April 13, 2022

To: Gene Sperling, American Rescue Plan Act Coordinator
Shalanda Young, Director, Office of Management and Budget
Jason Miller, Deputy Director, Office of Management and Budget
Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology
Brian Deese, Director, National Economic Council

Dear Mr. Sperling, Director Young, Deputy Director Miller, Ms. Neuberger, and Director Deese:

We were thrilled to see President Biden's State of the Union pledge on March 1 to issue an Executive Order (EO) to "prevent and detect identity theft involving public benefits, while protecting privacy and civil liberties and preventing bias that results in disparate outcomes," as well as "direct new actions to support the victims of identity fraud."

The COVID-19 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. The Administration's attention to this issue is welcome and appreciated.

The Fact Sheet accompanying this announcement rightly focused on the need for the Justice Department to ramp up prosecutions of the organized criminals who have been stealing identities, as well as the need for expanded prosecutions of egregious pandemic fraud.

As the Administration drafts this new EO, we believe it is imperative that four additional priorities are addressed:

1. **Prioritize giving Americans tools that they can use to protect themselves from identity thieves.**

   Today it is far too easy for criminals to steal identity, given that many identity proofing solutions are built around the premise that "knowing several things about you" means "someone is you." NIST long ago made clear that knowledge-based verification tools are not sufficient for identity proofing, but newer tools in the market are not yet able to solve all challenges, and do not work for all Americans – and this contributed to the massive identity theft and fraud seen over the last two years.

   The single best way to prevent identity theft is to give Americans tools that they can use to protect themselves from identity thieves. Here, we are collectively excited about the ways that mobile driver's licenses (mDLs) can help, and believe the Biden-Harris administration must take steps in the EO to accelerate state deployment of mDL

applications, as well as other identity proofing solutions that meet Identity Assurance Level 2 (IAL2), as defined by NIST.

The benefits of mDLs are straightforward: rather than force Americans to go through a new government-run process that replicates the in-person identity proofing process they already went through to get a driver's license or state ID card, Americans should instead be given the opportunity to reuse a high assurance credential they already have.

A number of states have started to introduce mDL apps that allow someone to effectively prove their identity with a digital app rather than a plastic ID card. Congress passed a law in 2020 giving physical and digital IDs legal equivalency under the REAL ID Act. However, early use cases are focused on in-person use cases such as proving identity to the TSA at airports, whereas the most urgent problems mDLs can solve are focused in the digital world.

The EO should:

a) Direct NIST and DHS to accelerate the development of standards and guidance to states to enable them to launch remote identity proofing applications for mDLs. Current standards around mDLs such as ISO 18013-5 are limited to in-person use cases. With thousands of Americans victimized by identity theft each year – and tens of billions of dollars lost each year to identity fraud – the United States cannot wait years for the International Standards Organization (ISO) to create standards to support digital identity proofing via mDLs. NIST should lead an effort – with support from DHS and other agencies – 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.

b) Fund grants to states to help them accelerate their deployment of mDL apps – with funds tied to adherence to these standards. Note that Treasury Assistant Secretary Elizabeth Rosenberg proposed this idea in a January 24, 2022 speech; the EO should look for ways to advance the concept, potentially with Treasury in the lead on administering these grants.[1]

c) Ensure that at least 10% of grants are used to support "Identity Inclusion" efforts – helping 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, or afford to obtain them. This particularly impacts the elderly, the poor, foster youth, as well as survivors of domestic violence and those reentering society

[1] See https://www.nextgov.com/cybersecurity/2022/01/treasury-considering-state-and-local-grants-implement-digital-id-systems/361226/

after time in prison.[2] New funding will allow states to better assist the most vulnerable in getting both physical and digital credentials.

The Biden Administration has driven tremendous cybersecurity improvements in the "authentication layer" of identity, by introducing new requirements in the Federal Zero Trust Strategy for agencies to use possession-based authentication rather than knowledge-based authentication. Solving identity proofing will require the same shift – getting people away from knowledge-based solutions to ones that create a digital equivalent to the secure plastic ID cards they have in their wallets.

States and the Federal government can leverage mDL solutions to enable more trusted digital services, cut down on fraudulent benefits claims, and protect citizen information.

Had mDLs been widely deployed at the start of the COVID-19 pandemic, Federal and state agencies could have easily used them to securely and remotely verify the identities of applicants for benefits, and prevented the vast majority of identity theft and fraud.

2. Ensure that identity theft victims have access to direct assistance

The Federal Trade Commission's 2021 data shows 25% of fraud reported to the Commission in 2021 was identity related. That translates into 1.4 million Americans and more than $5.2B in reported fraud losses. The Federal Bureau of Investigation's IC3 report for 2021 shows a similarly large number of suspected identity related crimes: 847,376 reports representing nearly $7B in potential losses to individuals and businesses.

