

.....
(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To establish a government-wide approach to stopping identity fraud and theft in the financial services industry, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. SESSIONS introduced the following bill; which was referred to the Committee on _____

A BILL

To establish a government-wide approach to stopping identity fraud and theft in the financial services industry, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Stop Identity Fraud
5 and Identity Theft Act of 2026”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) The lack of an easy, affordable, and reliable
2 way for organizations, businesses, and government
3 agencies to identify whether an individual is who
4 they claim to be online creates an attack vector that
5 leads to millions of Americans being victimized by
6 China and North Korea, and other hostile nation-
7 states, as well as organized crime gangs, all of whom
8 steal and compromise identities to commit
9 cybercrime and fraud.

10 (2) Incidents of identity theft and identity
11 fraud continue to rise in the United States, where
12 more than 353 million people were impacted by data
13 breaches in 2023.

14 (3) The Government Accountability Office
15 (GAO) estimated that the Federal government could
16 lose between \$233 billion and \$521 billion annually
17 to fraud; GAO estimated that the amount of fraud
18 in unemployment insurance programs during the
19 COVID-19 pandemic was likely between \$100 billion
20 and \$135 billion and found that the majority of this
21 fraud occurred because compromises of identity.

22 (4) The Financial Crimes Enforcement Net-
23 work of the Department of the Treasury reported
24 that \$212 billion worth of suspicious financial trans-
25 actions in 2021 was tied to some form of identity

1 compromise; in 2024, they revealed that this number
2 had exploded in 2023, covering over 70 percent of
3 all Suspicious Activity Reports (SARs) filed by
4 banks, tied to \$394 billion of transactions.

5 (5) In 2024, the Department of the Treasury
6 report on “Managing Artificial Intelligence-Specific
7 Cybersecurity Risks in the Financial Services Sec-
8 tor” flagged the threat of new “deepfake” attacks
9 powered by artificial intelligence and noted “The vol-
10 ume of these types of exploitations or cyber-enabled
11 attacks is likely to rise as technological developments
12 like Generative AI reduce the cost, complexity, and
13 time required to leverage gaps in our digital infra-
14 structure.”.

15 (6) The inadequacy of current digital identity
16 solutions degrades security and privacy for all Amer-
17 icans, and as “deepfake” attacks become more prev-
18 alent, next generation solutions are needed that can
19 protect consumers, businesses, and government
20 agencies from identity-related cybercrime.

21 (7) Government entities, as authoritative
22 issuers of identity in the United States, are uniquely
23 positioned to deliver critical components that ad-
24 dress deficiencies in our identity infrastructure and

1 augment private sector identity and authentication
2 solutions.

3 (8) State governments are particularly well
4 suited to play a role in enhancing digital identity so-
5 lutions used by both the public and private sectors,
6 given the role of State governments as the issuers of
7 driver's licenses and other identity documents com-
8 monly used today.

9 (9) The National Institute of Standards and
10 Technology (NIST) was directed in the CHIPS and
11 Science Act of 2022 to launch new work to develop
12 a framework of common definitions and voluntary
13 guidance for digital identity management systems,
14 including identity and attribute validation services
15 provided by Federal, State, and local governments,
16 and work is underway at NIST to create this guid-
17 ance. However, State and local agencies lack re-
18 sources to implement this new guidance, and if this
19 does not change, it will take decades to harden defi-
20 ciencies in identity infrastructure.

21 (10) It should be the policy of the Government
22 to use the authorities and capabilities of the Govern-
23 ment to enhance the security, reliability, privacy,
24 and convenience of digital identity solutions that
25 support and protect transactions between individ-

1 uals, government entities, and businesses, and that
2 enable Americans to prove who they are online.

3 **SEC. 3. IDENTITY FRAUD PREVENTION INNOVATION**
4 **GRANTS.**

5 (a) IN GENERAL.—The Secretary of the Treasury
6 shall, not later than 1 year after the date of the enactment
7 of this section, establish a grant program to provide iden-
8 tity fraud prevention innovation grants to States.

9 (b) USE OF AMOUNTS.—

10 (1) IN GENERAL.—States shall use amounts
11 provided under this section to—

12 (A) develop digital versions of driver’s li-
13 censes and other identity credentials that com-
14 ply with the guidelines for identity and at-
15 tribute validation services developed by the Na-
16 tional Institute of Standards and Technology
17 under section 504 of the Cybersecurity En-
18 hancement Act of 2014;

19 (B) protect the privacy and security of in-
20 dividuals, including guarding against
21 “deepfake” attacks powered by artificial intel-
22 ligence;

23 (C) catalyze the development, deployment,
24 and use of more resilient, interoperable solu-

1 tions Americans can use to protect and assert
2 their identity online;

3 (D) reduce identity theft and fraud by re-
4 placing legacy identity systems that are highly
5 vulnerable to attack from organized criminals
6 and hostile nation-states with more robust solu-
7 tions that can defeat these attacks;

8 (E) ensure the integrity of Government
9 benefit programs paid through the Department
10 of the Treasury;

11 (F) protect the United States financial sys-
12 tem from abuse by illicit actors; and

13 (G) enable more trusted transactions on-
14 line.

15 (2) REQUIREMENT.—Not less than 10 percent
16 of any amounts provided to a State under this sec-
17 tion shall be used by such State to provide services
18 designed to assist individuals with obtaining any
19 identity credentials or identity verification services
20 that are required to obtain a digital driver's license
21 or other digital identity credential offered by such
22 State physical; and

23 (c) LIMITATIONS.—A State may not use any amounts
24 provided under this section to—

1 (1) require a person to obtain or use a digital
2 driver's license or digital identity credential;

3 (2) support any effort by such State to elimi-
4 nate the issuance of physical driver's licenses and
5 physical identity credentials; or

6 (3) support the issuance of drivers licenses or
7 identity credentials to unauthorized immigrants.

8 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
9 tion may be construed to require any State to develop or
10 issue digital versions of driver's licenses or other identity
11 credentials.

12 (e) DEFINITIONS.—In this section:

13 (1) SECRETARY.—The term “Secretary” means
14 the Secretary of the Treasury.

15 (2) IDENTITY CREDENTIAL.—The term “iden-
16 tity credential” means a document or other evidence
17 of the identity of an individual issued by a State
18 that conveys the identity of the individual, including
19 a driver's license, State-issued identification card, or
20 birth certificate.

21 (3) UNAUTHORIZED IMMIGRANT.—The term
22 “unauthorized immigrant” means a person who is
23 not—

24 (A) is not citizen or national of the United
25 States;

1 (B) is not an alien lawfully admitted for
2 permanent or temporary residence in the
3 United States;

4 (C) does not have conditional permanent
5 resident status in the United States;

6 (D) does not have an approved application
7 for asylum in the United States; and

8 (E) did not enter into the United States
9 in refugee status.