109TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 109–454
Part 1

FINANCIAL DATA PROTECTION ACT OF 2006

MAY 4, 2006.—Ordered to be printed

Mr. OXLEY, from the Committee on Financial Services, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 3997]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the bill (H.R. 3997) to amend the Fair Credit Reporting Act to provide for secure financial data, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

49–006

AMENDMENT

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; FINDINGS.

(a) SHORT TITLE.—This Act may be cited as the "Financial Data Protection Act of 2006".

(b) FINDINGS.—The Congress finds as follows:

(1) Protecting the security of sensitive information relating to consumers is important to limiting account fraud and identity theft.

(2) While the Gramm-Leach-Bliley Act requires financial institutions to protect the security and confidentiality of the nonpublic personal information of the customers of financial institutions, the scope of covered entities and type of information needs to be broadened to fully protect consumers.

(3) Some Federal agencies have issued model guidance under the Gramm-Leach-Bliley Act requiring banks to investigate and provide notice to customers of breaches of data security involving customer information that could lead to account fraud or identity theft, but these standards need to broadened to apply to other entities acting as consumer reporters, in order to create a single, uniform data security standard that applies to all parties to transactions involving such financial information.

(4) Requiring all consumer reporters handling sensitive financial personal information to provide notice to consumers of data security breaches that are likely to result in harm or inconvenience will help consumers protect themselves and mitigate against the risk of identity theft or account fraud.

(5) Therefore, all consumer reporters should—

(A) protect sensitive financial personal information;

(B) investigate potential data security breaches;

(C) provide breach notices as appropriate to the United States Secret Service, functional regulators, involved third parties, and consumers;

(D) restore the security of the information and improve safeguards after a breach; and

(E) provide consumers free file monitoring where appropriate to reduce the risk of identity theft.

SEC. 2. DATA SECURITY SAFEGUARDS.

(a) IN GENERAL.—As set forth in section 630 of the Fair Credit Reporting Act, as amended by the Act, in the event a consumer reporter becomes aware of information suggesting a breach of data security, such consumer reporter shall immediately conduct an investigation, and notify authorities and consumers as appropriate.

(b) FCRA DATA SECURITY AMENDMENT.—The Fair Credit Reporting Act (15 U.S.C. 1681) is amended by adding at the end the following new section:

"SEC. 630. DATA SECURITY SAFEGUARDS.

"(a) PROTECTION OF SENSITIVE FINANCIAL PERSONAL INFORMATION.—

"(1) DATA SECURITY OBLIGATION POLICY.—It is the policy of the Congress that each consumer reporter has an affirmative and continuing obligation to protect the security and confidentiality of sensitive financial personal information.

"(2) SECURITY POLICIES AND PROCEDURES.—Each consumer reporter shall have an affirmative obligation to implement, and a continuing obligation to maintain, reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information relating to any consumer that is handled by such consumer reporter against any loss, unauthorized access, or misuse that is reasonably likely to result in harm or inconvenience to such consumer.

"(3) DATA DESTRUCTION AND DATA DISPOSAL POLICIES AND PROCEDURES.—The policies and procedures described in paragraph (2) shall include providing for the proper disposal of sensitive financial personal information in accordance with the standards, guidelines, or regulations issued pursuant to this title.

"(b) INVESTIGATION REQUIREMENTS.—

"(1) INVESTIGATION TRIGGER.—A consumer reporter shall immediately conduct a data security breach investigation if it—

"(A) becomes aware of any information indicating a reasonable likelihood that a data security breach has occurred or is unavoidable;

"(B) becomes aware of information indicating an unusual pattern of misuse of sensitive financial personal information handled by a consumer reporter indicative of financial fraud; or

"(C) receives a notice under subsection (e).

"(2) SCOPE OF INVESTIGATION.—Such investigation shall be conducted in a manner commensurate with the nature and the amount of the sensitive financial personal information that is subject to the breach of data security, including appropriate actions to—

"(A) assess the nature and scope of the potential breach;

"(B) identify the sensitive financial personal information potentially involved;

"(C) determine whether such information is usable by the parties causing the breach; and

"(D) determine the likelihood that such information has been, or will be, misused in a manner that may cause harm or inconvenience to the related consumer.

"(3) ENCRYPTION AND OTHER SAFEGUARDS.—

"(A) SUGGESTED SAFEGUARDS.—The regulators described in subsection (k)(1) shall jointly develop standards and guidelines to identify and regularly update appropriate technology safeguards for making consumer reporter's sensitive financial personal information unusable in a manner commensurate with the nature and the amount of such information, including—

"(i) consideration of the encryption standards adopted by the National Institute of Standards and Technology for use by the Federal Government; and

"(ii) appropriate management and protection of keys or codes necessary to protect the integrity of encrypted information.

