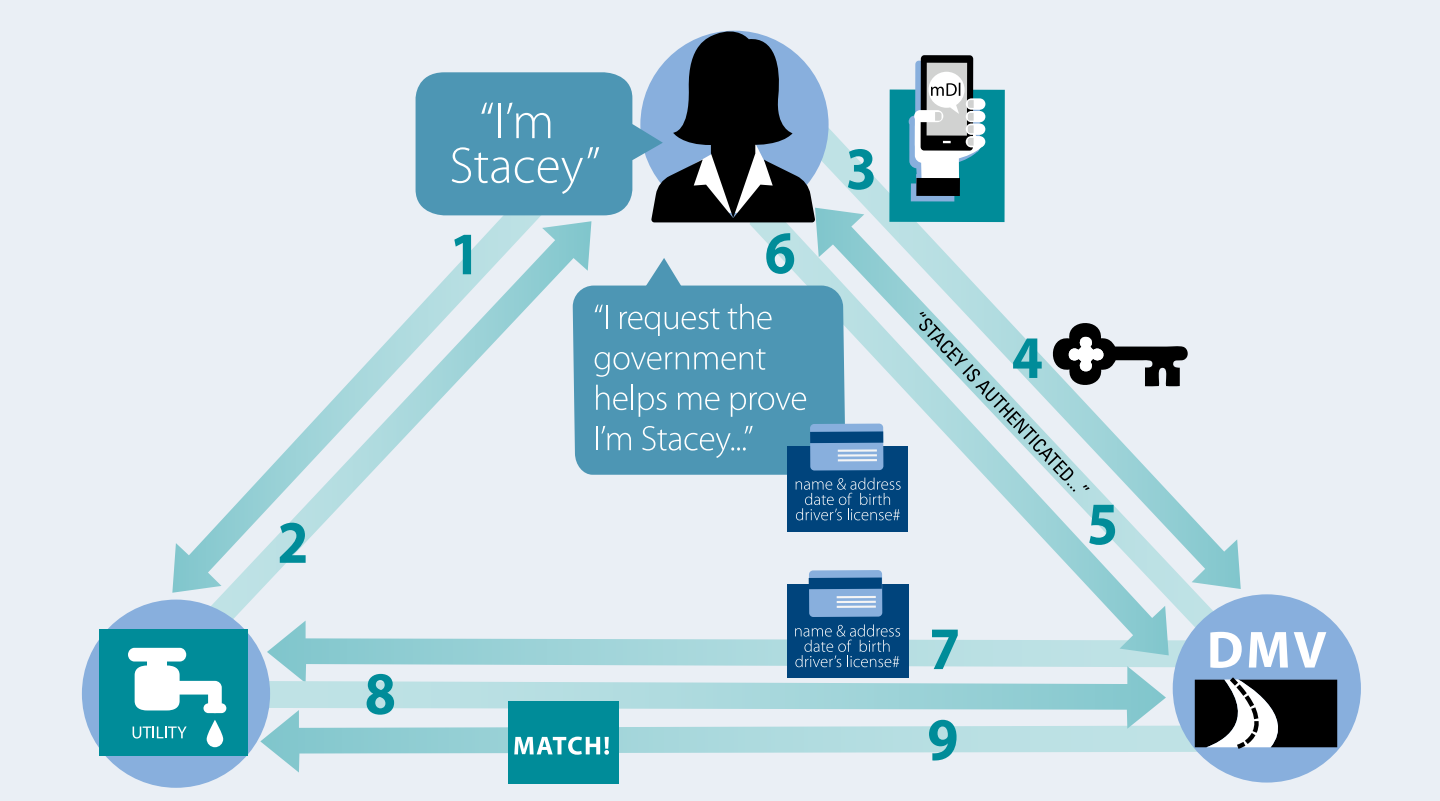
6. Stacey would electronically request – through her bank – that her state government validate whether there really is an individual with her name, address, date of birth and driver's license number. The bank would then ping the state with this request – submitting these four attributes.
7. The bank would receive a "yes/no" answer from the state as to whether there is a match. Again, the state is not sharing any of Stacey's personal information – they are only telling the bank whether that person actually exists in their records.

> ***Impact:*** *The bank now knows that the information provided by the applicant corresponds to a real person that is not only validated by the SSA, but also a state DMV. Synthetic identity theft attacks are averted.*

**The approach in the scenario below could be enhanced through new mobile Driver's License (mDL) apps offered by states – giving consumers more direct control over their data, including the ability to 1) directly authorize release of data for identity verification purposes, and 2) authenticate themselves through the app.**

**Here is how a new account opening using this app would work for Stacey – who is now opening an account online at a utility company, such as her local water department:**

## SCENARIO 2: GOVERNMENT APPS ENABLE CONSUMERS TO EASILY PROVE THEIR IDENTITY




1. Stacey would submit the information the utility requires for an application – much as she does today.
2. The utility would ask Stacey to help prove that 1) the information she provided actually belongs to a real person, and 2) that the person applying for the account is actually Stacey.
3. Stacey would click on a "Login with my mDL" link on the utility firm's website and then launch the "Mobile Driver's License" app on her smart phone. The app contains a digital version of her driver's license that was previously bound to her phone at the time the license was issued, containing all of the information that is on her printed license – and in the state's driver's license records.
4. The app securely logs her in with high-assurance FIDO multi-factor authentication leveraging 1) an on-device match of her biometric, which 2) then unlocks a private cryptographic key that corresponds with a public key tied to her account in the state's records.
5. Once the state authenticates she is in possession of the correct cryptographic key, she is logged in.
6. Stacey can now quickly authorize the state to validate to the utility that the information from her mDL app matches the information the DMV has about her.
7. The state then queries the utility for the information Stacey provided.
8. The utility sends it to the state.
9. The state then validates to the utility whether this data matches what is in their records.

> ***Impact:*** *The utility now knows 1) that the data Stacey provided matches the data in the state's driver's licensing records, and 2) that it was Stacey herself (and not a fraudster) who authorized the release of the information. Both synthetic and traditional identity theft attacks are averted.*

## DMVs and Identity: Potential Future Enhancements

In the future, this service could be augmented by new offerings from State DMVs that allow consumers to leverage their driver's licenses in additional ways to prove their identity online.

For example, a consumer in the future may be able to electronically request that the state which issued their driver's license validate whether a "selfie" image that they take matches the driver's license image on file in the state DMV. This validation service would effectively let a third party determine whether a remote user in possession of a driver's license is who they claim to be – rather than someone who might have stolen a license.

Likewise, the second scenario where a consumer can leverage cryptographically-signed, device-bound data from her driver's license is a future-state enhancement.

We do not believe states have the infrastructure or trust frameworks in place today to deliver such services today – and we address this issue in the next section. But with additional investments – and a proper framework of standards to ensure security and privacy – such a solution may be feasible five years from now.

**Two important items to note with the examples provided:**

- SSA and the state are not selling Stacey's data. Rather they are – at her request – validating that certain attributes about her exist in their systems. Everything is centered around Stacey's requirements – and no information is shared without her explicit authorization.

- SSA and the state could choose to charge for this service. Indeed, legislation recently passed by Congress and signed into law – which directs SSA to offer an attribute validation service to reduce fraud in financial services – calls for SSA to charge a fee to any company utilizing this service.[18] Given the value of the information, companies are willing to pay for it.

---

**This idea was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity**[19], which, in response to the wave of attacks leveraging compromised identities, set a clear goal for the country:

"The Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021."

As a key element of this action item, the Commission 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) Establish the interagency task force called for by the Commission to 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-preserving way. Through the NSTIC program, NIST funded work in a public-private partnership called the Identity Ecosystem Steering Group (IDESG); the framework it created may be relevant here.

