OCTOBER 1, 2020

For more information, contact:

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Mike Dohmann
+1 202 626 9263
mdohmann@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

The "Improving Digital Identity Act of 2020" Presents Bipartisan Digital Identity Infrastructure Reform

On September 11, 2020, U.S. Representatives Bill Foster (D-IL), John Katko (R-NY), Jim Langevin (D-RI), and Barry Loudermilk (R-GA) introduced H.R. 8215, the Improving Digital Identity Act of 2020 ("the Act") to address the rising problem of identity fraud.

In its findings section, the Act highlights the increasing prevalence and problem of data security incidents and identity fraud. In 2019, over 164 million consumer records containing personally identifiable information were affected in the U.S. by data security incident, with identity fraud losses approaching $17 billion. Citing the inadequacy of current digital identity solutions, the Act seeks to address the pressing rise of identity fraud by:

1) Creating an "Improving Digital Identity Task Force" ("the Task Force") that would serve as a coordinated governmentwide effort aimed at protecting individual privacy;

2) Directing the National Institute of Standards and Technology ("NIST") to create new standards to guide government agencies when providing digital identity services; and

3) Establishing within the Department of Homeland Security ("DHS") a grant program to provide funding for States to upgrade systems that provide drivers' licenses and other types of identity credentials to support the development of highly secure, interoperable State systems that enable digital identity verification.

The Task Force:

The interdisciplinary Task Force would sit within the Executive Office of the President and comprise senior federal, state, and local officials, including the Secretaries of Treasury, Homeland Security, State, and Education; Directors of the Office of Management and Budget and NIST; Commissioner of the Social Security Administration; and Administrator of General Services (or their designees), as well as five State and five local government officials who represent agencies that issue identity credentials and who have knowledge of the systems used to provide such credentials. The Task Force's mandate would be to:

- Identify federal, state, and local agencies that issue identity information or hold information related to identifying an individual;
- Assess restrictions with respect to the abilities of such agencies to verify information for other agencies and nongovernmental organizations and identify any necessary statutory, regulatory, or policy changes to address such restrictions;
- Recommend a standards-based architecture to enable agencies to provide services related to digital identity verification in a way that is secure, protects privacy, and is rooted in consumer consent;
- Identify funding or resources needed to support such agencies that provide digital identity verification;
- Determine whether it would be practicable for such agencies to use a fee-based model to provide digital identity verification to private sector entities;
- Determine if any additional steps are necessary with respect to Federal, State and local agencies to improve digital identity verification and management processes for the purpose of enhancing the security, reliability, privacy, and convenience of digital identity solutions that support and protect transactions between individuals, government entities, and businesses;
- Assess risks related to potential criminal exploitation of digital identity verification services; and
- To the extent practicable, seek input from and collaborate with interested parties in the private sector.

Under the legislation, the Task Force would be required to publish recommendations within 180 days of enactment regarding: priorities for research and development in the systems that enable digital identity verification; and the standards-based architecture to be developed by NIST.

NIST Framework of Standards:

The Act would require the Director of NIST to develop a framework of standards, methodologies, procedures, and processes as a guide for Federal, State, and local governments to follow when providing services related to digital identity verification. In developing the framework, the NIST Director would be required to consider methods to protect the privacy of individuals; security needs; and the needs of potential end-users and individuals that will use services related to digital identity verifications.

Department of Homeland Security Grants:

No later than 18 months after enactment of the Act, the Secretary of Homeland Security would be required to award grants to States to upgrade systems that provide drivers' licenses and other types of identity credentials to support the development of highly secure, interoperable State systems that enable digital identity verification. A State that receives a grant would be required to use grant funds for services related to digital identity verification using the

NIST Framework. A grant recipient also would be required to use not less than 10 percent of grant funds to provide services that assist individuals with obtaining identity credentials or identity verification services needed to obtain a driver's license or State identity cards. The Act further would require the Secretary of Homeland Security to issue binding operational directives to Federal agencies for implementing the required NIST guidelines and the Office of Management and Budget's May 21, 2019 memorandum on ''Enabling Mission Delivery through Improved Identity, Credential, and Access Management.''

Potential Impacts of the Bill:

If enacted, the Act would encourage Federal, State, and local governments to upgrade their identity privacy infrastructures. Responsive governments likely would begin by offering new forms of digital identification to supplement or even replace commonly used digital identifiers such as social security numbers to comply with the NIST framework. Of course, for new forms of digital identification to have a meaningful impact, they would need to be interoperable and adopted by a critical mass of states. To that end, DHS grants offered under the Act would be instrumental in getting the program off the ground and helping to achieve this necessary critical mass.

If new forms of digital identification are adopted as recommended by the framework, the impact on consumer data security could be significant. The advancement of digital identification solutions promises increased security by offering a more trustworthy source of identification for online transactions. Some countries already have implemented digital identification systems that rely on biometric information. While using biometric information as a form of government issued identification may be unpalatable for some U.S. consumers, less invasive forms of digital identification, such as digital trails, may provide an appropriate level of security without sacrificing privacy. The additional security offered by digital identification also could help reduce the overall risk and severity of data breaches and identity fraud.

Road to Passage:

With commerce and financial transactions increasingly being conducted online due to the COVID-19 public health emergency, it is ideal timing for innovations in digital identification solutions. The sponsors of H.R. 8215 have taken a positive and bipartisan step forward in Congress' attempt to address the problem of identity fraud. The bill's introduction this late in the current Congress likely will preclude any meaningful consideration this year, particularly in view of the abbreviated legislative calendar and focus on the 2020 elections. Another complicating factor stems from the fact that the bill was referred to three different committees for consideration due to jurisdictional overlap. That said, the legislation is an important marker and the issue of digital identification is likely to remain top of mind for some time. Indeed, the bill's sponsors have already indicated their intention to reintroduce the measure at the start of the 117th Congress next year.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	GENEVA	MOSCOW	RIYADH	TOKYO
ATLANTA	CHICAGO	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
AUSTIN	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	
BRUSSELS	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE	