I

108TH CONGRESS
1ST SESSION

H. R. 1636

To protect and enhance consumer privacy, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 3, 2003

Mr. STEARNS (for himself, Mr. BOUCHER, Mr. TAUZIN, Mr. TERRY, Mr. BASS, Ms. ESHOO, Mr. WHITFIELD, Mr. GORDON, Mrs. BONO, Mr. MORAN of Virginia, Mr. GILLMOR, Mr. BILIRAKIS, Mr. TOWNS, Mr. DEAL of Georgia, Mr. WELLER, Mr. SHIMKUS, Mr. GREENWOOD, Mr. UPTON, Ms. DEGETTE, Mr. WALDEN of Oregon, Ms. HARMAN, Mr. WELDON of Florida, and Mr. SHADEGG) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To protect and enhance consumer privacy, 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 ''Consumer Privacy Protection Act of 2003''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 3. DEFINITIONS.

In this Act:

(1) The term ''Commission'' means the Federal Trade Commission.

(2) The term ''consumer'' means an individual acting in the individual's personal, family, or household capacity.

(3)(A) The term ''data collection organization'' means an entity (or an agent or affiliate of the entity) that collects (by any means, through any medium), sells, discloses for consideration, or uses personally identifiable information of the consumer.

(B) Such term does not include—

(i) a governmental agency;

(ii) a not-for-profit entity, to the extent that personally identifiable information is not used for a commercial purpose;

(iii) an entity that—

(I) has annual gross revenue under $1,000,000 (based on the value of such amount in fiscal year 2000, adjusted for current dollars);

(II) has fewer than 25 employees;

(III) collects or uses personally identifiable information from fewer than 1,000 consumers for a purpose unrelated to a transaction with the consumer;

(IV) does not process personally identifiable information of consumers; and

(V) does not sell or disclose for consideration such information to another person;

(iv) a provider of professional services, or any affiliate thereof, to the extent that such provider is obligated by rules of professional ethics, or by applicable law or regulation, not to voluntarily disclose confidential client information without the consent of the client; or

(v) a data processing outsourcing entity.

(4)(A) The term ''personally identifiable information'', with respect to a data collection organization means individually identifiable information relating to a living individual who can be identified from that information.

(B) Such term includes—

(i) first and last name, whether given at birth or adoption, assumed, or legally changed;

(ii) home or other physical address including street name and name of a city or town;

(iii) electronic mail address;

(iv) telephone number;

(v) social security number; or

(vi) any other unique identifying information that a data collector and processor collects and combines with any information described in the preceding subparagraphs of this paragraph.

(C) Such term does not include—

(i) anonymous or aggregate data, or any other information that does not identify a unique living individual;

(ii) information about a consumer inferred from data maintained about a consumer; or

(iii) information about a consumer obtained from a public record.

(5) The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company.

(6) The term ''information-sharing affiliate'' means any affiliate that is under common control with a data collection organization, and is contractually obligated to comply with the practices enumerated under the privacy policy statement of the organization required under section 102.

(7) The term ''data processing outsourcing entity'' means, with respect to a data collection organization, a non-affiliated entity that—

(A) provides information technology processing, Web hosting, or telecommunications services to the data collection organization;

(B) is contractually obligated to comply with security controls specified by the data collection organization; and

(C) has no right to use the data collection organization's personally identifiable information other than for performing data processing outsourcing services for the data collection organization or as required by law.

(8) The term ''process'', with respect to personally identifiable information, means any value-added activity performed on data by automated means.

(9) The term ''transaction'' means an interaction between a consumer and a data collection organization resulting in—

(A) any use of information that is necessary to complete the interaction in the course of which information is collected, or to maintain the provisioning of a good or service requested by the consumer, including use—

(i) to approve, guarantee, process, administer, complete, enforce, provide, or market a product, service, account, benefit, transaction, or payment method that is requested or approved by the consumer; or

(ii) to deliver goods, services, funds, or other consideration to, or on behalf of, the consumer;

(B) any disclosure of information that is necessary for the consumer to enforce any right of the consumer;

(C) any disclosure of information that is required by law or by a court order; and

(D) any use of information to verify personally identifiable information by the consumer, evaluate, detect, or reduce the risk of fraud or other criminal activity, or other risk-management activities.