"(B) SAFEGUARD FACTORS.—In determining the likelihood of a data security breach, a consumer reporter may consider whether the information subject to the potential breach is unusable because it is encrypted, redacted, requires technology to use that is not generally commercially available, or has otherwise similarly been rendered unreadable.

"(C) SAFE HARBOR FOR PROTECTED DATA.—As set forth in the standards and guidelines issued pursuant to subparagraph (A), a consumer reporter may reasonably conclude that a data security breach is not likely to have occurred where the sensitive personal financial information involved has been encrypted, redacted, requires technology to use that is not generally commercially available, or is otherwise unlikely to be usable

"(D) EXCEPTION.—Subparagraphs (B) and (C) shall not apply if the consumer reporter becomes aware of information that would reasonably indicate that the information that was the subject of the potential breach is usable by the entities causing the breach or potentially misusing the information, for example because—

"(i) an encryption code is potentially compromised,

"(ii) the entities are believed to have the technology to access the information; or

"(iii) there is an unusual pattern of misuse of such information indicative of financial fraud.

"(c) BREACH NOTICES.—If a consumer reporter determines that a breach of data security has occurred, is likely to have occurred, or is unavoidable, the consumer reporter shall in the order listed—

"(1) promptly notify the United States Secret Service;

"(2) promptly notify the appropriate functional regulatory agency for the consumer reporter;

"(3) notify as appropriate and without unreasonable delay—

"(A) any third party entity that owns or is obligated on an affected financial account as set forth in the standards or guidelines pursuant to subsection (k)(1)(G), including in such notification information reasonably identifying the nature and scope of the breach and the sensitive financial personal information involved; and

"(B) any other appropriate critical third parties whose involvement is necessary to investigate the breach; and

"(4) without unreasonable delay notify any affected consumers to the extent required in subsection (f), as well as—

"(A) each nationwide consumer reporting agency, in the case of a breach involving sensitive financial identity information relating to 1,000 or more consumers; and

"(B) any other appropriate critical third parties who will be required to undertake further action with respect to such information to protect such consumers from resulting fraud or identity theft.

"(d) SYSTEM RESTORATION REQUIREMENTS.—If a consumer reporter determines that a breach of data security has occurred, is likely to have occurred, or is unavoidable, the consumer reporter shall take prompt and reasonable measures to—

"(1) repair the breach and restore the security and confidentiality of the sensitive financial personal information involved to limit further unauthorized misuse of such information; and

"(2) restore the integrity of the consumer reporter's data security safeguards and make appropriate improvements to its data security policies and procedures.

"(e) THIRD PARTY DUTIES.—

"(1) COORDINATED INVESTIGATION.—Whenever any consumer reporter that handles sensitive financial personal information for or on behalf of another party becomes aware that an investigation is required under subsection (b) with respect to such information, the consumer reporter shall—

"(A) promptly notify the other party of the breach;

"(B) conduct a coordinated investigation with the other party as described in subsection (b); and

"(C) ensure that the appropriate notices are provided as required under subsection (f).

"(2) CONTRACTUAL OBLIGATION REQUIRED.—No consumer reporter may provide sensitive financial personal information to a third party, unless such third party agrees to fulfill the obligations imposed by subsections (a), (d), and (h), as well as that whenever the third party becomes aware that a breach of data security has occurred, is reasonably likely to have occurred, or is unavoidable, with respect to such information, the third party shall be obligated—

"(A) to provide notice of the potential breach to the consumer reporter;

"(B) to conduct a coordinated investigation with the consumer reporter to identify the sensitive financial personal information involved and determine if the potential breach is reasonably likely to result in harm or inconvenience to any consumer to whom the information relates; and

"(C) provide any notices required under this section, except to the extent that such notices are provided by the consumer reporter in a manner meeting the requirements of this section.

"(f) CONSUMER NOTICE.—

"(1) POTENTIAL IDENTITY THEFT RISK AND FRAUDULENT TRANSACTION RISK.—A consumer reporter shall provide a consumer notice if, at any point the consumer reporter becomes aware—

"(A) that a breach of data security is reasonably likely to have occurred or be unavoidable, with respect to sensitive financial personal information handled by the consumer reporter;

"(B) of information reasonably identifying the nature and scope of the breach; and

"(C) that such information is reasonably likely to have been or to be misused in a manner causing harm or inconvenience against the consumers to whom such information relates to—

"(i) commit identity theft if the information is sensitive financial identity information, or

"(ii) make fraudulent transactions on such consumers' financial accounts if the information is sensitive financial account information.