These statistics indicate that identity fraud exceeds all violent crimes on an annual basis and are second only to larceny in terms of the overall number of offenses committed each year, according to the FBI. Yet, there is no formal local, state, or federal infrastructure designed to support victims of identity-related crimes. The primary federal agency tasked with assisting identity theft victims – the FTC – does not offer direct victim assistance at scale, instead the Commission relies on an on-line self-service delivery model.

A single non-profit – the Identity Theft Resource Center (ITRC) – serves as the only national organization which provides direct assistance free of charge to victims of identity crimes. In 2020, 2021, and continuing through today, the ITRC has worked with more than 3,900 individuals who have reported being the victim of pandemic benefit related identity fraud. A significant number of these individuals reported hardships as a result of being denied benefits as well as difficulty accessing government services needed to resolve their issues. (See 2021 ITRC Consumer Aftermath Report.)

Therefore, we recommend the EO include provisions to:

[2] 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

a) Ensure identity crime victims have access to direct assistance, free of charge, across multiple delivery channels including digital and in-person, including telephone, support services. Providing only digital services results in a significant portion of the victim population being denied assistance because of a lack of access, lack of skill, or lack of ability.

b) Provide adequate funding for government and non-government organizations to offer identity crime victim assistance at a scale that matches the volume and velocity of identity crimes; ensure the assistance offered by established organizations is culturally competent and addresses the unique needs of underserved groups as well as the majority population.

c) Develop, over the long-term, a public-private "one-stop shop" for identity crime victim support. This model would allow victims to access services from local, state, and federal government agencies as well as access private sector and non-profit services from a single virtual contact center or series of regional centers.

3. Establish a government-wide approach to enable identity attribute validation services.

While less powerful as a stand-alone identity proofing tool than mDLs, identity attribute validation services that provide a "Yes/No" answer as to whether data someone submitted (i.e., Name, DOB, SSN) matches what an agency has on file have proven to be a powerful tool in improving remote identity proofing tools.

The SSA has established the electronic Consent Based Social Security Number Verification (eCBSV) service, which allows financial institutions and their service providers to validate identity information against SSA data, helping to address what the Federal Reserve estimates is a $20 billion per year synthetic identity fraud problem. As a secondary benefit, early participants in eCBSV report that the definitive "Yes/No" answer that SSA provides has helped them approve tens of thousands of credit applications that might have been otherwise rejected due to insufficient proof of identity. Identity attribute validation services thus help fight fraud and improve inclusion. However, while eCBSV is available to banks, it is not available to government agencies – or the industry partners they leverage – looking to vet applicants for services or benefits.

Meanwhile, GSA has announced plans to create an Identity Verification API[3] that is described as "a privacy preserving shared service that enables identity verification with government authoritative sources, simplifying processes and saving the government money." However, unlike eCBSV, this API would not be available to the private sector. Identity attribute validation services can help solve identity theft challenges in both

[3] See TTS American Rescue Plan: Projects and Impact, https://www.gsa.gov/technology/government-it-initiatives/tts-american-rescue-plan/tts-american-rescue-plan-projects-and-impact#identity

public and private sector applications – and Americans are at risk of identity theft and fraud in both.

As part of any EO, the Administration should mandate the creation of a government-wide approach to these attribute validation services that enable them to be accessed with uniform fees and terms by the public and private sector.

4. **Direct NIST to create a Digital Identity Framework of standards and best practices to help agencies at all levels of government establish attribute validation and other digital identity services in a way that is standardized, and sets a high bar for security, privacy, and equity.**

   With authoritative government issuers of identity divided between across Federal, state and local agencies, it will be important to ensure that every agency playing a role in digital identity services follows standards that set a high bar for security and privacy, and ensure interoperability of solutions. NIST should be tasked with developing and periodically updating a Framework of standards, methodologies, procedures, and processes as a guide for Federal, State, and local governments to follow when providing services to support digital identity verification.

   We note that language authorizing this NIST work was included in section 10225 of the recently passed House version of the America COMPETES ACT. While the fate of that bill is uncertain, NIST can begin work on a Framework today through an EO.

Together, these four initiatives will ensure that any EO prioritizes helping Americans avoid ever becoming identity theft victims, and assure that those Americans who are victimized will be able to get the help they need to be made whole. They will reduce identity theft involving public benefits, protect privacy and civil liberties, and prevent bias that results in disparate outcomes.

We appreciate the Administration's consideration of our request, and offer our organizations' collective expertise should assistance be helpful as the EO is crafted.

Sincerely,

Better Identity Coalition
Cybersecurity Coalition
Electronic Transactions Association (ETA)
Identity Theft Resource Center (ITRC)
National Cyber Security Alliance (NCSA)
US Chamber of Commerce Technology Engagement Center (C_TEC)