3) Identify any legal or regulatory barriers that Federal or state agencies need to address to enable these services.

4) Fund work to get it started. We note that the proposed FY19 budget directs GSA to establish a new "Modernizing Identity Proofing" Program Management Office (PMO), focused on having GSA "work with agencies to identify public-facing systems that are vulnerable to fraud and ripe for new approaches to digital identity proofing, then pilot new and innovative methods of secure identity proofing." This office should be fully funded and empowered to drive action across government.

### Why State Governments and the SSA are Key

Government Attribute Validation Services do not need to be limited to states and the SSA; other government agencies may also be well-positioned to offer these services.

However, the SSA and State DMVs are the two entities best positioned to make a material impact on this topic.

In the absence of a formal national ID system, the SSN and driver's license together represent the two most important elements of America's government-administered identity system.

- The SSN is America's de-facto nation-wide identifier
- The driver's license – by virtue of it being the most commonly obtained photo ID (87% of the driving-age population has one) – is the document that is most commonly used to prove one's identity

To be clear, neither the SSN nor the driver's license is universal, and thus, getting SSA and states to offer attribute validation services will not solve America's identity problems for everybody. However, the perfect should not be the enemy of the good – these are two initiatives that can make things materially better.

The Driver's License is particularly unique:

- It is the one government-issued photo ID that the overwhelming majority of Americans obtain in their lives.
- Applicants must go through a rigorous in-person identity proofing process – equivalent to the highest Identity Assurance Level (IAL3) as defined by NIST[20] – at a government office to get one.
- The identity proofing process is now consistently robust across most states, given that the Real ID Act of 2005 established a Federal standard for states to follow.[21] We acknowledge

that the Real ID Act has been controversial, and we are not taking a position on the law. However, now that states and individuals both have to go through the process to comply with the Real ID Act, consumers can derive significant benefit if Real ID compliant driver's licenses are enhanced to support digital transactions.

The Driver's License is thus the credential that can reliably identify the greatest number of people at the highest level of assurance.

Moreover, states have already started piloting mobile driver's license (mDL) solutions in partnership with the Federal government. Under grants provided by the National Strategy for Trusted Identities in Cyberspace (NSTIC) program at NIST, states including Virginia, Georgia, North Carolina, Alabama, Colorado, Maryland, Idaho and Washington D.C. have all launched projects to pilot different aspects of this concept.[22] In addition, the American Association of Motor Vehicle Administrators (AAMVA) has launched an effort with the states and NIST to create standards that support this DMV-backed service.[23]

The success of these pilots and the ongoing standards work make clear that this is not a "pie in the sky" idea, but rather one that has been proven viable. The Federal government should provide additional support to these efforts to accelerate the pace – with the goal being a mDL offering that is ubiquitous across all 50 states.

Beyond SSA and DMVs, other agencies that may be suited to offer Government Attribute Validation Services include:

- The United States Postal Service (USPS) who performs identity proofing services for U.S. Passport applicants, and maintains authoritative data on name and addresses. In addition, USPS has recently launched a service to offer the same in-person identity proofing service it offers for the Passport for other parties.

- Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) – both of which require applicants to undergo an in-person proofing process for the Global Entry and TSA PreCheck programs.

- U.S. Citizenship & Immigration Services (USCIS) – who run more than 135 Application Support Centers (ASCs) across the country that are used to conduct in-person identity proofing for applicants for citizenship, Green Cards and visas. Given their focus, ASCs may be able to support identity verification for people who do not have a long history in the United States.

- Counties and cities – as the principal issuers of birth certificates and marriage licenses in the United States.

## Improving Identity While Preserving Privacy

As we noted in section II, Better Identity in America must deliver Better Privacy – shifting the predominant model for identity verification from one based on firms aggregating personal data without consent to one where data is shared only when consumers proactively request it.

Against that backdrop – it is important to note that the history of government identity systems, privacy and personal data has not always been a happy one. In 1994, Congress passed the Driver's Privacy Protection Act (DPPA) after issues arose with some state DMVs failing to properly protect personal information – leading, among other things, to a murder after a stalker obtained his victim's home address from a state DMV. The DPPA places strict limitations on who can access DMV data, and under what circumstances.

The DPPA does allow for DMVs to share data if the subject of that data consents[24] – meaning that the use case described above would be permitted under the law.

That said, new identity proofing solutions backed by government must be architected to protect privacy, not place it at risk. Beyond potential harm to individuals, protecting privacy is essential to gaining the trust of consumers to actually use these new solutions.

Accordingly, new identity proofing solutions should be crafted with a "privacy by design" approach. That means:

- Privacy implications are considered up front at the start of the design cycle -- and protections are embedded in the solution architecture
- Identity data is shared only when consumers request it
- Identity data that is shared is only used for the purpose specified
- Consumers can request release of information about themselves at a granular level – allowing them to choose to share or validate only certain attributes about themselves without sharing all their identifying data

This "privacy by design" approach is consistent with the European General Data Protection Regulation (GDPR), which has established a new high-water mark for consumer protection. Indeed, the European Union (EU) has recognized the importance of robust digital identity solutions as a critical component of protecting consumer privacy and enabling online commerce; the EU's eIDAS Directive complements GDPR by outlining ways for consumers to leverage digital identity solutions across borders in a way that is secure, privacy-protecting and convenient for consumers and businesses.

Amidst calls in the United States for comprehensive privacy legislation, the approach we have proposed here aligns with the requirements of GDPR.

It will be important to ensure that any new privacy laws or regulations in the U.S. take a similar approach to GDPR when it comes to consent – policies must be designed to allow consumers to control their data and enable them to request sharing of their attributes to deliver improvements in identity security, convenience and privacy.

> **2. The Federal government should offer grants to states to support their migration to being digital identity providers.** While states are in an ideal position to help transform digital identity, the costs involved to update and migrate legacy systems present a barrier that will inhibit states from moving forward. Many states are running their DMVs off of legacy infrastructure that is 20-30 years old, and is not capable of supporting the kinds of modern identity services envisioned in this paper.

The Federal government can help to catalyze the participation of state governments as offerors of privacy-protecting, consumer-centric digital identity solutions by providing grants to the states that assist with transition costs and incent states to play a larger role.

A five-year, $200 million-per-year Federal grant program will provide states with the seed money needed to invest their own resources in modernizing DMVs and other identity infrastructure.

This number is justified by a review of procurement data for the handful of DMVs that have conducted modernization efforts[25] over the last five years. Those efforts ranged in cost from $16 million to $85 million per state. Moreover, a review of state DMV presentations on these modernization efforts makes clear that their focus was primarily to retire old mainframe computer systems, not create new infrastructure capable of supporting digital identity transactions.

Given the costs of past modernization efforts – as well as the fact that most DMVs have yet to launch such efforts – there is $2.5-3 billion in unaddressed funding needs across U.S. DMVs to support their transition to becoming digital identity providers. While the Federal government should not bear this full cost, states are unlikely to launch these modernizations without seed funding.

Relative to the $16.8 billion lost in 2017 to identity fraud, this short-term infusion of capital into state identity infrastructures will provide a significant return on investment and deliver material reductions in identity fraud. There is a far greater cost to the market if states do not invest in modernizing their driver's license systems to support digital identity solutions.

Models worthy of consideration for these grants include:

- Federal Motor Carrier Safety Administration (FMCSA) grants, which provide funding each year to states to support improvements in commercial motor vehicle safety activities, including grants focused on improvements to state Commercial Driver's License (CDL) systems.[26] The fact that the Federal government previously established grant funding for state CDL programs to improve safety and security provides a precedent for Federal grants to support DMV grants to improve identity ecosystem security.

