



(Original Signature of Member)

117TH CONGRESS  
1ST SESSION

**H. R.**

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

Mr. MCHENRY introduced the following bill; which was referred to the  
Committee on \_\_\_\_\_

**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.

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 “Ransomware and Fi-  
5 nancial Stability Act of 2021”.

1 **SEC. 2. RANSOMWARE ATTACK DETERRENCE.**

2 (a) IN GENERAL.—Section 108 of title I of division  
3 Q of the Consolidated Appropriations Act, 2021 (Public  
4 Law 116–260; 135 Stat. 2173; 12 U.S.C. 1811 note) is  
5 amended—

6 (1) in the subsection heading, by striking “**RE-**  
7 **PORT**”;

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

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

12 “(d) RANSOMWARE ATTACK DETERRENCE.—

13 “(1) REQUIREMENTS.—

14 “(A) IN GENERAL.—A covered U.S. finan-  
15 cial institution subject to a ransomware attack  
16 may not make a ransomware payment in re-  
17 sponse to such ransomware attack —

18 “(i) before submitting the notification  
19 described in paragraph (2); and

20 “(ii) in an amount greater than  
21 \$100,000, unless the payment is subject to  
22 a ransomware payment authorization.

23 “(B) RULE OF CONSTRUCTION.—Nothing  
24 in this subsection shall be construed to permit  
25 a ransomware payment that is otherwise pro-  
26 hibited by law.

1 “(2) NOTIFICATION DESCRIBED.—

2 “(A) IN GENERAL.—The notification de-  
3 scribed in this paragraph shall be submitted by  
4 a covered U.S. financial institution to the Di-  
5 rector of the Financial Crimes Enforcement  
6 Network and shall include—

7 “(i) a determination by such institu-  
8 tion that such institution is subject to a  
9 ransomware attack; and

10 “(ii) a description of the ransomware  
11 attack and any associated ransomware  
12 payment demanded.

13 “(B) CONTENTS.—To ensure efficient noti-  
14 fication and resolution of a ransomware attack,  
15 the Secretary of the Treasury—

16 “(i) shall, in consultation with inter-  
17 ested persons, issue guidance specifying in-  
18 formation required to be included in the  
19 notification described in this paragraph;  
20 and

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

1           “(3) WAIVER.—The President may waive the  
2 requirements of paragraph (2) with respect to a cov-  
3 ered U.S. financial institution if the President deter-  
4 mines that the waiver is in the national interest of  
5 the United States and notifies such institution and  
6 the appropriate members of Congress of such waiv-  
7 er.

8           “(4) SAFE HARBOR WITH RESPECT TO  
9 RANSOMWARE PAYMENT AUTHORIZATIONS AND  
10 GOOD-FAITH DETERMINATIONS.—

11           “(A) IN GENERAL.—With respect to a  
12 ransomware payment made under paragraph  
13 (2)(B) or a waiver issued under paragraph  
14 (3)—

15           “(i) a U.S. financial institution shall  
16 not be liable under subchapter II of chap-  
17 ter 53 of title 31, United States Code, or  
18 chapter 2 of title I of Public Law 91–508  
19 (12 U.S.C. 1951 et seq.) for making a  
20 ransomware payment consistent with the  
21 parameters and timing of a ransomware  
22 payment authorization; and

23           “(ii) no Federal or State department  
24 or agency may take any adverse super-  
25 visory action with respect to the U.S. fi-

1           nancial institution solely for making a  
2           ransomware payment consistent with the  
3           parameters and timing of the authoriza-  
4           tion.

5           “(B) GOOD-FAITH EFFORTS TO ASSESS  
6           RANSOMWARE ATTACKS.—A covered U.S. finan-  
7           cial institution may not be held liable for defi-  
8           ciencies in describing a ransomware attack in a  
9           notification described under paragraph (2) if  
10          such institution engaged in good-faith efforts to  
11          determine the nature of the ransomware attack.

12          “(C) RULE OF CONSTRUCTION.—Nothing  
13          in this paragraph may be construed—

14                 “(i) to prevent a Federal or State de-  
15                 partment or agency from verifying the va-  
16                 lidity of a ransomware payment authoriza-  
17                 tion with the law enforcement agency sub-  
18                 mitting that authorization;

19                 “(ii) to relieve a U.S. financial institu-  
20                 tion from complying with any other provi-  
21                 sion of law, including the reporting of sus-  
22                 picious transactions under section 5318(g)  
23                 of title 31, United States Code; or

1 “(iii) to extend the safe harbor de-  
2 scribed in this paragraph to any actions  
3 taken by the U.S. financial institution—

4 “(I) before the date of issuance  
5 of ransomware payment authorization;  
6 or

7 “(II) after any termination date  
8 stated in the ransomware payment au-  
9 thorization

10 “(D) RANSOMWARE PAYMENT AUTHORIZA-  
11 TION TERMINATION DATE.—Any ransomware  
12 payment authorization submitted under this  
13 subsection shall include a termination date after  
14 which that authorization shall no longer apply.

