BETTER IDENTITY COALITION

eta ELECTRONIC TRANSACTIONS ASSOCIATION

July 21, 2021

The Honorable Nancy Pelosi
Speaker, U.S. House of Representatives
1236 Longworth Building
Washington, DC 20515

The Honorable Charles Schumer
Majority Leader, United States Senate
322 Hart Senate Building
Washington, DC 20510

The Honorable Kevin McCarthy
Minority Leader, U.S. House of Representatives
2468 Rayburn Building
Washington, DC 20515

The Honorable Mitch McConnell
Minority Leader, United States Senate
317 Russell Senate Building
Washington, DC 20510

Dear Madam Speaker, Mr. Minority Leader McCarthy, Mr. Leader Schumer, and Mr. Minority Leader McConnell:

We are writing to request your assistance in ensuring that any infrastructure plan that advances includes funding to create more robust digital identity infrastructure, focused on reducing fraud and improper payments and enabling more trusted digital transactions online for every American.

The pandemic has 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. Many of the poorest Americans have been particularly hard hit, as their applications for assistance have 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.

The good news: as Secretary Yellen noted in February's Financial Sector Innovation Policy Roundtable hosted by Treasury, "The same digital ID technology that protects against money laundering can also help us reach more people with relief."

As we prepare to invest billions in more resilient infrastructure, it is essential that Congress and the White House ensure that every person, business, organization, and agency in America can trust digital infrastructure to access secure, privacy-protecting digital services. Done right, the benefits of investing in identity infrastructure will extend beyond fraud reduction; economists at McKinsey forecast that U.S. GDP could grow an extra 4% by 2030. And the Federal government would save billions annually by offering more online services; NIST has estimated that digital identity infrastructure could save the IRS alone more than $300M each year.

So many services – in banking, health care, government, and e-commerce – depend on knowing "who is on the other side" of a transaction. In 2021, 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 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.

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 state DMVs to create digital counterparts to the plastic IDs they issue today. It’s an idea based on a well-vetted, consensus proposal detailed in the bipartisan Improving Digital Identity Act of 2021 (H.R. 4258), using technology pioneered and piloted by NIST.

A $3 billion investment will deliver a digital mobile Driver’s License (mDL) to everyone in America who wants one, and create robust digital identity infrastructure key elements of which should include:

- $2 billion to support grants to states to fund digital mDLs at no cost to their residents. DMVs – as the one place where almost every adult American goes through a robust, in-person identity proofing process that is based on a Federal standard (REAL ID) – are the most logical place to help improve identity through mDL apps and other identity validation services. But they have antiquated infrastructure, and most DMVs aren’t incented to modernize identity.

  Note that NIST funded the first mDL pilots through the Obama Administration’s National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative, demonstrating the security, privacy, and practical benefits of robust digital identity solutions. This investment would enable every state to embrace this proven model.

- $580 million to support implementation of new digital identity solutions at Federal agencies. These may include “government attribute validation services” that allow Americans to ask an agency that already issued them a credential to “vouch” for them when they are trying to prove who they are online, as well as other innovative digital identity solutions.

- $400 million 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. This particularly impacts the elderly, the poor, as well as survivors of domestic violence and those reentering society after time in prison. New funding will allow states to better assist the most vulnerable in getting both physical and digital credentials.

- $10 million to support a new “Improving Digital Identity Task Force” in the White House, tasked with bringing together key federal agencies with state and local government representatives to develop secure methods for government agencies to validate identity attributes to protect the privacy and security of individuals, and support reliable, interoperable digital identity verification tools in the public and private sectors. This task force will create the blueprint that guides the spending outlined above.

- $10 million for NIST to create a "Digital Identity Framework" of standards, methodologies, procedures, and processes that supports the Task Force deliverables, and that agencies at all levels of government can use to deliver identity services in a standardized way that is secure, interoperable, is designed around the needs of consumers, and protects privacy.

States and the Federal government can leverage this new identity infrastructure to enable more trusted digital services, cut down on fraudulent benefits claims, and protect citizen information. And the private sector can also leverage it for remote identity proofing required for high-trust transactions in sectors such as financial services and health care.

In 2019, DHS designated Identity Management and Associated Trust Services as one of 55 National Critical Functions – 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.*" Despite this designation, identity has gotten scant investment and attention. Meanwhile, our counterparts in Europe, Canada, Australia, and Asia have all launched major digital identity initiatives, funded with significant investments. Infrastructure legislation is the ideal place to address this oversight.

By investing in digital identity infrastructure, we will prevent costly cybercrime, give businesses and consumers new confidence, improve inclusion, and foster growth and innovation across our economy.

We are eager to work with you on these efforts and look forward to hearing your thoughts on how to best improve digital identity infrastructure.

Sincerely,

Better Identity Coalition
Electronic Transactions Association

cc: Gene Sperling, Jason Miller