- The Driver's License Security Grant Program (DLSGP) and Real ID Demonstration Grant Program, which together provided more than $228 million from 2008-2011 to help states make upgrades to their driver's license systems to comply with the Real ID Act.[27] The program was administered by DHS. Here, the government did not cover the full costs of upgrades needed to support Real ID compliance; states leveraged these dollars alongside their own to fund these projects. The model proposed here is similar – with the Federal government providing seed funding that incents states to move forward with digital identity upgrades.

- 2018 Election Security Grants administered by DHS under the Help America Vote Act (HAVA). A pool of $380 million was made available to states under these grants, which states can apply for to fund investments in election security. Of note, Congress – when approving these funds – laid out specific criteria governing how states can use these dollars.[28] A similar approach could be used here – ensuring that dollars are only spent on specific improvements to identity systems focused on enabling consumer-centric attribute validation and mDL solutions.

### > 3. Develop a forward-looking investment strategy for R&D and standards work in identity.

While government has the ability to validate identity attributes today, the technologies we use in identity systems continue to evolve, as do the attack vectors employed by adversaries to break them.

The Federal government has a strong record of helping to drive advances in identity through its work supporting R&D and standards, as evidenced by its partnership with – and contributions to – standards crafted by organizations including the International Organization for Standardization (ISO), the Open ID Foundation and the FIDO Alliance. However, government investment has waned.

For example, the FY 2018 Administration budget 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. In addition, NIST has stopped funding innovative pilot projects in the identity space, as part of its efforts to scale back activity associated with the NSTIC program.

Beyond NIST cuts, there is no concrete Federal strategy for investments in this area. In addition to NIST, important work in R&D and standards for identity is performed by other agencies, including the Department of Homeland Security, the State Department and the Department of Defense.

The Federal government should develop a new, forward-looking investment strategy for R&D and standards work in identity that 1) ensures alignment in priorities across agencies, and 2) ensures that necessary work around identity is adequately funded.

Focus areas should include:

- Augmenting private sector-led R&D and standards work with other initiatives necessary to fill critical gaps
- Active partnership, where appropriate, with private sector standards efforts to ensure the government's perspectives and requirements are reflected in new standards
- Research and standards around privacy-preserving technologies in identity systems
- A framework that recognizes the role of the states, cities and counties alongside the Federal government as the issuers of identity documents (birth certificate, marriage, divorce, name change, adoption, death, etc.)

### > 4. Address policy and regulatory barriers that inhibit private sector entities from innovating around identity– and create incentives that promote adoption of innovations.

As technology – and threats – evolve, policy needs to evolve with it. There are a number of areas, however, where legacy rules and regulations are precluding the use of innovations that could improve identity solutions. In other cases, ambiguity over how old rules may be interpreted in response to new innovations is casting a "pall of uncertainty" that discourages the market from using these innovations. For example:

- Some states have enacted strict protections against commercial use of DMV data in response to privacy concerns – but have inadvertently created obstacles to a consumer requesting that a state share their data to assist the consumer with a transaction.
- Ambiguity from some financial regulators on the use of digital identity solutions has inhibited banks from embracing digital identity – as well as a broader role in the identity ecosystem by serving as identity providers to other sectors.
- Newly passed legislation focused on improving the use of digital identity technologies for new account openings at financial institutions may inadvertently preclude the use of advanced Artificial Intelligence (AI) and Machine Learning (ML) capabilities that can be used to better detect whether a driver's license is real or fraudulent. It could also make it easier for criminals to change the data on a real license in an attempt to use it for fraudulent purposes.[29]

At a time when the vulnerabilities of many first generation identity technologies are on full display, government needs to design policy and regulatory frameworks that embrace innovation in identity.

Likewise, the Federal government can help to catalyze the identity market by creating incentives to promote the adoption of new innovations. For example:

- The Federal government could incentivize use of new mobile driver's license (mDL) applications by stating that the Transportation Security Administration (TSA) will accept them at an airport checkpoints, and that the U.S. Postal Service (USPS) and the State Department will recognize them for passport applications.

- The Department of the Treasury should convene a Digital Identity Task Force that includes regulators in the Federal Financial Institutions Examination Council (FFIEC), focused on exploring how government policy can drive the adoption of more resilient digital identity solutions across the financial services market with a focus on reducing fraud, enabling innovation in financial services, and promoting financial inclusion.

- Government should formally recognize the role of identity trust frameworks – agreements laying out standards and operating rules that multiple parties agree to follow to ensure better identity practices. In the past, the government has gone as far as to formally certify private sector Trust Frameworks through a program run by the General Services Administration (GSA),[30] but this certification has never been recognized sufficiently by regulated industries, inhibiting Trust Framework adoption. This, in turn, has inhibited the growth and uptake of accredited private sector identity solutions that could complement government-run solutions.

## ACTION ITEMS

**To enable next-generation identity verification services, the Federal government should:**

1. Establish the White House led, interagency task force – as called for in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity – 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."*

2. Advance the work of the task force by funding the "Modernizing Identity Proofing" PMO called for in the FY19 budget – and also funding NIST to develop a framework of standards and operating rules that agencies at all levels of government can leverage to deliver attribute validation services in a way that is secure, designed around the needs of consumers, and protects privacy.

3. Stand up the service at the SSA called for in Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act to establish an attribute validation service for consumer financial applications that fall under the Fair Credit Reporting Act (FCRA).

4. Amend Section 215 to cover account opening use cases not covered by the FCRA where SSN must still be collected and verified.

5. Create a new five year, $200 million per year grant program to support states in their migration to being digital identity providers; work with the states and AAMVA to accelerate development of the mDL standard, and; incentivize adoption of mDL solutions by accepting them in lieu of traditional driver's licenses across the Federal government.

6. Develop a new, forward-looking investment strategy for R&D and standards work in identity that 1) ensures alignment in priorities across agencies, and 2) ensures that necessary work around identity is adequately funded.

7. Address policy and regulatory barriers that inhibit private sector entities from innovating around identity – and create incentives that promote adoption of innovations.

8. Convene a Digital Identity Task Force led by Treasury and including regulators in the Federal Financial Institutions Examination Council's (FFIEC), focused on exploring how government policy can drive the adoption of more resilient digital identity solutions across the financial services market.

**To enable next-generation identity verification services, state governments should:**

1. Work with the states, Federal government and AAMVA to accelerate development of the mDL standard and other standards to enable states to validate attributes.

2. Launch mDL and attribute validation offerings to enable citizens to more easily verify identity online.

## 2. Change the way America uses the Social Security Number (SSN).

A number of industry and government leaders have called for the country to develop a wholesale replacement for the Social Security Number (SSN) or ban some entities from using it. These proposals have helped to kick off an interesting discussion, however, they have not offered solutions that are feasible to implement, or that that would actually address the underlying challenges America has with the SSN.

| IDENTIFIERS | AUTHENTICATORS |
|---|---|
| Used to determine which of the 3,847 Jordan Pooles are a "particular Jordan Poole" | Used to determine whether the person claiming to be a "particular Jordan Poole" is in fact that person |
| **999-99-XXXX**<br>jordanp@foo.org<br>**@JordanPooleMI** | **Passw00rd**<br>  <br>  <br>  |
| Typically, this is a username or number. It may be widely known, but it is unique, and linked to a particular individual. | Typically, this is something a person possesses and controls (such as a password, a biometric, or a cryptographic key). It should not be widely known. |

Nevertheless, with every breach where SSNs are targeted, it has become clear that the way the SSN is used today must change.