(10) The term ''display'' means intentionally communicating or otherwise making available (on the Internet or in any other manner) to another person.

(11) The term ''public record'' means any item, collection, or grouping of information about an individual that is maintained by a Federal, State, or

local government entity and that is made available to the public.

(12) The term ''purchase'' means providing, directly or indirectly, anything of value in exchange for a good or service.

(13) The term ''State'' includes the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, American Samoa, Guam, the Virgin Islands, the Freely Associated States, and any other territory or possession of the United States.

TITLE I—PROTECTION OF INDIVIDUAL PRIVACY IN INTERSTATE COMMERCE

SEC. 101. PRIVACY NOTICES TO CONSUMERS.

(a) NOTICE REQUIRED.—A data collection organization shall provide to a consumer a notice containing the information required under subsection (b) as follows:

(1) Upon the first instance of collection from the consumer of personally identifiable information, that may be used for a purpose unrelated to the transaction, by a data collection organization, the organization shall provide the notice at the time personally identifiable information is collected.

(2) Upon a material change in the organization's privacy policy under section 102(a), the organization shall provide the notice, not later than the first time after such change in policy that the organization seeks to collect, sell, disclose for consideration, or use personally identifiable information to the extent practicable, to each consumer from whom the organization has collected such information.

(b) FORM AND CONTENTS OF NOTICE.—A notice required under subsection (a) shall be provided in a clear and conspicuous manner, be prominently displayed or explicitly stated to the consumer, and contain the following information:

(1) A statement that the personal information collected by the data collection organization may be used or disclosed for purposes or transactions unrelated to that for which it was collected, as described in the organization's privacy statement.

(2) A description of the manner in which the consumer may obtain a privacy policy statement that meets the requirements of section 102, which may include providing the consumer with an Internet website, a hyperlink to such a website, or a toll-free telephone number from which such a statement may be obtained. If the notice required under subsection

(a) is provided to the consumer by means of an Internet website, one manner in which the consumer may obtain the privacy policy statement must be by means of an Internet website.

(3) If the notice is required under subsection (a)(2), a statement that there has been a material change in the organization's privacy policy.

SEC. 102. PRIVACY POLICY STATEMENTS.

(a) PRIVACY POLICY.—A data collection organization shall establish a privacy policy with respect to the collection, sale, disclosure for consideration, dissemination, use, and security of the personally identifiable information of consumers, the principal elements of which shall be embodied in a privacy policy statement (or statements) that meets the requirements of subsection (b).

(b) STATEMENT.—The statement (or statements) required under subsection (a) shall meet the following requirements:

(1) The statement must be brief, concise, clear, and conspicuous and written in plain language.

(2) The statement must be accessible to all consumers of the data collection organization (regardless of the means by which a consumer conducts a transaction with the organization)—

(A) at no charge to the consumer; and

(B) at the time the data collection organization first collects personally identifiable information about the consumer that may be used for a purpose unrelated to a transaction with the consumer and subsequently.

(3) The statement must disclose only the following:

(A) The identity of each data collection organization, or a description of each class or type of data collection organization, that may collect or use the information.

(B) The types of information that may be collected or used.

(C) How the information may be used.

(D) Whether the consumer is required to provide the information in order to do business with the data collection organization.

(E) The extent to which the information is subject to sale or disclosure for consideration to a data collection organization that is not an information-sharing affiliate of the data collection organization providing the statement, including—

(i) a clear and prominent statement of the fact that the information is subject to such sale or disclosure for consideration;

(ii) a description of each class or type of data collection organization to which the information may be sold or disclosed for consideration;

(iii) to the extent practicable, the purpose for which the information may be used; and

(iv) the types of information that may be sold or disclosed for consideration.

(F) Whether the information security practices of the data collection organization meet the security requirements of section 105 in order to prevent unauthorized disclosure or release of personally identifiable information.