15 “(E) RECORDS.—Any Federal law enforce-  
16 ment agency that submits to a U.S. financial  
17 institution a ransomware payment authorization  
18 shall, not later than 2 business days after the  
19 date on which the authorization is submitted to  
20 the U.S. financial institution—

21 “(i) submit to the Director of the Fi-  
22 nancial Crimes Enforcement Network a  
23 copy of the authorization; and

1                   “(ii) alert the Director as to whether  
2                   the U.S. financial institution has imple-  
3                   mented the request.

4                   “(F) GUIDANCE.—The Secretary of the  
5                   Treasury, in coordination with the Attorney  
6                   General, shall issue guidance on the required  
7                   elements of a ransomware payment authoriza-  
8                   tion.

9                   “(5) CONFIDENTIALITY OF INFORMATION.—

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

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

18                   “(ii) may not be made publicly avail-  
19                   able.

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

22                   “(i) Information relevant to any ad-  
23                   ministrative or judicial action or pro-  
24                   ceeding.

1           “(ii) Information requested by the ap-  
2           propriate members of Congress or other-  
3           wise required to be submitted to Congress.

4           “(iii) Information required for Federal  
5           law enforcement or intelligence purposes  
6           (as determined by the Attorney General),  
7           in consultation with the Director of the Fi-  
8           nancial Crimes Enforcement Network to be  
9           disclosed to a domestic governmental entity  
10          or to a governmental entity of a United  
11          States ally or partner, only to the extent  
12          necessary for such purposes, and subject to  
13          appropriate confidentiality and classifica-  
14          tion requirements.

15          “(iv) Anonymized information re-  
16          quired for the production of aggregate data  
17          or statistical analyses.

18          “(v) Information that the U.S. finan-  
19          cial institution has consented to be dis-  
20          closed to third parties.

21          “(6) DEFINITIONS.—In this subsection:

22                 “(A) COVERED U.S. FINANCIAL INSTITU-  
23                 TION.—The term ‘covered U.S. financial insti-  
24                 tution’ means—



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

7           “(ii) any exchange registered under  
8           section 6 of the Securities Exchange Act of  
9           1934 that facilitates trading in any na-  
10          tional market system security, as defined  
11          in section 242.600 of title 17, Code of  
12          Federal Regulations (or any successor reg-  
13          ulation), and which exchange during at  
14          least four of the preceding six calendar  
15          months had—

16               “(I) with respect to all national  
17               market system securities that are not  
18               options, 10 percent or more of the av-  
19               erage daily dollar volume reported by  
20               applicable transaction reporting plans;  
21               or

22               “(II) with respect to all listed op-  
23               tions, 15 percent or more of the aver-  
24               age daily dollar volume reported by  
25               applicable national market system

1 plans for reporting transactions in  
2 listed options; and

3 “(iii) any technology service provider  
4 in the Significant Service Provider Pro-  
5 gram of the Financial Institutions Exam-  
6 ination Council that provides core proc-  
7 essing services that is determined by the  
8 Council to be a significant technology serv-  
9 ice provider.

10 “(B) MALICIOUS SOFTWARE.—The term  
11 ‘malicious software’ means software that, when  
12 deployed, results in the loss of access to data or  
13 the loss of functionality of an information and  
14 communications system or network of a U.S. fi-  
15 nancial institution.

16 “(C) RANSOMWARE ATTACK.—The term  
17 ‘ransomware attack’ means the deployment of  
18 malicious software for the purpose of demand-  
19 ing payment in exchange for restoring critical  
20 access to, or the critical functionality of, an in-  
21 formation and communications system or net-  
22 work.

23 “(D) RANSOMWARE PAYMENT.—The term  
24 ‘ransomware payment’ means a payment made  
25 by a U.S. financial institution (including a pay-

1           ment made through use of digital currency) to,  
2           at the request of, or for the benefit of a person  
3           responsible for a ransomware attack in ex-  
4           change for restoration of the access or  
5           functionality of an information and communica-  
6           tions system or network of the institution.

7           “(E) RANSOMWARE PAYMENT AUTHORIZA-  
8           TION.—The term ‘ransomware payment author-  
9           ization’ means, with respect to a ransomware  
10          payment made by a U.S. financial institution, a  
11          written notice from a Federal law enforcement  
12          agency to authorize such ransomware pay-  
13          ment.”;

14          (4) in subsection (f), as so redesignated, by  
15          striking “after the date of enactment of this Act”  
16          and inserting “after the date of enactment of the  
17          Ransomware and Financial Stability Act of 2021”;  
18          and

19          (5) by adding at the end the following new sub-  
20          section:

21          “(g) SHORT TITLE.—This section may be cited as the  
22          ‘Cybersecurity and Financial System Resilience Act’.”.

23          (b) APPLICABILITY.—

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

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

6               (A) 30 days after publication in the Fed-  
7               eral Register of rules implementing this Act; or

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

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