**There are five steps that the government should take to change – and improve – the way we treat the SSN.**

> **1. Frame every proposal about the future of the SSN on the basis of whether it looks to impact the use of the SSN as an authenticator, an identifier, or both.** Many proposals around the SSN have muddled the debate by failing to differentiate between whether the proposal targets the use of 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. Understanding this differentiation is essential to constructing proposals about how the SSN should be used going forward.

The SSN was first created as an identifier: a 9-digit code, issued by the Social Security Administration at birth, that is used to help the government know "which John Doe" they should associate wage and tax data with, and to help administer the delivery of Social Security benefits[31].

Over time, the use of the SSN as an identifier has expanded beyond the purposes for which it was intended. Other government agencies have collected it to assist with the administration of other government services. And thousands of private sector entities have started to collect the SSN as part of the account opening experience – in some cases because of a legal requirement, in other cases, as a way to leverage this unique identifier to assist with private sector business operations.

There is a reason the SSN is so widely used as an identifier: both government and industry have found that identifiers are essential to operating services. Moreover, there are advantages – particularly when vetting an individual for new account openings – to leveraging a common identifier that transcends domains.

More recently, public and private sector entities alike have also started using the SSN as an authenticator: something that can be used to verify that someone is who they claim to be. Every time a party asks for the last four digits of an SSN, for example, the premise is that the SSN is a secret — and that possession of the SSN could be used to authenticate a person.

Every proposal to replace the SSN – or change how it can be used – must be framed up front to explain whether the goal is to address its use as an identifier, as an authenticator, or both.

**> 2. Stop using the SSN as an authenticator. Use of the SSN as an authenticator rests on the idea that the SSN is a "secret" – and that knowledge of an SSN can thus be used to prove that someone is who they claim to be.** There was a time when using the 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 years of massive data breaches where millions of SSNs have been stolen — most Americans have had their SSN compromised by at least one bad actor; its value as an authenticator is thus diminished.

The Equifax breach may have highlighted this fact, but for several years now, SSNs have been widely available on the dark web for just a dollar or two. 58% of Americans 18 years and older had their SSN compromised as a result of the Equifax breach alone.

Government and industry alike need to move away from using the SSN as an authentication factor – and migrate to alternative solutions that can more securely authenticate consumers. Authentication is an important enough issue that it merits its own section (#3) which follows.

To support this migration, the President should issue an Executive Order which precludes Federal agencies from using the SSN for authentication. Such an approach would improve the Federal government's security, and also send a strong signal to the private sector that they should look to migrate to more secure authentication solutions.

**> 3. Preserve use of the SSN as an identifier – but look to reduce its use wherever feasible.** While the SSN has been grossly overused as an identifier relative to its intended purpose, the risks involved with using it as an identifier are much smaller relative to those associated with its use as an authenticator.

Indeed, when architecting a system for security, identifiers don't have to be a secret – and many times it is desirable that they be known. The key assumption in such a system is that the identifier is treated as a widely-available number. Building systems with this assumption has the effect of devaluing the identifier; it is not presumed to be secret and thus has no security value on its own.

Under this paradigm, a devalued SSN is still appropriate for continued use as an identifier. Moreover, given that thousands of legacy systems in industry and government rely upon the SSN as an identifier, it will take years and significant investment to reduce or eliminate the use of the SSN.

Key to continued use of the SSN as an identifier is ensuring that the broader security model of each system is one that presumes the SSN is widely known; once the security architecture reflects this presumption, the SSN's value to adversaries and criminals is diminished.

That said, it still makes sense – where feasible – for companies and governments to look to reduce their use of SSN as an identifier – and look to protect it better where it continues to be used. Many members of the Better Identity Coalition believe that using SSN beyond government-mandated applications has become a risk for companies, and are taking steps to reduce the number of instances of SSNs in their systems in favor of single-domain or context-specific identifiers.

## CASE STUDY: Aetna and its six-year effort to reduce use of SSNs

In 2014, Aetna launched the SPEaR (SSN Protection, Elimination, and Remediation) initiative – a comprehensive program to reduce Aetna's reliance on the SSN by limiting its use only to those cases where the firm had legal or regulatory requirements for usage.

This was not a change that could be made overnight, nor was it one without significant costs: the SPEaR initiative will take six years to fully implement and cost Aetna approximately $60 million. The cost and duration of the initiative is largely driven by the fact that Aetna, like many large firms, had dozens of legacy systems, forms, and data sets that included the SSN. Change requires a material investment.

To date, Aetna has eliminated more than 10 billion instances of SSNs in its systems through the SPEaR initiative, leveraging a three-pronged "Remove, Replace, Protect" approach:

- The primary goal is **Removing SSNs** wherever possible – many legacy systems and forms included SSNs despite no clear need to do so.
- Where there is a need for a record or system to use a unique identifier, Aetna has pursued a strategy of **Replacing SSNs** with alternative identifiers wherever possible.
- In instances where a legal or regulatory requirement necessitates the continued use of the SSN, Aetna has prioritized **Protecting the SSN** through a risk based, layered approach to protection which includes field level encryption.

This three-pronged approach to SSN reduction has helped to mitigate risks to Aetna customers, as well as the firm itself.

One challenge in implementation has been that Aetna interacts with hundreds of other providers and vendors in the healthcare ecosystem – including the Federal government – that remain reliant on the SSN as an identifier. Thus, even when a single firm is committed to reducing use of the SSN, the requirements of business partners can make it difficult to fully eliminate its use.

Beyond that, the best way to reduce the risk of using the SSN as an identifier is to devalue its appeal to adversaries by treating SSNs like the widely available numbers that they are.

> **4. Consider changing laws and regulations that require companies to collect and retain SSN.** A major driver for the overuse of the SSN – and a major hindrance to changing the way it is used in America – has been government itself.

Appendix A of this document outlines 19 distinct government requirements – embodied in both laws and regulations – which require non-Federal entities in different sectors to collect SSNs. For example:

- Employers must collect an SSN each time they hire an individual
- Financial institutions must collect their customers' SSNs when they open an account or apply for a mortgage – and are required to retain it for up to five years after the account is closed
- College students must provide their SSN when applying for student loans
- State governments must collect the SSN – per Federal law – when Americans apply for a driver's license
- Health insurers must 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 SSNs to be collected as part of its Vessel Identification System

As this list of requirements demonstrates, even when industry wants to reduce its reliance on the SSN, there are cases where they are precluded from doing so given legal requirements.

Much of industry's ability to reduce its reliance on the SSN will be dependent on the government changing its requirements for industry to collect it. While Congress took an initial step toward this in 2010 with the passage of the Social Security Number Protection Act, the list above demonstrates that more may need to be done.

Moreover, this list 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. The government should not seek to replace the SSN.** A number of proposals from both government and industry have called for the Social Security Administration (SSA) to create a new, revocable identifier that would replace the SSN.

This would be a mistake – a wholesale replacement to the SSN would cost billions of dollars and create confusion for millions of Americans, while offering very little in terms of security benefits.

While some argue that the SSA can use new technology to eliminate the problems we have with SSNs today, the reality is that the introduction of a new identifier would require both government and industry to 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, each time this new identifier is revoked and reissued due to a security concern, dozens of systems would need to be updated. The likelihood 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: thousands, if not millions of problems will occur when a system fails to associate a new identifier with the right person.

As a general rule, to be useful across multiple systems a widely used identifier must be persistent, meaning that it stays constant over time.[32] The complexities induced by shifting an identifier to one that is not persistent – but revocable – are significant.