(c) COMMISSION FACILITATION.—The Commission shall take actions (including conducting industry-wide workshops) to facilitate the development of harmonized, universal wording or logo-based graphics in order to convey the contents of privacy policy statements required under this section.

SEC. 103. CONSUMER OPPORTUNITY TO LIMIT SALE OR DISCLOSURE OF INFORMATION.

(a) PRECLUSION OF SALE OR DISCLOSURE.—

(1) REQUIREMENT.—A data collection organization shall provide to the consumer, without charge, the opportunity to preclude any sale or disclosure for consideration of the consumer's personally identifiable information, provided in a particular data collection, that may be used for a purpose other than a transaction with the consumer, to any data collection organization that is not an information-sharing affiliate of the data collection organization providing such opportunity

(2) DURATION.—A preclusion on sale or disclosure for consideration of information established by a consumer under this subsection shall remain in effect for 5 years or until the consumer indicates otherwise, whichever occurs sooner. A data collection organization may not seek reconsideration of a consumer's preclusion of such sale or disclosure until at least 1 year after such preclusion has been imposed by the consumer.

(b) PERMISSION FOR SALE OR DISCLOSURE.—A data collection organization may provide the consumer an opportunity to permit the sale or disclosure described in subsection (a)(1) in exchange for a benefit to the consumer.

(c) ACCESSIBILITY.—The opportunity to preclude (or if offered, to permit) the sale or disclosure for consideration of information under this section must be both easy to access and use, and the notice of the opportunity to preclude must be clear and conspicuous..

SEC. 104. CONSUMER OPPORTUNITY TO LIMIT OTHER INFORMATION PRACTICES.

If a data collection organization provides to a consumer the opportunity to limit other practices of the data collection organization with respect to a particular collection or use of personally identifiable information regarding the consumer, other than that required by section 103—

(1) a notice and description of such opportunity must appear in the privacy statement;

(2) such opportunity must be easy to access and to use; and

(3) any limitation exercised by the consumer pursuant to such opportunity shall remain in effect, unless—

(A) the limitation is withdrawn by the consumer; or

(B) the data collection organization provides the consumer at least 30 days notice before materially changing the limitation or terminating its compliance with the limitation.

SEC. 105. INFORMATION SECURITY OBLIGATIONS.

(a) INFORMATION SECURITY POLICY.—

(1) IMPLEMENTATION.—A data collection organization shall prepare, revise as necessary, and implement an information security policy that is applicable to the information security practices and treatment of personally identifiable information maintained by the data collection organization, that is designed to prevent the unauthorized disclosure or release of such information.

(2) MANAGEMENT APPROVAL.—An information security policy created pursuant to paragraph (1) shall be considered and approved by the senior management officials of the data collection organization.

(3) CONTENTS.—An information security policy required under paragraph (1) shall include—

(A) a process for taking corrective action pursuant to subsection (b); and

(B) identifying an officer of the data collection organization as the point of contact with responsibility for information security issues for the organization.

(b) CORRECTIVE ACTIONS.—

(1) INFORMATION SECURITY ADVISORIES AND ACTION.—Except as provided in paragraph (2), upon the issuance of an information security advisory (as

such term is defined in subsection (d)), a data collection organization shall, within a reasonable period of time after the issuance of such advisory and pursuant to its information security policy, take appropriate action reasonably necessary to mitigate against any vulnerability identified in such advisory, including implementing any changes to its security practices and the architecture, installation, or implementation of its network or operating software (including corrective patches) in response to such advisory.

(2) EXCEPTIONS.—A data collection organization shall not be required to take the action specified in an information security advisory under paragraph (1) if such organization can, in good faith, show that—

(A) the corrective action required would cause harm to, or weaken, the organization's existing information security for personally identifiable information or the procedures or systems of the organization;

(B) the organization takes, or has taken, other appropriate steps or corrective action to mitigate the vulnerabilities and exposure risks

identified in the information security advisory; or

(C) the specified corrective action is not necessary.

