November 21, 2022

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

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

The Honorable Mitch McConnell
Republican Leader
United States Senate
Washington, DC 20510

The Honorable Kevin McCarthy
Republican Leader
U.S. House of Representatives
Washington, DC 20515

Dear Speaker Pelosi, Republican Leader McCarthy, Majority Leader Schumer, and Republican Leader McConnell:

As Congress works to finalize its year-end spending bill, we urge you to include S. 4528, the Improving Digital Identity Act of 2022, in the legislation.

This bipartisan bill is essential to addressing a sharp and rapid increase in identity-centric cybercrime, where stolen or compromised identities are being used by organized criminals to steal billions of dollars from millions of Americans.

- Incidents of identity theft and identity fraud continue to rise in the United States, where more than 293 million people were impacted by data breaches in 2021. Since 2017, losses resulting from identity fraud have increased by 333 percent, and identity theft has now impacted nearly half of all Americans.

- In government, the COVID-19 pandemic saw cybercriminals steal billions of dollars and created major barriers for Americans trying to obtain critical benefits and services. The Inspector General at the Department of Labor has estimated that more than $45 billion was lost to fraudulent unemployment insurance (UI) payments, and stated that the actual number may be higher. Per the DOL OIG, "Hundreds of billions in pandemic funds attracted fraudsters seeking to exploit the UI program—resulting in historic levels of fraud and other improper payments." The Federal Trade Commission (FTC) reported a nearly 3000% increase in reports of identity theft involving public benefits from 2019 to 2020.

- In financial services, FinCEN has stated that "The abuse of personally identifiable information and other building blocks of identity is a key enabler behind much of the

fraud and cybercrime impacting the United States today." FinCEN also notes, "Analysis of the over 3 million Suspicious Activity Reports that financial institutions filed with us in 2021 shows that the majority include reference to potential breakdowns in the identity verification process." The Federal Reserve has estimated that losses from synthetic identity theft alone now exceed $20 billion annually – with many of the victims being children who have their social security numbers stolen.

So many services – in banking, health, government, and e-commerce – depend on knowing "who is on the other side" of a transaction. In 2022, 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.

We are pleased that this bill looks to tackle the problem head-on: by closing the gap between the nationally recognized, authoritative credentials that are widely trusted in the paper world – such as driver's licenses, passports, and birth certificates – and the lack of any way to easily use those credentials in the digital world. Importantly, the bill prioritizes tackling this challenge in a way that not only improves security, but also protects privacy and civil liberties.

The benefits of prioritizing identity infrastructure would extend beyond security and privacy; economists forecast that U.S. GDP could grow an extra 4% by 2030. And the Federal government could save billions annually by offering more online services; NIST has estimated that digital identity infrastructure could save one agency alone more than $300M each year.

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. Passage of the Improving Digital Identity Act is the best place to start.

By prioritizing digital identity infrastructure, we will prevent costly cybercrime, help ensure Americans never become identity theft victims, give businesses and consumers new confidence, and foster growth and innovation across the economy.

We are grateful for your leadership, and look forward to working with you to advance this legislation this year.

Sincerely,

Bank Policy Institute
Better Identity Coalition
BSA | The Software Alliance
College of Healthcare Information Management Executives (CHIME)
Cybersecurity Coalition
Electronic Transactions Association (ETA)

Identity Theft Resource Center (ITRC)
Software & Information Industry Association (SIIA)
TechNet
US Chamber of Commerce Technology Engagement Center (C_TEC)

cc: Members of the Senate Committee on Appropriations
cc: Members of the House Committee on Appropriations
cc: Members of the Senate Homeland Security & Governmental Affairs Committee
cc: Members of the House Committee on Oversight & Reform