As a country, America clearly needs to replace the SSN as an authenticator – something that is quite feasible, as detailed in the section below. But government should refrain from any effort to replace the SSN with a new identifier, and instead focus on how SSA can play a more constructive role in the identity ecosystem going forward.

## ACTION ITEMS

1. Government and industry alike need to move away from using the SSN as an authentication factor – and migrate to alternative solutions that can more securely authenticate consumers. To ensure the government can lead the way, the President should issue an Executive Order banning agencies from using the SSN as an authenticator.

2. Congress and/or the Administration should launch a task force charged with reviewing existing laws and regulations that require the use of the SSN and identifying whether any can be changed.

**3.** **Promote and prioritize the use of strong authentication.** Inherent in any policy change that prohibits use of the SSN as an authenticator is a way to replace it with something better. Here, the problem is not just with SSNs, but also with passwords and other "shared secrets" that are easily compromised by adversaries.

No attack vector is as frequently exploited as the shared secret: Verizon's 2017 data Breach Investigations Report found that 81% of all breaches were enabled by compromised passwords. That number means it is an anomaly when a breach occurs and identity is not the attack vector. There is no such thing as a "strong" password or "secret" SSN in 2018 and America should stop trying to pretend otherwise. The country needs to move to stronger forms of authentication, based on multiple factors that are not vulnerable to these common attacks.

The good news here is that industry and government have recognized the problems with old authenticators like passwords and SSNs, and worked together these past few years to make strong authentication easier. Multi-stakeholder efforts like the Fast Identity Online (FIDO) Alliance, the World Wide Web Consortium (W3C), and the GSMA have developed standards for next-generation authentication that are now being embedded in most devices, operating systems and browsers, in a way that enhances security, privacy and user experience.

In addition, we've seen the emergence of technology that can deliver continuous risk-based authentication – applying data from dozens of data points that can be used to create a "risk score" that determines how much and what access to provide.

A risk-based approach is critical to ensuring that digital applications deliver the right level of strong authentication. Both government and industry should look to leverage risk-based guidance such as NIST's Digital Identity Guidelines (SP 800-63-3),[33] which lays out a comprehensive approach to assessing risk and selecting appropriate authentication controls to address those risks.[34]

The Federal government should continue work already underway in promoting strong authentication in sectors such as financial services, health care, government and consumer applications, as well as modernizing rules that govern use of strong authentication and reducing barriers to its adoption.

An important consideration for policymakers when crafting new legislation or regulation on privacy and security is to make sure that new rules are not written so broadly that they might preclude use of promising technologies for risk-based authentication. For example, 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.[35]

To that point:

- Recital 47 of GDPR states: *"The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."*

- Recital 49 of GDPR states: *"The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.*

  *"This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopped 'denial of service' attacks and damage to computer and electronic communication systems."*

Likewise, the recently passed California Consumer Privacy Act of 2018[36] creates an exception for requirements to delete personal information about a consumer if that information: *"is necessary for the business or service provider to maintain the consumer's personal information in order to…Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity."*

If other states were to pass laws that applied a different standard to use of data for protecting security and preventing fraud, it could have a chilling effect on the market – as companies would then have to grapple with a variety of laws across 50 states that each sets its own definitions, standards, and requirements for security and fraud prevention. Such a patchwork approach could inhibit the deployment of new, innovative authentication technologies and place consumers at risk.

## ACTION ITEMS

a. The Administration should enforce Executive Order 13681,[37] which requires "all agencies making personal data accessible to citizens through digital applications (to) require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."

b. The "Lock Down Your Login" initiative[38] – jointly developed by industry and government to promote the importance of strong authentication to consumers and businesses – should be reinvigorated and expanded, with a focus on providing more practical implementation guidance to businesses on how to deliver stronger authentication to employees and customers.

c. Where government offers guidance to industry on use of strong authentication – including in regulated industries – the government should look to modernize rules that govern use of strong authentication.

d. States should avoid creating new restrictions that might preclude use of promising technologies for risk-based authentication that can assure security and prevent fraud.

**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.

As the U.S. develops better identity solutions to address these challenges, it should explore how they can be aligned with global efforts in this area, such as Europe's eIDAS initiative and ongoing work in the Financial Action Task Force (FATF). Doing so can help to streamline the ability of Americans to more easily transact business on the global stage.

eIDAS[39] is an initiative of the European Union (EU) to ensure interoperability of different member-state identity credentials across all of Europe – allowing, for example, a French citizen to use her ID card to prove her identity to a business in Portugal. There is significant focus in Europe on how eIDAS may be able to be leveraged to assist banks with new account opening – particularly when it comes to meeting KYC, AML and Payment Services Directive 2 (PSD2) legal obligations.[40] The U.S. government should move to recognize eIDAS for KYC and AML purposes involving European applicants for American accounts, and also seek to have U.S. identity solutions recognized under eIDAS in Europe.

Likewise, the U.S. should look to leverage ongoing work in the FATF[41] 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.

## ACTION ITEMS

1. The Administration should task the Department of the Treasury with developing and executing a plan to engage with the eIDAS office in the European Commission, with an explicit focus around ensuring harmonization of international account openings.
2. The Administration should task the Department of the Treasury with developing and executing a plan to engage the FATF, with an explicit focus around ensuring harmonization of international account openings.

## 5. Educate consumers and businesses about better identity.

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.

### ACTION ITEMS

1. The Administration should partner with NCSA to develop a new initiative focused on educating both consumers and businesses about identity.

## IV. NEXT STEPS - A CALL TO ACTION

### The United States faces a clear choice:

We can sit back and fail to modernize our identity policies. Identity-related breaches will keep getting worse and legacy solutions will continue to fail – a step that will likely create additional barriers to the availability of services online, and erode trust in digital commerce.

Or we can take a proactive approach and take action to get ahead of the identity conundrum – a step that will position the U.S. to address security challenges and enable new digital products to thrive.

This Blueprint for Policymakers lays out a clear set of policy initiatives that are both significant in impact and achievable – should government choose to act on them – in the next 2-3 years.

The Administration, Congress and state governments should each move to advance the initiatives outlined in this Blueprint, with an eye toward a market where identity is the great enabler – driving trusted digital service delivery in a way that enhances security, privacy, convenience and innovation.

## ACTION PLAN: A PATH TO BETTER IDENTITY

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

Adversaries have caught up with the systems America has used for remote identity proofing and verification. Next-generation solutions are needed that are not only more resilient, but also more convenient for consumers.

#### ACTION ITEMS

**To enable next-generation identity verification services, the Federal government should:**

1. Establish the White House led, interagency task force – as called for in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity – 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."*
2. Advance the work of the task force by funding the "Modernizing Identity Proofing" PMO called for in the FY19 budget – and also funding NIST to develop a framework of standards and operating rules that agencies at all levels of government can leverage to deliver attribute validation services in a way that is secure, designed around the needs of consumers, and protects privacy.
3. Stand up the service at the SSA called for in Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act to establish an attribute validation service for consumer financial applications that fall under the Fair Credit Reporting Act (FCRA).
4. Amend Section 215 to cover account opening use cases not covered by the FCRA where SSN must still be collected and verified.
5. Create a new five year, $200 million per year grant program to support states in their migration to being digital identity providers; work with the states and AAMVA to accelerate development of the mDL standard, and; incentivize adoption of mDL solutions by accepting them in lieu of traditional driver's licenses across the Federal government.
6. Develop a new, forward-looking investment strategy for R&D and standards work in identity that 1) ensures alignment in priorities across agencies, and 2) ensures that necessary work around identity is adequately funded.
7. Address policy and regulatory barriers that inhibit private sector entities from innovating around identity – and create incentives that promote adoption of innovations
8. Convene a Digital Identity Task Force led by Treasury and including regulators in the Federal Financial Institutions Examination Council (FFIEC), focused on exploring how government policy can drive the adoption of more resilient digital identity solutions across the financial services market.