(c) EFFECT OF RELEASE OF PERSONALLY IDENTIFIABLE INFORMATION.—If the security of a data collection organization has been compromised, resulting in the unauthorized release of a consumer's personally identifiable information, the data collection organization shall be presumed to be in violation of this section if such organization has failed to respond to an information security advisory in accordance with subsection (b)(1).

(d) DEFINITION.—As used in this section, the term ''information security advisory'' means an information security advisory issued by the Federal Computer Incident Response Center of the Department of Homeland Security, or its successor agency.

SEC. 106. SELF-REGULATORY PROGRAMS.

(a) SELF-REGULATORY PROGRAM.—

(1) PRESUMPTION OF COMPLIANCE.—The Commission shall presume that a data collection organization is in compliance with the provisions of sections 101 through 105 if that organization—

(A) participates in a self-regulatory program approved under subsection (b); and

(B) has been determined by a self-regulatory program to be in compliance with the guidelines, procedures, requirements, and restrictions of the program (including a remedial process under subsection (c)(7)).

(2) EFFECT OF WILLFUL NONCOMPLIANCE.—A data collection organization that participates in a self-regulatory program under this section shall not be liable for a civil penalty arising out of a violation of any provision of sections 101 through 105 unless such violation results from willful noncompliance with the guidelines, procedures, requirements, or restrictions of the program.

(b) APPROVAL BY COMMISSION.—

(1) APPROVAL.—The Commission shall, within 90 days after submission of an application for approval of a self-regulatory program under this section (or of a material change in a program previously approved by the Commission), approve such program (or change) if the Commission finds that the program (or change) complies with the requirements of subsection (c).

(2) FORM OF APPLICATION.—The Commission shall accept an application for approval under para-

graph (1) in any reasonable form the applicant may submit.

(3) DURATION UNTIL RENEWAL.—A self-regulatory program approved by the Commission under paragraph (1) shall be approved for a period of 5 years.

(4) REVOCATION OF APPROVAL.—The Commission may, after notice and opportunity for a hearing, revoke approval granted under paragraph (1), if the Commission finds that a self-regulatory program fails to meet the requirements of subsection (c).

(5) JUDICIAL REVIEW.—Any order by the Commission denying approval of a self-regulatory program shall be subject to judicial review, as provided in section 706 of title 5, United States Code.

(c) REQUIREMENTS OF SELF-REGULATORY PROGRAM.—A self-regulatory program complies with the requirements of this subsection if the program provides each of the following:

(1) Guidelines and procedures requiring a program participant to provide substantially equivalent or greater protections for consumers and their personally identifiable information as are provided under sections 101 through 105.

(2) Procedures and requirements to provide for—

(A) an initial review of a participant's privacy statement and privacy policy, and subsequent review whenever such statement or policy is substantively changed, to determine whether the participant complies with the self-regulatory program's guidelines;

(B) an initial self-review and self-certification of a participant's privacy policy and practices to ensure compliance with the guidelines, procedures, requirements, and restrictions of the program established under this subsection;

(C) subsequent periodic self-reviews and self-certifications, which shall occur at least annually, of the participant's privacy policy and practices to ensure continued compliance with such guidelines, procedures, requirements, and restrictions;

(D) submission of self-reviews and self-certifications under this paragraph to any administrator of the program; and

(E) random compliance testing of participants, which may concentrate on selected com-

pliance issues, if the self-regulatory program conducts—

(i) a random compliance test with respect to each participant not less frequently than every 3 years;

(ii) a full compliance test in any case where non-compliance with any of the selected compliance issues is identified; and

(iii) full compliance tests of participants with a high number of complaints against them.

(3) Procedures and requirements that ensure that a program participant provides a process for resolving disputes with consumers relating to the privacy policy and practices of the participant. Such dispute resolution process—

(A) must be available without charge to a consumer;

(B) must be available at a cost to the participant that is reasonable and does not discourage participation by the participant in such process;

(C) must ensure that consumers are informed of how to utilize the process;

(D) may include, as one choice among others, binding arbitration; and

(E)(i) must be completed within 60 days after submission of the dispute by the consumer; or

(ii) must be completed within 90 days after submission of the dispute by the consumer, if the participant—

(I) determines that additional time is required to obtain information to make an informed decision with respect to the dispute; and

(II) notifies the consumer and the self-regulatory program that such additional time is required.

