Jeremy Grant
Coordinator, The Better Identity Coalition

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

"I Am Who I Say I Am: Verifying Identity while Preserving Privacy in the Digital Age"

July 16, 2021

Chairman Foster, Ranking Member Gonzalez and members of the committee, thank you for the opportunity to discuss the topic of identity verification with you today.

I am here today on behalf of the Better Identity Coalition[1] – an organization launched in 2018 focused on bringing together leading firms from different sectors to develop a set of consensus, cross-sector policy recommendations that promote the adoption of better solutions for identity verification and authentication. The Coalition's founding members include recognized leaders from diverse sectors of the economy, including financial services, health care, technology, FinTech, payments, and security.

Up front, I want to flag that the Better Identity Coalition is not seeking to push the interests of any one technology or industry. Instead, our members are united by a common recognition that the way we handle identity today in the U.S. is broken – and by a common desire to see both the public and private sectors each take steps to make identity systems work better. It's very fitting that the Task Force has called this hearing in this particular week, as it's one that marks the

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

three-year anniversary of our publication of "Better Identity in America: A Blueprint for Policymakers" – laying out five key initiatives that government should launch around identity that are both meaningful in impact and practical to implement. And as I will discuss today, the need for government action here is greater than ever.

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

I will cover three core topics in my testimony today:

1. First, I will set the stage by detailing some of the problems with our existing approach to identity verification – and the enormous costs they present.

2. Second, I will discuss how these problems can be solved – looking at the question of "What should government and industry do about identity now?" I'll explain why

government – as the only authoritative issuer of identity – must play a role in the solution, and how doing so can help to spur not just improvements in security, but also economic growth. Chairman Foster's recently introduced "Improving Digital Identity Act of 2021" is critical here.

3. Third, given that this hearing is in the Artificial Intelligence (AI) Taskforce, I will discuss the role of AI and Machine Learning (ML) in identity verification – looking at how these technologies being used to deliver better identity outcomes, as well as identifying potential risks, and ways to mitigate those risks.

Setting the stage

Let me say up front that I am grateful to the Committee's AI Task Force for calling this hearing today, as well as to Chairman Foster for his leadership on this topic. The legislation that he and Congressmen Katko, Langevin and Loudermilk introduced two weeks ago – "The Improving Digital Identity Act of 2021" – is the single most important policy initiative the government can undertake to address the inadequacies of America's identity infrastructure.

At a high level, that should be one of the top takeaways for members of this Task Force today – identity is critical infrastructure 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 United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any

combination thereof."[2] Despite this designation, identity has gotten scant investment and attention. The Improving Digital Identity Act, if approved, will get us started.

And we are overdue to get started! The way we handle identity in America impacts our security, our privacy, and our liberty. And from an economic standpoint, particularly as we move high-value transactions into the digital world, identity can be the great enabler – providing a foundation for digital transactions and online experiences that are more secure, more enjoyable for the user, and ideally, more respectful of their privacy.

But when we don't get identity right, we enable a set of great attack points for criminals and other adversaries looking to execute attacks in cyberspace. And with it, we end up creating new burdens for consumers, businesses, and government agencies who need to accurately verify identity to enable high value transactions to be delivered online.

This was already a problem when this Task Force last convened nearly two years ago to consider digital identity, but the enormity of the problem has been magnified several times over the last 18 months amidst a pandemic that literally made it impossible to engage in most in-person transactions. The pandemic laid bare the inadequacies of the nation's digital identity infrastructure – enabling cybercriminals to steal billions of dollars and creating major barriers for Americans trying to obtain critical benefits and services.

More than $63 billion was stolen from state unemployment insurance (UI) programs by cybercriminals exploiting weak identity verification and authentication systems, according to the Labor Department's Inspector General. On the flip side, we've seen hundreds of stories about

[2] See https://www.cisa.gov/national-critical-functions-set

Americans who are out of work because of the pandemic, and who have been unable to get the UI benefits that they desperately need, because their application has been falsely flagged for "fraud" when they are unable to successfully navigate the convoluted, labyrinthine processes many states have put in place to verify identity.

Beyond UI, the inadequacy of our identity infrastructure remains a major challenge in financial services: FinCEN last year reported banks are losing more than $1 billion each month due to identity-related cybercrime.[3] Meanwhile, millions of Americans cannot get a bank account because they don't have the foundational identity documents needed to prove who they are. Amidst all of this, identity theft losses soared by 42% last year.[4]

On the cybersecurity front, it remains an anomaly when a major incident occurs and identity does not provide the attack vector. The SolarWinds attack several months ago was just the latest example of this, with Russian attackers targeting the administrative layer of identity and access management systems to do devastating damage.

As a leader at the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security stated back in March, "Identity is everything now."[5]

Why are there so many problems here? A key takeaway for this Committee to understand today is that attackers have caught up with many of the "first-generation tools" we have used to protect, verify and authenticate identity. Recent incidents may have driven this point home, but

[3] Per FinCEN at the 2020 Federal Identity Forum
[4] See https://aitegroup.com/report/us-identity-theft-stark-reality
[5] See https://federalnewsnetwork.com/cybersecurity/2021/03/cisa-identity-is-everything-for-cyber-defense-post-solarwinds/

the reality is that these tools have been vulnerable for quite some time. There are many reasons for this – and certainly blame to allocate – but the most important question is:

What should government and industry do about it now?

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

Let me say a few words about that bill: I've been asked quite a few times over the last year, "How do we fix identity verification in state unemployment systems?" or "How do we fix identity in banking?" or health care or government services? The answer is simple: you can't. In that identity is a national issue, and the core problems are the same for most every use case. Anyone trying to focus on "solving identity" for a particular use case, while well-meaning, is going to fail.

The good news is that these problems are not insurmountable. The U.S. can address its shortcomings by investing in creating "Digital First" identity infrastructure that leverages our existing nationally recognized, authoritative identity systems to create digital counterparts to the paper and plastic IDs they issue today. The Improving Digital Identity Act will do just that, and it is a critical piece of legislation.

In terms of level setting, it might be helpful to define "what we're talking about when we talk about digital identity." In that the term "identity" is thrown around a lot and used in a lot of different ways.

Fundamentally, there are two core challenges we are trying to solve.

1. The first is figuring out whether someone is who they claim to be at account opening – what's generally called "identity proofing." Exploiting weaknesses in our identity proofing infrastructure is what has allowed criminals to steal tens of billions of dollars from state UI programs, as well as financial services firms.
2. And second is "authentication." Once an account has been created – how you create systems that can securely log customers in to that account? This has become quite important in a world where passwords just don't cut it anymore, and cybercriminals are exploiting the weaknesses of passwords and other weak authentication tools to launch billions of attacks each day.

Here, the challenges faced by the market are not the same. I made a point two years ago that I will make again today, which is that across the identity marketplace: Authentication is getting easier, but Identity Proofing is getting harder.

Authentication is getting easier, but Identity Proofing is getting harder

Let me unpack that first part: Authentication is getting easier. By that, I mean that while passwords are broken, the ability of consumers and businesses to access tools that they can use in addition to – or in lieu of – passwords is greater than it's ever been. And with multi-stakeholder industry initiatives like the FIDO Alliance creating next-generation multi-factor authentication

(MFA) standards that are getting baked into most devices, browsers and operating systems, it is becoming easier than ever to deliver on the vision of better security, privacy and convenience. Microsoft, Google and Apple all support the FIDO standards via built-in support in Windows, Android, iOS and macOS, meaning it's hard for someone to buy a device these days that does not support FIDO authentication out of the box. This, in turn, is making it easier than ever for firms in financial services and other sectors to deliver passwordless experiences. The development and adoption of the FIDO standards is, in my view, the most significant development in the authentication marketplace in the last 20 years. I expect FIDO authentication to also play a big role in the Federal government's efforts to comply with the Biden Administration's recent Executive Order mandate for universal MFA across all government systems, helping to fill in the gaps where the government's legacy, PKI-based smart card authentication tools cannot easily do the job.

By pairing new authentication standards like FIDO with analytics solutions that use AI and ML to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords.