**To enable next-generation identity verification services, state governments should:**

1. Work with the states, Federal government and AAMVA to accelerate development of the mDL standard and other standards to enable states to validate attributes
2. Launch mDL and attribute validation offerings to enable citizens to more easily verify identity online.

### 2. Change the way America uses the Social Security Number (SSN).

The SSN plays a unique role in America's identity infrastructure, serving as both an identifier and an authenticator. With every breach where SSN's are targeted or exploited, it has become clear that the way the SSN is used must change.

#### ACTION ITEMS

1. Government and industry alike need to move away from using the SSN as an authentication factor – and migrate to alternative solutions that can more securely authenticate consumers. To ensure the government can lead the way, the President should issue an Executive Order banning agencies from using the SSN as an authenticator.
2. Congress and/or the Administration should launch a task force charged with reviewing existing laws and regulations that require the use of the SSN and identifying whether any can be changed.

**3. Promote and prioritize the use of strong authentication.** Inherent in any policy change that prohibits use of the SSN as an authenticator is a way to replace it with something better. Here, the problem is not just with SSNs, but also with passwords and other "shared secrets" that are easily compromised by adversaries.

### ACTION ITEMS

1. The Administration should enforce Executive Order 13681, which requires *"all agencies making personal data accessible to citizens through digital applications (to) require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."*
2. The "Lock Down Your Login" initiative – jointly developed by industry and government to promote the importance of strong authentication to consumers and businesses – should be reinvigorated and expanded, with a focus on providing more practical implementation guidance to businesses on how to deliver stronger authentication to employees and customers.
3. Where government offers guidance to industry on use of strong authentication – including in regulated industries – the government should look to modernize rules that govern use of strong authentication. Government should embrace multi-stakeholder efforts like the Fast Identity Online (FIDO) Alliance, the World Wide Web Consortium (W3C), and the GSMA, who have developed standards for next-generation authentication.
4. States should avoid creating new restrictions that might preclude use of promising technologies for risk-based authentication that can assure security and prevent fraud.

**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 or frameworks where feasible and compatible with American values.

### ACTION ITEMS

1. The Administration should task the Department of the Treasury with developing and executing a plan to engage with the eIDAS office in the European Commission, with an explicit focus around ensuring harmonization of international account openings.
2. The Administration should task the Department of the Treasury with developing and executing a plan to engage the FATF, with an explicit focus around ensuring harmonization of international account openings.

**5. Educate consumers and businesses about better identity.** 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.

### ACTION ITEMS

1. The Administration should partner with NCSA to develop a new initiative focused on educating both consumers and businesses about identity.

# APPENDIX A

## Federal Laws and Regulations Related to Obtaining and Maintaining Social Security Numbers (SSNs)

As this paper details, much of industry's ability to reduce its reliance on the SSN will be dependent on the government changing requirements for different sectors to collect, retain and use it.

The list below outlines 19 separate laws and regulations detailing Federal requirements for collection, use and retention of Social Security Numbers and other identity information. The list demonstrates just how embedded the SSN is as an identifier in so many U.S. identity processes – and helps to frame the complexity and cost associated with any effort to replace it. We appreciate the assistance of the Financial Services Roundtable (FSR) in compiling the financial services portion of this document.

| STATUTE or REGULATION | SOCIAL SECURITY NUMBER REQUIREMENT |
|---|---|
| **A. Financial Services** | |
| **Customer Identification Program**<br><br>*31 C.F.R. § 1020.220* | **Prior to opening an account**, the bank/thrift/credit union must, at a minimum, obtain the customer's name, date of birth, address (residential or business), and an **identification number** (can be taxpayer identification number).<br><br>The bank must retain identifying information for **five years after the account is closed**. |
| **Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks**<br><br>*31 C.F.R. § 1010.415* | **No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for $3,000 or more in currency unless it maintains records of the following information,** which must be obtained for each issuance or sale of one or more of these instruments to any individual purchaser which involves currency in amounts of $3,000-$10,000 inclusive:<br><br>**If the purchaser does not have a deposit account with the financial institution:**<br><br>(A) The name and address of the purchaser;<br><br>(B) The **social security number** of the purchaser, or if the purchaser is an alien and does not have a social security number, the alien identification number;<br><br>(C) The date of birth of the purchaser;<br><br>(D) The date of purchase;<br><br>(E) The type(s) of instrument(s) purchased;<br><br>(F) The serial number(s) of the instrument(s) purchased; and<br><br>(G) The amount in dollars of each of the instrument(s) purchased.<br><br>Records required to be kept shall be retained by the financial institution for a period of **five years** and shall be made available to the Secretary upon request at any time. |

| | |
|---|---|
| **Beneficial Ownership**<br><br>*31 C.F.R. § 1010.230 (effective May 11, 2018)* | Financial institutions are required to obtain, verify, and record the identities of the beneficial owners of legal entity customers.<br><br>As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and **social security number** or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.<br><br>A financial institution must retain the records for **five years** after the date the account is closed. |
| **Application for a residential mortgage loan (Truth in Lending Act)**<br><br>*12 C.F.R. §§ 1026.3(a)(3)(ii); 1026.25* | For residential mortgage transactions, an application consists of the submission of the consumer's name, the consumer's income, the consumer's **social security number** to obtain a credit report, the property address, an estimate of the value of the property, and the mortgage loan amount sought.<br><br>A creditor shall retain evidence of compliance for **two years** after the date disclosures are required to be made or action is required to be taken. |
| **Red Flags Rule**<br><br>*12 C.F.R. pt. 334, App.J (and corresponding regs)* | Requires financial institutions and creditors to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.<br><br>Each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:<br><br>• Social security number has not been issued or is listed on the Social Security Administration's Death Master File<br>• Lack of correlation between the SSN range and date of birth<br>• The SSN provided is the same as that submitted by other persons opening an account or other customers. |
| **Duties of Consumer Reporting Agencies Regarding Identity Theft**<br><br>*12 C.F.R. § 1022.123* | **Consumer reporting agencies shall develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity** where the consumer asserts a good-faith belief that have been a victim of identity fraud or a related crime.<br><br>**Examples of information** that might constitute reasonable information requirements for proof of identity are provided for illustrative purposes only:<br><br>*Consumer file match.* The identification information of the consumer including his or her full name (first, middle initial, last, suffix), any other or previously used names, current and/or recent full address (street number and name, apt. no., city, state, and zip code), full nine digits of **Social Security number**, and/or date of birth. |