(4) Provisions for the use by participants in the program of a means (including the use of a seal) to represent the participant's participation in the program.

(5) With respect to any nonvoluntary suspension or termination of participation in the program because of the participant's failure to comply with the program, procedures or requirements to provide for the following:

(A) Publication of notice and the reasons for any such suspension or termination, except that no personally identifiable information related to such suspension or termination may be published.

(B) Notice to the Commission of any such termination.

(6) Requirements and restrictions that assure independence with respect to program eligibility, compliance, and dispute resolution mechanisms and decisions from improper interference by management or ownership of the self-regulatory program participant.

(7) A process for a noncompliant participant to take timely remedial action in order to come back into compliance with the program before suspension or termination of participation in the program.

(d) CONSUMER DISPUTE RESOLUTION.—

(1) SELF-REGULATORY DISPUTE PROCESS.—If a consumer has a dispute with a participant in a self-regulatory program under this section or under section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that such dispute pertains to the entity's privacy policy or practices required for participation in the self-regulatory program, the

consumer shall initially seek resolution through the participant's dispute resolution process (established in accordance with subsection (c)(3)). The Commission shall promptly refer to the participant involved any dispute submitted to the Commission for which resolution has not been initially sought through such process.

(2) RESOLUTION BY COMMISSION.—A consumer may submit to the Commission for resolution a dispute with a participant in a self-regulatory program under this section, if the following requirements are met:

(A) The dispute was initially submitted under paragraph (1) for resolution through the participant's dispute resolution process.

(B) The dispute submitted under paragraph (1) is not resolved—

(i) within 60 days after submission of the dispute by the consumer; or

(ii) to the satisfaction of the consumer.

(C) Notice of the facts of the dispute is submitted to the Commission not later than 30 days after the date on which the consumer is

notified of the resolution through the participant's dispute resolution process.

(D) The consumer has not voluntarily accepted a resolution of the dispute under paragraph (1).

(E) The dispute was not resolved through binding arbitration.

(3) LIMITATION.—Nothing in this Act shall prevent the Commission from investigating compliance with this Act by a participant in a self-regulatory organization based upon a complaint from an individual or organization other than a consumer with a dispute with such participant, or on its own initiative, except that prior to instituting any such investigation the Commission shall afford the self-regulatory organization a reasonable opportunity to invoke its own remedial procedures and assure compliance by the participant.

(4) CLEAR AND CONVINCING EVIDENCE.—The presumption established by paragraph (1) of subsection (a) may be overcome by clear and convincing evidence of non-compliance.

(e) NONRELEASE OF CERTAIN INFORMATION.—The Commission may not compel a participant in a self-regulatory program approved under subsection (b) (or an ad-

ministrator of such a program) to provide proprietary information or personally identifiable information of consumers to the Commission unless the Commission provides assurances that such information will not be released to the public.

(f) MISREPRESENTATION OF SELF-REGULATORY PROGRAM PARTICIPATION.—It is unlawful for a data collection organization to misrepresent that it is a participant in a self-regulatory program (including through any mechanism provided under subsection (c)(4)) when such organization is not, in fact, such a participant.

(g) EXEMPTED ENTITY PARTICIPATION.—An entity that is not a data collection organization and that voluntarily participates in a self-regulatory program under this section shall enjoy the rights and benefits provided under this section in any action or investigation under section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that such action or investigation pertains to the entity's privacy policy or practices required for participation in the self-regulatory program.

SEC. 107. ENFORCEMENT.

(a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A violation of any provision of this title by a data collection organization is an unfair or deceptive act or practice unlawful under section 5(a)(1) of the Federal Trade Com-

mission Act (15 U.S.C. 45(a)(1)), except that the amount of any civil penalty under such Act shall be doubled for a violation of this title, but may not exceed $500,000 for all related violations by a single violator (without respect to the number of consumers affected or the duration of the related violations).