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

This means that it is harder than ever for businesses and government – as more transactions move online – to verify someone's identity when someone is creating an account or applying for a new service. Better tools are needed here. But unlike with passwords – where the market has

responded with tools like FIDO authentication and behavior analytics to fix the problem – the market has not yet sorted things out here. To be clear, there is great industry innovation in the identity proofing space, including by many of the Coalition's members. But the one thing that has become clear in discussion with industry is that the private sector cannot solve this problem on its own.

Why is that? Well, as one of our members noted, the title of this hearing – "I am who I say I am" – is technically incorrect, since for all purposes, when it comes to identity, you are who the government says you are. One might ask the government to recognize a name change if you want to go by a different name – an Iowa man named Jeffrey Wilschke famously changed his name several years ago to Beezow Doo-doo Zopittybop-bop-bop[6] – but it's safe to say his bank, the DMV, the TSA, the IRS, the SSA, his health insurer, and dozens of other parties he engages with would not be willing to recognize that name had the government not first done so.

This point really gets to the heart of the issue when it comes to identity proofing: At the end of the day, government is the only authoritative issuer of identity in the United States. But the identity systems government administers are largely stuck in the paper world, whereas commerce has increasingly moved online. This "identity gap" – a complete absence of credentials 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.

A core challenge here is that 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

[6] More on Mr. Doo-doo Zopittybop-bop-bop and his journey is at https://madison.com/wsj/news/local/beezow-doo-doo-zopittybop-bop-bop-behind-the-name-a-complex-figure/article_14ccf4aa-87f6-11e1-83e2-0019bb2963f4.html

"identity gap" in the U.S. caused by the lack of any formal digital identity system – for example, Knowledge-Based Verification (KBV) systems that attempt to verify identity online by asking applicants several questions that, in theory, only they should be able to answer. Now that adversaries, through multiple breaches, have obtained enough data to defeat many KBV systems; the answers that were once secret are now commonly known. Next generation solutions are needed that are not only more resilient, but also more convenient for consumers.

Industry is innovating here, and AI-enabled solutions are one of the tools that can help. But they alone are not enough. The single best way to address the weaknesses of KBV and other first-generation identity verification tools is for the government to fill the "identity gap" that led to their creation. This idea is at the heart of the Better Identity Coalition's key recommendations for how government and the private sector can improve the identity ecosystem, as well as the Improving Digital Identity Act.

It's an idea that eschews the tired, old idea of trying to solve problems with a national ID card. The reality is that we don't need new identity systems – and part of our problem is that we have too many cards today, another one will not help. Instead, we need to leverage the authoritative government identity systems that we already have at the Federal, state and local level, but that are largely stuck in the paper world; none of them can be easily used – or validated – online.

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

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

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

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

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

Indeed, the SSA has built just the sort of Attribute Validation Service that we called for, the Electronic Consent Based Social Security Number Verification (eCBSV) Service. SSA is doing so in response to Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act, which was signed into law in 2018 thanks, in part, to this Committee's work.

The eCBSV system now allows financial institutions and their service providers to electronically get a "Yes/No" answer as to whether an individual's SSN, name, and date of birth combination matches Social Security records. We're thrilled to see SSA lead the way here.

First, because eCBSV will change the game in the fight against synthetic identity fraud, which costs the country $6-$8 billion annually. The fact that fraudsters have been targeting the SSNs

of children to commit this fraud is especially galling – eCBSV has given the country a tool to fight back.

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

The Improving Digital Identity Act would jumpstart the creation of similar services at the Federal, State and Local level through four core initiatives:

- First, it would state that it is the policy of the U.S. Government to use its authorities and capabilities to enhance the security, reliability, privacy, and convenience of digital identity solutions that support and protect transactions between individuals, government entities, and businesses, and that enable Americans to prove who they are online. With this, the bill would set up a formal, White-House led "Improving Digital Identity Task Force" charged with bringing together key Federal, state, and local agencies who all issue identity credentials to develop secure methods for government agencies to validate identity attributes in a way that protects the privacy and security of individuals, and supports reliable, interoperable digital identity verification tools in the public and private sectors.