| | |
|---|---|
| **Disclosure by CRA of Consumer File to Consumer; Free Annual Report;**<br><br>*15 U.S.C. §§ 1681g, 1681h, 1681j(a); 12 C.F.R. pt. 1022, subpart N.* | Every consumer reporting agency shall, upon request, clearly and accurately disclose to the consumer **all information in the consumer's file** at the time of the request, except that if the consumer to whom the file relates requests that the first five digits of the SSN not be included, and the reporting agency has adequate proof of the identity of the requester, the reporting agency shall so truncate the disclosure.<br><br>A CRA shall require, as a condition of making that disclosure, that the consumer furnish **proper identification**.<br><br>Free Annual Reports: There is a centralized source for requesting annual file disclosures from nationwide CRAs which collects only as much **personally identifiable information** as is reasonably necessary to properly identify the consumer and to process the transaction requested by the consumer.<br><br>Any **personally identifiable information** collected from consumers as a result of a request for annual file disclosure, or other disclosure required by the FCRA, made through the centralized source, may be used or disclosed by the centralized source or a nationwide consumer reporting agency only:<br><br>(1) To provide the annual file disclosure or other disclosure required under the FCRA requested by the consumer;<br><br>(2) To process a transaction requested by the consumer at the same time as a request for annual file disclosure or other disclosure;<br><br>(3) To comply with applicable legal requirements, including those imposed by the FCRA and this part; and<br><br>(4) To update personally identifiable information already maintained by the nationwide consumer reporting agency for the purpose of providing consumer reports, provided that the nationwide consumer reporting agency uses and discloses the updated personally identifiable information subject to the same restrictions that would apply, under any applicable provision of law or regulation, to the information updated or replaced. |
| **B. Employment** | |
| **Income Tax Collected at Source**<br><br>*Enacting legislation does not have a specific name. Public Law 96-601 is titled "An Act" "to simply certain provisions of the Internal Revenue Code of 1954, and for other purposes."<br><br>*26 U.S.C. § 3402* | A request that an annuity or any sick pay be subject to withholding under this chapter… shall be made by the payee in writing to the person making the payments and shall contain the **social security number** of the payee. |
| **Verification of Identity and Employment Authorization**<br><br>*8 C.F.R. § 274a.2* | A person or entity that hires or recruits or refers for a fee an individual for employment must ensure that the individual properly completes section 1 - "Employee Information and Verification" - on the Form I-9 at the time of hire.<br><br>Section 1 of Form I-9 includes a field for **social security numbers**. |

| C. Education | |
|---|---|
| **Returns Relating to Higher Education Tuition and Related Expenses**<br><br>Taxpayer Relief Act of 1997<br><br>*26 U.S.C. § 6050S* | Any person: (1) which is an eligible educational institution which enrolls any individual for any academic period; (2) which is engaged in a trade or business of making payments to any individual under an insurance arrangement as reimbursements or refunds (or similar amounts) of qualified tuition and related expenses; or (3) except as provided in regulations, which is engaged in a trade or business and, in the course of which, receives from any individual interest aggregating $600 or more for any calendar year on one or more qualified education loans, **shall make the return** described in subsection (b) with respect to the individual at such time as the Secretary may by regulations prescribe.<br><br>**A return** is described in this subsection if such return: (1) is in such form as the Secretary may prescribe, and (2) contains: (A) the name, address, and **TIN** of any individual (i) who is or has been enrolled at the institution and with respect to whom transactions described in subparagraph (B) are made during the calendar year… |
| **Social Security Number**<br><br>*34 C.F.R. § 668.36* | [T]he Secretary attempts to confirm the **social security number** a student provides on the Free Application for Federal Student Aid (FAFSA) under a data match with the Social Security Administration. If the Social Security Administration confirms that number, the Secretary notifies the institution and the student of that confirmation.<br><br>An institution may not disburse any title IV, HEA program funds to a student until the institution is satisfied that the student's reported **social security number** is accurate. |
| **D. Healthcare** | |
| **Reporting of Health Insurance Coverage**<br><br>The Patient Protection and Affordable Care Act<br><br>*26 U.S.C. § 6055* | Every person who provides minimum essential coverage to an individual during a calendar year shall, at such time as the Secretary may prescribe, make a **return** described in subsection (b).<br><br>A **return** is described in this subsection if such return: (A) is in such form as the Secretary may prescribe, and (B) contains (i) the name, address and **TIN** of the primary insured and the name and **TIN** of each other individual obtaining coverage under the policy… |
| **Eligibility Determinations**<br><br>The Patient Protection and Affordable Care Act<br><br>*42 U.S.C. § 18081* | An applicant for enrollment in a qualified health plan offered through an Exchange in the individual market shall provide:<br><br>(A) the name, address, and date of birth of each individual who is to be covered by the plan (in this subsection referred to as an "enrollee"); and (B) the information required by any of the following paragraphs that is applicable to an enrollee.<br><br>The following information shall be provided with respect to every enrollee: (A) In the case of an enrollee whose eligibility is based on an attestation of citizenship of the enrollee, the enrollee's **social security number**; (B) In the case of an individual whose eligibility is based on an attestation of the enrollee's immigration status, the enrollee's **social security number** (if applicable) and such identifying information with respect to the enrollee's immigration status as the Secretary, after consultation with the Secretary of Homeland Security, determines appropriate. |
| **Eligibility Process**<br><br>*45 C.F.R. § 155.310* | The Exchange must require an applicant who has a **Social Security number** to provide such number to the Exchange. |

| **E. Driver's License** | |
|---|---|
| **Minimum Issuance Standards**<br><br>REAL ID Act<br><br>*49 U.S.C. § 30301 note* | To meet the requirements of this section, a State shall require, at a minimum, presentation and verification of the following information before issuing a driver's license or identification card to a person: (A) A photo identity document, except that a non-photo identity document is acceptable if it includes both the person's full legal name and date of birth; (B) Documentation showing the person's date of birth; (C**) Proof of the person's social security account number or verification that the person is not eligible for a social security account number**; (D) Documentation showing the person's name and address of principal residence. |
| **Application and Documents the Applicant Must Provide**<br><br>*6 C.F.R. § 37.11* | (1) Except as provided in paragraph (e)(3) of this section, individuals presenting the identity documents listed in § 37.11(c)(1) and (2) must present his or her **Social Security Administration account number card**; or, if a Social Security Administration account card is not available, the person may present any of the following documents bearing the applicant's **SSN**: (i) A W-2 form; (ii) A SSA-1099 form; (iii) A non-SSA-1099 form; or (iv) A pay stub with the applicant's name and SSN on it.<br><br>(2) The State DMV must verify the **SSN** pursuant to § 37.13(b)(2) of this subpart.<br><br>(3) Individuals presenting the identity document listed in § 37.11(c)(1)(vi) must present an SSN or demonstrate non-work authorized status. |
| **Requirement of Statutorily Prescribed Procedures to Improve Effectiveness of Child Support Enforcement**<br><br>Personal Responsibility and Work Opportunity Reconciliation Act of 1996<br><br>*42 U.S.C. § 666* | Each State must have in effect laws requiring the use of the following procedures…:<br><br>Procedures requiring that the **social security number** of—<br>(A) any applicant for a professional license, **driver's license**, occupational license, recreational license, or marriage license be recorded on the application.<br><br>For purposes of subparagraph (A) (cited above), if a State allows the use of a number other than the social security number to be used on the face of the document while the social security number is kept on file at the agency, the State shall so advise any applicants. |

| F. Miscellaneous | |
|---|---|
| **Blood Donor Locator Service**<br><br>Technical and Miscellaneous Revenue Act of 1988<br><br>*42 U.S.C. § 1320b-11c* | A request for address information under this section shall be filed in such manner and form as the Commissioner of Social Security shall by regulation prescribe, shall include the blood donor's **social security account number**, and shall be accompanied or supported by such documents as the Commissioner of Social Security may determine to be necessary. |
| **Establishment of a Vessel Identification System**<br><br>Coast Guard Authorization Act of 1989<br><br>*46 U.S.C. § 12501* | The vessel identification system shall include information prescribed by the Secretary including:<br>(1) identifying a vessel;<br><br>(2) identifying the owner of the vessel, including—<br><br>(A) the owner's **social security number** or, if that number is not available, other means of identification acceptable to the Secretary; or<br><br>(B) for an owner other than an individual—<br><br>(i) the owner's taxpayer identification number; or<br><br>(ii) if the owner does not have a taxpayer identification number, the **social security number** of an individual who is a corporate officer, general partner, or individual trustee of the owner and who signed the application for documentation or numbering for the vessel; |

## ENDNOTES

[1] The challenges faced by Americans who struggle to prove their identity are quite notable, as documented by the article "The Invisibles: The cruel Catch-22 of being poor with no ID."