(b) GUIDELINES AND OPINIONS.—In order to assist in compliance with this title, the Federal Trade Commission may promulgate regulations and interpretive rules under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a), with respect to specific types of acts or practices that would, or would not, comply with this title.

SEC. 108. NO PRIVATE RIGHT OF ACTION.

This title may not be considered or construed to provide any private right of action. No private civil action relating to any act or practice governed under this title may be commenced or maintained in any State court or under State law (including a pendent State claim to an action under Federal law).

SEC. 109. EFFECT ON OTHER LAWS.

(a) QUALIFIED EXEMPTION FOR COMPLIANCE WITH OTHER FEDERAL PRIVACY LAWS.—To the extent that personally identifiable information protected under this title is also protected under a provision of Federal privacy law described in subsection (c), a data collection organiza-

tion that complies with the relevant provision of such other Federal privacy law shall be deemed to have complied with the corresponding provision of this title.

(b) PROTECTION OF OTHER FEDERAL PRIVACY LAWS.—Nothing in this title may be construed to modify, limit, or supersede the operation of the Federal privacy laws described in subsection (c) or the provision of information permitted or required, expressly or by implication, by such laws, with respect to Federal rights and practices.

(c) OTHER FEDERAL PRIVACY LAWS DESCRIBED.—The provisions of law to which subsections (a) and (b) apply are the following:

(1) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974).

(2) The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.).

(3) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(4) The Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq.).

(5) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(6) Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 et seq.).

(7) The Electronic Communications Privacy Act of 1986 (Public Law 99–508).

(8) The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.).

(9) The Family Educational Rights and Privacy Act of 1974 (20 U.S.C. 1221 note, 1232g).

(10) Section 445 of the General Education Provisions Act (20 U.S.C. 1232h).

(11) The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et seq.).

(12) Section 222 of the Communications Act of 1934 (47 U.S.C. 222) relating to the Customer Proprietary Network Information.

(13) The Cable Communications Policy Act of 1984 (47 U.S.C. 521 et seq.).

(14) The Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(15) The Video Privacy Protection Act of 1988 (Public Law 100–618).

(16) The Telephone Consumer Protection Act of 1991 (Public Law 102–243).

(17) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191), as it relates to an entity described in section 1172(a) of the Social Security Act (42 U.S.C. 1320d-1(a)) or

to activities regulated under section 1173 of such Act (42 U.S.C. 1320d-2).

(d) PREEMPTION OF STATE PRIVACY LAWS.—This title preempts any statutory law, common law, rule, or regulation of a State, or a political subdivision of a State, to the extent such law, rule, or regulation relates to or affects the collection, use, sale, disclosure, retention, or dissemination of personally identifiable information in commerce. No State, or political subdivision of a State, may take any action to enforce this title.

SEC. 110. EFFECTIVE DATE.

This title shall apply with respect to personally identifiable information collected on or after the date that is 1 year after the date of enactment of this Act.

TITLE II—IDENTITY THEFT PREVENTION AND REMEDIES

SEC. 201. FACILITATING ELECTRONIC IDENTITY THEFT AFFIDAVITS.

The Commission shall take such action as necessary to permit (including by electronic means) consumers that have a reasonable belief that they are a victim of identity theft—

(1) to enter required consumer information in the commission-developed document entitled ''Identity Theft Affidavit''; and

(2) to submit completed forms and other supplemental information to the Commission and other entities.

SEC. 202. PROMOTING USE OF COMMON IDENTITY THEFT AFFIDAVIT.

The Commission shall take such action as necessary to solicit the acceptance and acknowledgement of standardized Identity Theft Affidavit by entities that receive disputes regarding the unauthorized use of accounts of such entities from consumers that have reason to believe that they are victims of identity theft.

SEC. 203. TIMELY RESOLUTION OF IDENTITY THEFT DISPUTES.

The Commission shall require entities that receive disputes regarding the unauthorized use of accounts of such entities from consumers that have reason to believe that they are victims of identity theft to conduct any necessary investigation and decide an outcome of a claim within 90 days from the date on which all necessary information to investigate the claim has been submitted to the entity.