  The focus on bringing Federal, state, and local governments together is essential, given that America's authoritative identity systems are split between all these levels of government. For example, my birth certificate was issued by the county I was born in, my driver's license is issued by my state DMV, and my passport was issued by the State Department. I should be able to ask any of those organizations to vouch for me when I am trying to prove who I am online – in a way that is standards-based, offers a consistent user experience, and supports excellent security and privacy.

- This last point brings up the very vital second initiative in this bill: funding the National Institute of Standards and Technology (NIST) to lead development of a framework of standards and operating rules to make sure these services are built in a way that sets a high bar for security and privacy. The bill recognizes from the start that any new digital identity systems, if crafted poorly, could create privacy and security concerns – and doesn't shy away from this issue. Instead, the bill tackles this head on. First by directing NIST to create a framework that engineers strong security and privacy protections in from the start, and second, by requiring that any new government systems follow this framework. There's nobody in government or the private sector with better expertise to do this than NIST. It's also worth noting on the privacy side that nothing in this bill envisions having government share data on Americans. The role of government is limited to validating – at an individual's request – that data submitted matches what a particular agency has in its authoritative identity systems. That approach significantly mitigates potential security and privacy risks with having government play a role here.

- Third, the bill would set up a new grant program to provide funding to states to help them implement this architecture and framework in state DMVs – accelerating their transition to being digital identity providers through new mobile Driver's License (mDL) apps and other digital identity solutions. All grant dollars would be tied to a state's adherence to the NIST framework, ensuring 1) that all states implement solutions that set a high bar for security and privacy, and 2) that all states implement solutions that are interoperable, ensuring that the country can get the full economic benefit of this investment. Notably, states would be required to allocate 10% of grant dollars to help people who may not be able to easily get an ID. One downside of the increased security requirements of the

REAL ID Act has been that many Americans cannot easily get a driver's license, because they cannot produce or access the multiple documents needed to prove who they are. This particularly impacts the elderly, the poor, as well as survivors of domestic violence. New funding will allow states to better assist the most vulnerable in getting both physical and digital credentials and ensure that any investment in new identity infrastructure can benefit all Americans.

- Finally, the bill would address longstanding concerns about the overuse of the Social Security Number (SSN) as an identifier by directing the Government Accountability Office (GAO) to analyze what laws and regulations require industry or government to collect SSNs, as well as whether they are all still relevant and needed, or could be addressed through something other than the SSN.

Together, these four initiatives will create a comprehensive approach to digital identity that will prevent costly cybercrime, give businesses and consumers new confidence, improve inclusion, and foster growth and innovation across our economy. Notably, it's also an approach that does not rely on government to provide the entire solution – only those elements to which it is uniquely suited. Given all the problems we've seen in digital identity over the past year, the time for action is now – we urge Congress to pass the bill immediately.

In addition, the Coalition believes that the pending infrastructure package currently being negotiated being Congress and the White House should include funding for the state grants envisioned in the Improving Digital Identity Act. Any investment in broadband that does not also invest in a proper "identity layer" to enable Americans to use that broadband for secure and trusted transactions will fall short of its goal. A $2 billion investment can deliver a digital

mobile Driver's License (mDL) to everyone in America who wants one, and create robust digital identity infrastructure that will deliver improved security, privacy, and economic growth.

If that cost seems high, consider that earlier this year, Congress approved an identical number solely to address concerns about state unemployment insurance systems tied to identity fraud prevention and benefit processing. We believe the same amount of money directed to new digital identity infrastructure in the states would be sufficient to address the majority of digital identity challenges tied to state ID systems.

The benefits of investing in digital identity go beyond stopping cybercrime and identity fraud – the economic benefits are notable. U.S. GDP could grow an extra 4% by 2030 with investments in robust digital identity infrastructure, according to a 2019 study by McKinsey.[7] And the Federal government would save billions annually by offering more online services; a 2013 government study estimated that digital identity infrastructure could save the IRS alone more than $300M each year while also enabling the IRS to deliver more trusted, high-assurance services to taxpayers through online channels.[8]

By failing to invest in digital identity infrastructure, the U.S. is leaving money on the table, while continuing to enable easy attack vectors for cybercriminals to prey on Americans.

