117TH CONGRESS
2D SESSION

S. 4985

To amend the Cybersecurity Information Sharing Act of 2015 to include voluntary information sharing of cyber threat indicators among cryptocurrency companies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 28, 2022

Mrs. BLACKBURN (for herself and Ms. LUMMIS) introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

---

A BILL

To amend the Cybersecurity Information Sharing Act of 2015 to include voluntary information sharing of cyber threat indicators among cryptocurrency companies, 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 ''Cryptocurrency Cybersecurity Information Sharing Act''.

SEC. 2. SHARING OF CYBER THREAT INDICATORS BY COVERED COMPANIES.

(a) IN GENERAL.—The Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) is amended—

(1) in section 102(15)(A) (6 U.S.C. 1501(15)(A)) by inserting ''covered company (as defined in section 110),'' after ''cooperative,'';

(2) by redesignating sections 110 and 111 (6 U.S.C. 1509, 1510) as sections 111 and 112, respectively; and

(3) by inserting after section 109 (6 U.S.C. 1508) the following:

''SEC. 110. SHARING OF CYBER THREAT INDICATORS BY COVERED COMPANIES.

''(a) DEFINITIONS.—In this section:

''(1) COVERED COMPANY.—

''(A) IN GENERAL.—Subject to subparagraph (B), the term 'covered company' means an entity—

''(i) that is—

''(I) engaged in the business of validating distributed ledger technology transactions;

''(II) engaged in the business of developing digital assets or the cor-

responding protocols for use of digital assets by other persons;

"(III) an association of entities that manage digital assets or distributed ledger technologies; or

"(IV) a commercial general liability insurance provider or property insurance provider offering products designed to mitigate losses from a variety of cyber incidents, including—

"(aa) data breaches;

"(bb) ransomware attacks;

"(cc) business interruption; and

"(dd) network damage; and

"(ii) that shares or receives information under this section.

"(B) MONEY SERVICES BUSINESSES AND FINANCIAL INSTITUTIONS.—For purposes of paragraphs (1), (2), and (3) of subsection (b), the term 'covered company' includes an entity that is a money services business, or that otherwise is a financial institution, as defined in section 5312 of title 31, United States Code, for

purposes of digital asset activity engaged in by the entity.

''(2) DIGITAL ASSET.—The term 'digital asset' means a natively electronic asset that—

''(A) confers economic, proprietary, or access rights or powers; and

''(B) is recorded using cryptographically secured distributed ledger technology, or any similar analogue.

''(3) DISTRIBUTED LEDGER TECHNOLOGY.—The term 'distributed ledger technology' means technology that enables the operation and use of a ledger that—

''(A) is shared across a set of distributed nodes that participate in a network and store a complete or partial replica of the ledger;

''(B) is synchronized between the nodes;

''(C) has data appended to the ledger by following the specified consensus mechanism of the ledger;

''(D) may be accessible to anyone or restricted to a subset of participants; and

''(E) may require participants to have authorization to perform certain actions or require no authorization.

''(b) VOLUNTARY INFORMATION SHARING AMONG COVERED COMPANIES.—

''(1) IN GENERAL.—Subject to paragraphs (2), (3), and (4), a covered company may, under the protection of the safe harbor from liability described in subsection (d), transmit, receive, or otherwise share information with any other covered company regarding individuals, entities, organizations, and countries for purposes of identifying and, as appropriate, reporting activities that the covered company suspects may involve possible cyber threat indicators.

''(2) INFORMATION SHARING BETWEEN COVERED COMPANIES.—

''(A) NOTICE REQUIREMENT.—

''(i) IN GENERAL.—A covered company that intends to share information as described in paragraph (1) shall submit a notice of intent to the Financial Crimes Enforcement Network and the Cybersecurity and Infrastructure Security Agency, which shall contain, at a minimum, a list of each other company the covered company intends to share information with.

''(ii) EFFECTIVE PERIOD.—Each notice provided under clause (i) shall be ef-

fective for the 1-year period beginning on the date of the notice.

''(iii) ADDITIONAL NOTICES.—Upon expiration of the 1-year period described in subclause (ii), a covered company shall submit an additional notice of intent at the beginning of each year during which the covered company intends to share information as described in paragraph (1).

''(iv) LIST OF COVERED COMPANIES THAT HAVE SUBMITTED NOTICE.—The Financial Crimes Enforcement Network shall periodically make available a list of covered companies that have submitted a notice under this subparagraph.

''(B) VERIFICATION REQUIREMENT.—Prior to sharing information as described in paragraph (1), a covered company shall take reasonable steps to verify that the company with which the covered company intends to share information is listed in a notice required under subparagraph (A).

''(3) PROTECTION AND USE OF INFORMATION BY COVERED COMPANIES.—

"(A) PURPOSE.—Information received by a covered company under this section may not be used for any purpose other than—

"(i) identifying and, as appropriate, reporting on cyber threat indicators; or

"(ii) assisting the covered company in complying with any requirement of this title.

