I

117TH CONGRESS
1ST SESSION

H. R. 5936

To include requirements relating to ransomware attack deterrence for a covered U.S. financial institution in the Consolidated Appropriations Act, 2021, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 9, 2021

Mr. MCHENRY introduced the following bill; which was referred to the Committee on Financial Services

---

A BILL

To include requirements relating to ransomware attack deterrence for a covered U.S. financial institution in the Consolidated Appropriations Act, 2021, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Ransomware and Financial Stability Act of 2021''.

SEC. 2. RANSOMWARE ATTACK DETERRENCE.

(a) IN GENERAL.—Section 108 of title I of division Q of the Consolidated Appropriations Act, 2021 (Public

Law 116–260; 135 Stat. 2173; 12 U.S.C. 1811 note) is amended—

(1) in the subsection heading, by striking ''**REPORT**'';

(2) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively;

(3) by inserting the following after subsection (c):

''(d) RANSOMWARE ATTACK DETERRENCE.—

''(1) REQUIREMENTS.—

''(A) IN GENERAL.—A covered U.S. financial institution subject to a ransomware attack may not make a ransomware payment in response to such ransomware attack—

''(i) before submitting the notification described in paragraph (2); and

''(ii) in an amount greater than $100,000, unless the payment is subject to a ransomware payment authorization.

''(B) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to permit a ransomware payment that is otherwise prohibited by law.

''(2) NOTIFICATION DESCRIBED.—

''(A) IN GENERAL.—The notification described in this paragraph shall be submitted by a covered U.S. financial institution to the Director of the Financial Crimes Enforcement Network and shall include—

''(i) a determination by such institution that such institution is subject to a ransomware attack; and

''(ii) a description of the ransomware attack and any associated ransomware payment demanded.

''(B) CONTENTS.—To ensure efficient notification and resolution of a ransomware attack, the Secretary of the Treasury—

''(i) shall, in consultation with interested persons, issue guidance specifying information required to be included in the notification described in this paragraph; and

''(ii) may not require, to be included in such notification, information that is unavailable to a covered U.S. financial institution, based on good-faith efforts of such institution to provide information.

''(3) WAIVER.—The President may waive the requirements of paragraph (2) with respect to a covered U.S. financial institution if the President determines that the waiver is in the national interest of the United States and notifies such institution and the appropriate members of Congress of such waiver.

''(4) SAFE HARBOR WITH RESPECT TO RANSOMWARE PAYMENT AUTHORIZATIONS AND GOOD-FAITH DETERMINATIONS.—

''(A) IN GENERAL.—With respect to a ransomware payment made under paragraph (2)(B) or a waiver issued under paragraph (3)—

''(i) a U.S. financial institution shall not be liable under subchapter II of chapter 53 of title 31, United States Code, or chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.) for making a ransomware payment consistent with the parameters and timing of a ransomware payment authorization; and

''(ii) no Federal or State department or agency may take any adverse supervisory action with respect to the U.S. fi-

nancial institution solely for making a ransomware payment consistent with the parameters and timing of the authorization.

''(B) GOOD-FAITH EFFORTS TO ASSESS RANSOMWARE ATTACKS.—A covered U.S. financial institution may not be held liable for deficiencies in describing a ransomware attack in a notification described under paragraph (2) if such institution engaged in good-faith efforts to determine the nature of the ransomware attack.

''(C) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed—

''(i) to prevent a Federal or State department or agency from verifying the validity of a ransomware payment authorization with the law enforcement agency submitting that authorization;

''(ii) to relieve a U.S. financial institution from complying with any other provision of law, including the reporting of suspicious transactions under section 5318(g) of title 31, United States Code; or

"(iii) to extend the safe harbor described in this paragraph to any actions taken by the U.S. financial institution—

"(I) before the date of issuance of ransomware payment authorization; or

"(II) after any termination date stated in the ransomware payment authorization

"(D) RANSOMWARE PAYMENT AUTHORIZATION TERMINATION DATE.—Any ransomware payment authorization submitted under this subsection shall include a termination date after which that authorization shall no longer apply.

"(E) RECORDS.—Any Federal law enforcement agency that submits to a U.S. financial institution a ransomware payment authorization shall, not later than 2 business days after the date on which the authorization is submitted to the U.S. financial institution—

"(i) submit to the Director of the Financial Crimes Enforcement Network a copy of the authorization; and

''(ii) alert the Director as to whether the U.S. financial institution has implemented the request.