It's worth noting that the U.S. is an outlier when compared to our peers: the UK, Europe, Australia and Canada all have significant digital identity initiatives underway, backed by the

[7] https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.pdf
[8] https://www.nist.gov/system/files/documents/2017/05/09/report13-2.pdf

highest levels of government and significant budgets. If America does not follow, our failure to invest here will soon become an issue of economic competitiveness.

The Role of Artificial Intelligence and Machine Learning

Given that this hearing is taking place in the AI Taskforce, it seems important to talk about the role of artificial intelligence and machine learning in identity verification systems – looking both at the benefits AI is offering today and will offer in the future, as well as some of the potential risks that go with it.

Earlier, I framed challenges around digital identity in two buckets: those focused on identity proofing, typically at account creation – and those in authentication, used to log in to an account after it has been created.

On the ID Proofing side, there are two primary use cases where AI and ML play a role:

- The first is in remote ID proofing tools that ask a consumer to take a photo of their ID (such as a driver's license), as well as a selfie picture. In many of these products, AI/ML is used to help validate whether an ID document is real or counterfeit, as well as whether the selfie matches the photo on the ID. The role of AI/ML in these products is generally one where they "study" different documents and "learn" over time how to better tell a real driver's license or passport from a fake. In addition, AI/ML is also often used in the "facial comparison" aspect of the product. Here, we are starting to see some firms address concerns about the accuracy and consistency of some weaker face matching

algorithms by shifting to algorithms based on 3D models of faces, rather than traditional 2D photos.

It is worth noting that Congress recognized the importance of these solutions in financial services in 2018 when it passed the Economic Growth, Regulatory Relief, and Consumer Protection Act. Section 213 of that bill was called the Making Online Banking Initiation Legal and Easy (MOBILE) Act, and it preempted some state laws that prevented banks from scanning a driver's license to support mobile applications for new accounts.

Today, the types of solutions detailed in the MOBILE Act are widely used – but not all of them use AI or ML, and performance of the products is inconsistent between vendors. Here it is worth noting that the FIDO Alliance has launched a new initiative to test and certify these solutions. Building on FIDO's success in developing testing and certification programs for authentication products, FIDO has now expanded its focus to identity proofing. While the certification program has not yet launched, FIDO has announced plans to establish performance criteria for these products, in partnership with a number of independent testing labs to measure whether products meet these performance criteria.

To the extent that there is a concern that that AI or ML technology used in some of these products might not measure up, this new testing and certification program will be a major asset. Many vendors are saying "trust us, our products work" – this program will verify that they actually do. I will note to the Committee that I am an advisor on this project – outside of the "hat" I wear with the Better Identity Coalition – and would be happy to talk about it further if there is interest.

- Second, AI and ML is used to deliver more accurate data-centric approaches to ID proofing. Here, vendors in the space look at lots of different signals and data sources, and use AI and ML to help predict over whether an applicant might be fraudulent or not – analyzing data and signals with algorithms that are constantly evolving and improving thanks to AI and ML, and that help companies root out fraud, including synthetic identity fraud, and make more accurate decisions.

  Signals and data sources may include what can be inferred about a device being used to apply for an account, or the way a user interacts with that device as they enter their information digitally. Examining a wider set of signals and data sources provides a multi-dimensional view of identity for enriched verification, and simultaneously allows vendors and implementers to identify patterns of repeated identity fraud across government agencies and the private sector driven by sophisticated crime rings. Given that it is these crime rings that were at the heart of much of staggering losses in the past year, this is an increasingly important use of AI and ML.

  While there are some concerns that algorithms used here might be biased – and that "putting the machines in charge" will lead to inequitable outcomes – most of what I have seen in the use of AI in these types of solutions, on balance, is improving equity and inclusion. For example, if a bank is looking at credit report data for identity proofing – but a consumer has a thin file, as is common for young people, immigrants, and historically marginalized groups – AI and ML can be used to look at other data sources and approve applicants at a higher rate. Likewise, if a consumer does not have a driver's license or passport – or does not have a smartphone – those "selfie match" tools I discussed earlier probably won't work. Again, these are areas where tools that leverage

AI and ML are often able to help fill in the "gaps" and provide an alternative path to approval.