"(B) PROCEDURES FOR PROTECTION OF INFORMATION.—Each covered company that engages in the sharing of information under this section shall maintain adequate procedures to protect the security and confidentiality of the information in accordance with the policies and guidelines established under subsection (c).

"(4) REPORTING REQUIREMENTS FOR COVERED COMPANIES.—

"(A) CYBERSECURITY THREAT INFORMATION.—A covered company that identifies cybersecurity threat information requiring immediate attention, such as suspected terrorist activity, shall, as soon as practicable but not later than 36 hours after identifying the information—

''(i) notify an appropriate law enforcement authority and the Cybersecurity and Infrastructure Security Agency Incident Reporting System; and

''(ii) comply with any other Federal requirements for reporting suspicious activity.

''(B) SUSPICIOUS ACTIVITY.—

''(i) VOLUNTARY REPORTING TO FEDERAL AGENCIES.—A covered company may voluntarily report suspicious activity to the Financial Crimes Enforcement Network and the Cybersecurity and Infrastructure Security Agency under this section.

''(ii) RULE OF CONSTRUCTION.—Nothing in this subparagraph shall be construed to—

''(I) modify the requirements for reporting suspicious activity if a covered company is subject to such regulations; or

''(II) create new suspicious activity reporting requirements for a covered company that is not currently subject to such a regulation.

''(C) EXEMPTION FROM DISCLOSURE.—Information shared under this paragraph shall be exempt from disclosure under any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records, in accordance with section 104(d)(4)(B).

''(c) INFORMATION SHARING BETWEEN COVERED COMPANIES AND THE FEDERAL GOVERNMENT.—

''(1) POLICIES AND PROCEDURES.—

''(A) IN GENERAL.—Not later than 180 days after the date of enactment of the Cryptocurrency Cybersecurity Information Sharing Act, the Director of the Financial Crimes Enforcement Network and the Director of the Cybersecurity and Infrastructure Security Agency shall, in consultation with the National Cyber Director and the heads of the appropriate Federal entities, jointly develop and make publicly available policies and procedures relating to the receipt by the Federal Government of cyber threat indicators shared by covered companies.

''(B) CONSIDERATIONS.—In developing the policies and procedures required under subparagraph (A), the Director of the Financial Crimes Enforcement Network and the Director of the Cybersecurity and Infrastructure Security Agency shall take into account the requirements described in subsections (a)(3) and (b)(3) of section 105.

''(C) COMPLIANCE WITH SIMILAR PROCEDURES.—In the case of a covered company that is required to comply with section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801) and the Payment Card Industry Data Security Standard, and applicable regulations issued thereunder, the covered company shall be considered to be acting in compliance with the requirements developed under this subsection if the covered company applies the procedures required under such section 501 to information shared under this section.

''(2) GUIDELINES.—

''(A) IN GENERAL.—Not later than 60 days after the date of enactment of the Cryptocurrency Cybersecurity Information Sharing Act, the Director of the Financial

Crimes Enforcement Network and the Director of the Cybersecurity and Infrastructure Security Agency shall jointly develop and make publicly available guidance—

"(i) to assist covered companies and promote sharing of cyber threat indicators with Federal entities under this section; and

"(ii) relating to adequate procedures to protect the security and confidentiality of information shared under this section, as required under subsection (b)(3)(B).

"(B) CONTENTS.—The guidelines required under subparagraph (A) shall include guidance relating to the following:

"(i) Identification of types of information that would qualify as a cyber threat indicator under this title and that would be unlikely to include information that—

"(I) is not directly related to a cybersecurity threat; and

"(II) is personal information of a specific individual or information that identifies a specific individual.

''(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

''(iii) Such other matters as the Director of the Financial Crimes Enforcement Network and the Director of the Cybersecurity and Infrastructure Security Agency consider appropriate for entities sharing cyber threat indicators with Federal entities under this title.

''(3) COMPLIANCE WITH THE PAPERWORK REDUCTION ACT.—In establishing requirements under this subsection, the Secretary shall ensure that the requirements comply with chapter 35 of title 44, United States Code (commonly known as the ''Paperwork Reduction Act'').

''(d) SAFE HARBOR FROM CERTAIN LIABILITY.—The liability protections in section 106 shall not apply to a covered company to the extent the company fails to comply with paragraphs (2), (3), and (4) of subsection (b).

''(e) EXEMPTION FROM DISCLOSURE.—In accordance with paragraphs (3) and (8) of section 502(e) of the Gramm-Leach-Bliley Act (15 U.S.C. 6802), if a covered company voluntarily shares information pursuant to this

section, the covered company shall not be required to provide any affected consumer the notice required under section 503 of the Gramm-Leach-Bliley Act (15 U.S.C. 6803).''.

(b) CONFORMING AMENDMENT.—The table of contents in section 1(b) of division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 129 Stat. 2935) is amended by striking the items relating to sections 110 and 111 and inserting the following:

''Sec. 110. Sharing of cyber threat indicators by covered companies.
''Sec. 111. Exception to limitation on authority of Secretary of Defense to disseminate certain information.
''Sec. 112. Effective period.''.

○