See https://www.washingtonpost.com/lifestyle/magazine/what-happens-to-people-who-cant-prove-who-they-are/2017/06/14/fc0aaca2-4215-11e7-adba-394ee67a7582_story.html?

[2] See "2018 Identity Fraud: Fraud Enters a New Era of Complexity" report from Javelin Strategy & Research – reference from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[3] See "2018 Identity Fraud: Fraud Enters a New Era of Complexity" report from Javelin Strategy & Research – reference from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[4] https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

[5] http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg

[6] http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg

[7] https://www.experian.com/blogs/ask-experian/the-state-of-online-shopping-fraud/

[8] http://www.acg.net/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group/

[9] https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf

[10] https://baymard.com/lists/cart-abandonment-rate

[11] See Thomson Reuters report https://blogs.thomsonreuters.com/financial-risk/risk-management-compliance/kyc-onboarding-still-a-pain-point-for-financial-institutions/

[12] See 2017 CIGI-Ipsos Global Survey on Internet Security and Trust, https://www.cigionline.org/internet-survey

[13] See http://docs.house.gov/meetings/IF/IF02/20171130/106662/HHRG-115-IF02-20171130-SD002.pdf

[14] See https://www.irs.gov/newsroom/irs-statement-on-get-transcript

[15] See http://www.acg.net/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group/

[16] See http://docs.house.gov/meetings/IF/IF02/20171130/106662/HHRG-115-IF02-MState-W000791-20171130.pdf

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

[18] See Section 215 "Reducing Identity Fraud" of S. 2155, the Economic Growth, Regulatory Relief, and Consumer Protection Act https://www.congress.gov/bill/115th-congress/senate-bill/2155

[19] Action Item 1.3 of the report. The full report is at: https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[20] See Digital Identity Guidelines - Enrollment and Identity Proofing – NIST Special Publication 800-63A at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[21] See https://www.dhs.gov/real-id

[22] Details at https://www.nist.gov/publications/nstic-pilots-catalyzing-identity-ecosystem-including-updates-09-20-2015

[23] See https://www.aamva.org/Mobile-Drivers-License/

[24] 18 U.S. Code § 2721 - Prohibition on release and use of certain personal information from State motor vehicle records

[25] See slides at the American Association of Motor Vehicle Administrators - https://www.aamva.org/system-modernization/

[26] See https://www.fmcsa.dot.gov/grants/cdl-program-implementation-grant/commercial-driver-license-cdl-program-implementation-grant

[27] See https://www.fema.gov/pdf/government/grant/2011/fy11_dlsgp_factsheet.pdf and https://www.fema.gov/media-library-data/20130726-1822-25045-0314/fy_2009_dlsgp_guidance_final.pdf

[28] See https://www.eac.gov/2018-hava-election-security-funds/

[29] Section 213 "Making Online Banking Initiation Legal And Easy" of S. 2155, the Economic Growth, Regulatory Relief, and Consumer Protection Act https://www.congress.gov/bill/115th-congress/senate-bill/2155

[30] https://www.idmanagement.gov/trust-services/

[31] An excellent history of the SSN is at https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

[32] For more on important characteristics of identifiers, see https://www.incommon.org/docs/other/identifiers-best-practices-200005.html

[33] See NIST Digital Identity Guidelines at https://pages.nist.gov/800-63-3/

[34] Note that the specific section of NIST's Digital Identity Guidelines that addresses authentication is SP 800-63B, "Authentication and Lifecycle Management" – see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[35] Full text of GDPR is available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[36] See https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

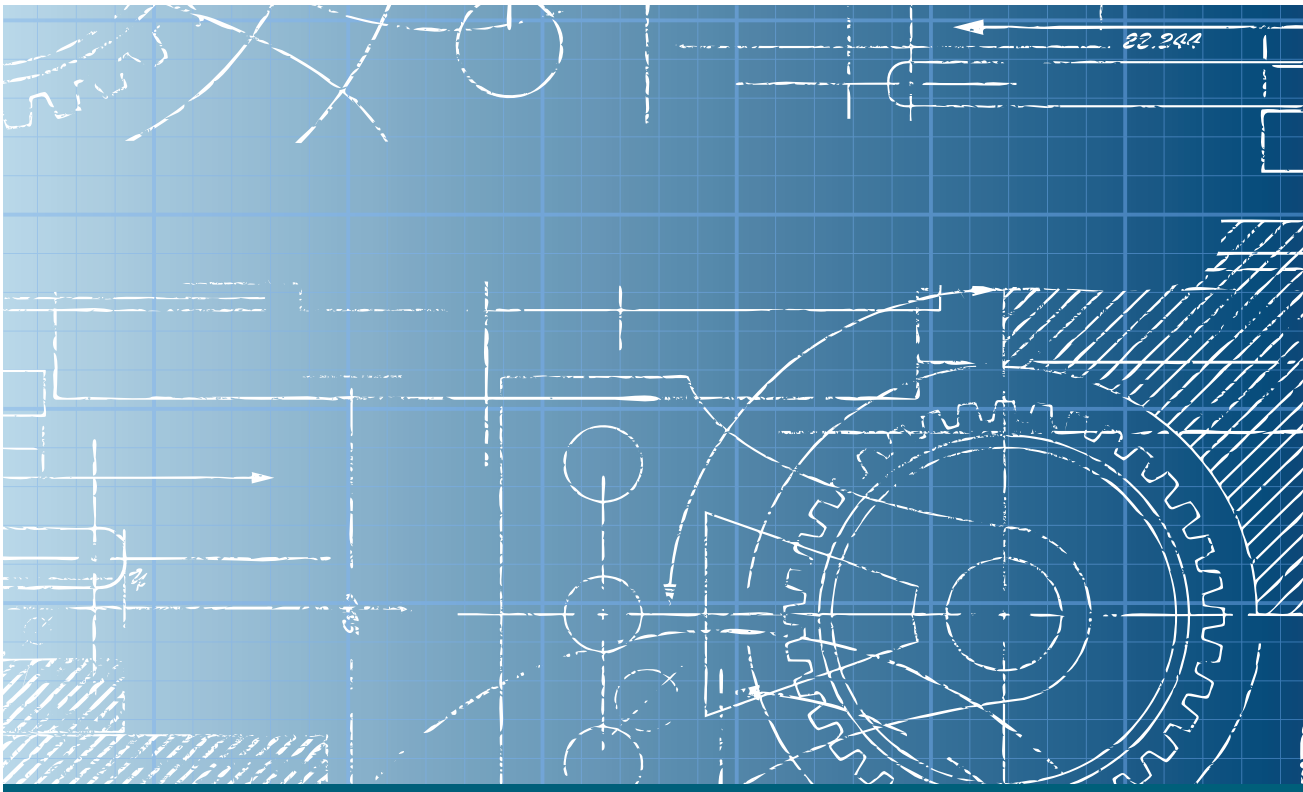
[37] See https://www.gpo.gov/fdsys/pkg/DCPD-201400778/html/DCPD-201400778.htm

[38] See https://www.lockdownyourlogin.org/

[39] More about eIDAS is at https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[40] See "Study on eID and digital on-boarding: Mapping and analysis of existing on-boarding bank practices across the EU" at https://publications.europa.eu/en/publication-detail/-/publication/8da08249-49cd-11e8-be1d-01aa75ed71a1/language-en/format-PDF/source-search.

[41] For more on the FATF, see http://www.fatf-gafi.org/



https://www.betteridentity.org