Overall, many of our members in the financial services space report that without AI/ML and risk-based models it would be difficult to perform thorough risk-based identity validation at scale.

On the Authentication side, AI and ML also play an important role as part of analytics solutions that look at dozens of different data points and signals about how an individual is 1) trying to authenticate or 2) interacting with a device or application after initial authentication.

Here, we are seeing firms in financial services and other sectors use tools that look at data such as behavior, location, typing pattern, access requests (trying to get to something they should not have access to), etc. The tools then study all these elements and then use AI to make a prediction as to whether anything seems "off" or shows a sign of account or device compromise.

By pairing more traditional authentication such as that using the FIDO standards with analytics solutions that use AI/ML to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords.

The emergence of reliable authentication analytics tools is contributing to the rise of a new model for authentication called "continuous, risk-based authentication." Here you pair a traditional authentication factor like a password or MFA with analytics tools that analyze different signals. Some might automatically remediate a sign of fraud by refusing authentication, in other cases it might trigger a signal that is then used to ask a user for additional factors of authentication. To be clear, not all of these tools use AI and ML, but many do.

As major banks and cloud providers see tens or hundreds of millions of fraudulent attacks each day on their login systems, AI and ML have emerged as essential tools to detect and block them.

Having offered this brief primer on how AI and ML are used in identity proofing an authentication, I'd like to offer the Task Force a few thoughts on how policymakers should think about these technologies going forward.

1. First, the points I just detailed should make clear that AI and ML technologies are an increasingly important tool in identity – particularly given the ongoing battle we are in against cybercriminals. These criminals are doubling or in some cases quintupling down on identity-centric attacks, putting the security and privacy of people's data and money at risk. The good guys need every tool in the toolbox.

   On that point, criminals themselves are starting to develop their own AI and ML tools to support cyber-attacks. This is slightly terrifying but should not be surprising; the same technology innovations that can be used to protect us will also be exploited by adversaries to try to attack us. We're seeing this in the early stages with criminals using bots for automated password spray and credential stuffing attacks. Attackers are always innovating, and we should be preparing for them to be using AI against us in new and innovative ways.

2. Second, To the point that there are policy concerns about the use of AI and ML, the answer is not to ban their use but rather to identify the specific concerns and work to address them. Because a blanket ban will almost certainly play into the hands of criminals and put consumers and businesses at great risk.

3. Third, an important part of issues surrounding AI and ML used in identity verification is the fact that many of the technologies are opaque: despite the efficiency of many algorithms, it still difficult to explain their decisions to most people. These issues can be greatly mitigated by independent certification and testing programs such as the one for remote ID proofing tools that I mentioned earlier that FIDO Alliance is developing – creating a way to independently validate the claims made by vendors and also determine whether there are any specific quirks or biases in a product or algorithm that may need to be addressed. In addition, NIST has done some great work to help vendors and implementers address potential bias concerns in its recent draft Special Publication 1270, *"A Proposal for Identifying and Managing Bias in Artificial Intelligence."*

4. Fourth, it is important that policymakers do not lose sight of the ways AI and ML can help with inclusion and equity. As I mentioned earlier, financial services firm are already starting to use AI to enable new approaches to identity proofing that can help bring more services to the "credit invisible" – such as more easily auto-approving more people for loans – relative to legacy tools that don't use AI.

5. Finally, I would state that the single best way to address concerns with regard to bias in AI and ML being used in identity proofing tools is to pass the Improving Digital Identity Act. In that every product using AI and ML to try to determine identity is trying to "guess" what only the government really knows. And there is no better way to address concerns about these probabilistic systems run amuck than to enable new deterministic systems that rely on the actual source of identity in government. As I have stated throughout my testimony, we're not going to truly solve identity proofing without the kinds of identity attribute validation services that the bill calls for.

In closing, while the current state of digital identity poses some challenges, Chairman Foster and his colleagues have put before Congress a proposal that will address these challenges in a complete and holistic fashion. The time to act on it is now.

I am grateful for the Committee's invitation to offer recommendations on how government can improve the identity ecosystem and look forward to your questions.