''(F) GUIDANCE.—The Secretary of the Treasury, in coordination with the Attorney General, shall issue guidance on the required elements of a ransomware payment authorization.

''(5) CONFIDENTIALITY OF INFORMATION.—

''(A) IN GENERAL.—Except as provided in paragraph (2), any information or document provided by a U.S. financial institution to a Federal law enforcement agency pursuant to this subsection—

''(i) shall be exempt from disclosure under section 552 of title 5, United States Code; and

''(ii) may not be made publicly available.

''(B) EXCEPTIONS.—Paragraph (1) shall not prohibit the disclosure of the following:

''(i) Information relevant to any administrative or judicial action or proceeding.

''(ii) Information requested by the appropriate members of Congress or otherwise required to be submitted to Congress.

''(iii) Information required for Federal law enforcement or intelligence purposes (as determined by the Attorney General), in consultation with the Director of the Financial Crimes Enforcement Network to be disclosed to a domestic governmental entity or to a governmental entity of a United States ally or partner, only to the extent necessary for such purposes, and subject to appropriate confidentiality and classification requirements.

''(iv) Anonymized information required for the production of aggregate data or statistical analyses.

''(v) Information that the U.S. financial institution has consented to be disclosed to third parties.

''(6) DEFINITIONS.—In this subsection:

''(A) COVERED U.S. FINANCIAL INSTITUTION.—The term 'covered U.S. financial institution' means—

''(i) any financial market utility that the Financial Stability Oversight Council has designated as systemically important under section 804 of the Dodd-Frank Wall Street Reform and Consumer Protection Act;

''(ii) any exchange registered under section 6 of the Securities Exchange Act of 1934 that facilitates trading in any national market system security, as defined in section 242.600 of title 17, Code of Federal Regulations (or any successor regulation), and which exchange during at least four of the preceding six calendar months had—

''(I) with respect to all national market system securities that are not options, 10 percent or more of the average daily dollar volume reported by applicable transaction reporting plans; or

''(II) with respect to all listed options, 15 percent or more of the average daily dollar volume reported by applicable national market system

plans for reporting transactions in listed options; and

''(iii) any technology service provider in the Significant Service Provider Program of the Financial Institutions Examination Council that provides core processing services that is determined by the Council to be a significant technology service provider.

''(B) MALICIOUS SOFTWARE.—The term 'malicious software' means software that, when deployed, results in the loss of access to data or the loss of functionality of an information and communications system or network of a U.S. financial institution.

''(C) RANSOMWARE ATTACK.—The term 'ransomware attack' means the deployment of malicious software for the purpose of demanding payment in exchange for restoring critical access to, or the critical functionality of, an information and communications system or network.

''(D) RANSOMWARE PAYMENT.—The term 'ransomware payment' means a payment made by a U.S. financial institution (including a pay-

ment made through use of digital currency) to, at the request of, or for the benefit of a person responsible for a ransomware attack in exchange for restoration of the access or functionality of an information and communications system or network of the institution.

''(E) RANSOMWARE PAYMENT AUTHORIZATION.—The term 'ransomware payment authorization' means, with respect to a ransomware payment made by a U.S. financial institution, a written notice from a Federal law enforcement agency to authorize such ransomware payment.'';

(4) in subsection (f), as so redesignated, by striking ''after the date of enactment of this Act'' and inserting ''after the date of enactment of the Ransomware and Financial Stability Act of 2021''; and

(5) by adding at the end the following new subsection:

''(g) SHORT TITLE.—This section may be cited as the 'Cybersecurity and Financial System Resilience Act'.''.

(b) APPLICABILITY.—

(1) IN GENERAL.—The amendments made by this Act shall apply to a covered U.S. financial insti-

tution (as defined in subsection (d) of the Cybersecurity and Financial System Resilience Act (Public Law 116–260; 135 Stat. 2173; 12 U.S.C. 1811 note), as added by this Act) beginning on the earlier of the date that is—

(A) 30 days after publication in the Federal Register of rules implementing this Act; or

(B) 1 year after the date of the enactment of this Act.

(c) SUNSET.—This Act and the amendments made by this Act shall be repealed 10 years after the applicability date described in subsection (b).

○