SEC. 204. IMPROVEMENTS TO CONSUMER CLEARINGHOUSE.

The Commission shall utilize the Identity Theft Clearinghouse to permit consumers that have a reasonable

belief that they are victims of identity theft to submit any information relevant to such identity theft to the Clearinghouse (including by means of an Identity Theft Affidavit), so that such information may be transmitted by the Clearinghouse to appropriate entities for necessary protective action and to mitigate losses resulting from such identity theft.

SEC. 205. IMPROVED IDENTITY THEFT DATA.

(a) IN GENERAL.—The Commission shall—

(1) establish a process to contact, not less than annually, public and private entities that receive and process complaints from consumers that have a reasonable belief that they are victims of identity theft; and

(2) obtain accurate data on the incidences and nature of complaints from such entities.

(b) INCLUSION IN DATABASE.—Such information shall be made part of the Commission's Identity Theft Clearinghouse database.

SEC. 206. CHANGE OF ADDRESS PROTECTIONS.

The Commission shall require appropriate entities to take reasonable steps to verify the accuracy of a consumer's address, including by confirming a consumer's change of address by sending a confirmation of such change to the old and the new address of the consumer.

SEC. 207. EFFECTIVE DATE.

This title shall take effect 180 days after the date of enactment of this Act.

TITLE III—INTERNATIONAL PROVISIONS

SEC. 301. STUDY BY COMPTROLLER GENERAL.

The Comptroller General of the United States shall conduct a study and issue a report analyzing the impact on the interstate and foreign commerce of the United States of information privacy laws, regulations, or agreements enacted, promulgated, or adopted by other nations, including regional or international agreements between nations, and whether the enforcement mechanisms or procedures of those laws, regulations, or agreements result in discriminatory treatment of United States entities. The first report under this section shall be issued not later than 120 days after the date of enactment of this Act and subsequent reports shall be issued every 3 years thereafter.

SEC. 302. REMEDIATION OF DISCRIMINATORY IMPACT BY SECRETARY OF COMMERCE.

If the Comptroller General of the United States finds, in the study and report under section 301, that such information privacy laws, regulations, or agreements substantially impede interstate and foreign commerce of the United States and that the enforcement mechanisms or

procedures of the information privacy laws, regulations, or agreements described in such subsection result in discriminatory treatment of United States entities, the Secretary of Commerce shall, to the extent permitted by law take all steps necessary to mitigate against such discriminatory impact within 180 days after the report making such findings is issued.

SEC. 303. EFFECT OF NONREMEDIATION.

(a) RECOMMENDATIONS.—If by the end of the 180-day period described in section 302, the Secretary of Commerce has not attained complete relief from the discriminatory impact described in such subsection, the Secretary shall report to the Congress and the President recommendations on action to relieve any such remaining discriminatory impact.

(b) FEDERAL AGENCY ACTION AFTER CONSIDERATION BY CONGRESS.—During the period after the Secretary reports recommendations under subsection (a) for mitigation of discriminatory impact and before the Congress acts with respect to such recommendations, no officer or employee of any Federal agency may take or continue any action to enjoin, or impose any penalty on, a United States entity, or a citizen or legal resident of the United States, for the purpose of fulfilling an international obligation of the United States under an international pri-

vacy agreement (other than such an obligation under a ratified treaty) that resulted in such discriminatory impact.

SEC. 304. HARMONIZATION OF INTERNATIONAL PRIVACY LAWS, REGULATIONS, AND AGREEMENTS.

Beginning on the date of enactment of this Act, the Secretary of Commerce shall provide notice of the provisions of this Act to other nations, individually, or as members of international organizations or unions that have enacted, promulgated, or adopted information privacy laws, regulations, or agreements, and shall seek recognition of this Act by such nations, organizations, or unions. The Secretary shall seek the harmonization of this Act with such information privacy laws, regulations, or agreements, to the extent such harmonization is necessary for the advancement of transnational commerce, including electronic commerce.

○