"(2) SECURITY PROGRAM SAFEGUARDS AND REGULATIONS.—

"(A) STANDARDS FOR SAFEGUARDS.—The regulators described in subsection (k)(1) shall issue guidelines relating to the types of sophisticated neural networks and security programs that are likely to detect fraudulent account activity and at what point detection of such activity is sufficient to avoid consumer notice under this subsection.

"(B) ALTERNATIVE SAFEGUARDS.—In determining the likelihood of misuse of sensitive financial account information and whether a notice is required under paragraph (1), the consumer reporter may additionally consider—

"(i) consistent with any standards promulgated under subparagraph (A), whether any neural networks or security programs used by, or on behalf of, the consumer reporter have detected, or are likely to detect on an ongoing basis over a reasonable period of time, fraudulent transactions resulting from the breach of data security; or

"(ii) whether no harm or inconvenience is reasonably likely to have occurred, because for example the related consumer account has been closed or its number has been changed.

"(3) COORDINATION WITH THE FAIR DEBT COLLECTION PRACTICES ACT.—The provision of a notice to the extent such notice and its contents are required

under this section shall not be considered a communication under the Fair Debt Collection Practices Act.

"(4) COORDINATION OF CONSUMER NOTICE DATABASE.—

"(A) IN GENERAL.—The Commission shall coordinate with the other government entities identified in this section to create a publicly available list of data security breaches that have triggered a notice to consumers under this subsection within the last 12 months.

"(B) LISTED INFORMATION.—The publicly available list described in subparagraph (A) shall include the following:

"(i) The identity of the party responsible that suffered the breach.

"(ii) A general description of the nature and scope of the breach.

"(iii) Any financial fraud mitigation or other services provided by such party to the affected consumers, including the telephone number and other appropriate contact information for accessing such services.

"(g) TIMING, CONTENT, AND MANNER OF NOTICES.—

"(1) DELAY OF NOTICE FOR LAW ENFORCEMENT PURPOSES.—If a consumer reporter receives a written request from an appropriate law enforcement agency indicating that the provision of a notice under subsection (c)(3) or (f) would impede a criminal or civil investigation by that law enforcement agency, or an oral request from an appropriate law enforcement agency indicating that such a written request will be provided within 2 business days—

"(A) the consumer reporter shall delay, or in the case of a foreign law enforcement agency may delay, providing such notice until—

"(i) the law enforcement agency informs the consumer reporter that such notice will no longer impede the investigation; or

"(ii) the law enforcement agency fails to—

"(I) provide within 10 days a written request to continue such delay for a specific time that is approved by a court of competent jurisdiction; or

"(II) in the case of an oral request for a delay, provide a written request within 2 business days, and if such delay is requested for more than 10 additional days, such request must be approved by a court of competent jurisdiction; and

"(B) the consumer reporter may—

"(i) conduct appropriate security measures that are not inconsistent with such request; and

"(ii) contact such law enforcement agency to determine whether any such inconsistency would be created by such measures.

"(2) HOLD HARMLESS PROVISION.—A consumer reporter shall not be liable for any fraud mitigation costs or for any losses that would not have occurred but for notice to or the provision of sensitive financial personal information to law enforcement, or the delay provided for under this subsection, except that—

"(A) nothing in this subparagraph shall be construed as creating any inference with respect to the establishment or existence of any such liability; and

"(B) this subparagraph shall not apply if the costs or losses would not have occurred had the consumer reporter undertaken reasonable system restoration requirements to the extent required under subsection (d), or other similar provision of law, except to the extent that such system restoration was delayed at the request of law enforcement.

"(3) CONTENT OF CONSUMER NOTICE.—Any notice required to be provided by a consumer reporter to a consumer under subsection (f)(1), and any notice required in accordance with subsection (e)(2)(A), shall be provided in a standardized transmission or exclusively colored envelope, and shall include the following in a clear and conspicuous manner:

"(A) An appropriate heading or notice title.

"(B) A description of the nature and types of information and accounts as appropriate that were, or are reasonably believed to have been, subject to the breach of data security.

"(C) A statement identifying the party responsible, if known, that suffered the breach, including an explanation of the relationship of such party to the consumer.

"(D) If known, the date, or the best reasonable approximation of the period of time, on or within which sensitive financial personal information related to the consumer was, or is reasonably believed to have been, subject to a breach.

"(E) A general description of the actions taken by the consumer reporter to restore the security and confidentiality of the breached information.

"(F) A telephone number by which a consumer to whom the breached information relates may call free of charge to obtain additional information about how to respond to the breach.

"(G) With respect to notices involving sensitive financial identity information, a copy of the summary of rights of consumer victims of fraud or identity theft prepared by the Commission under section 609(d), as well as any additional appropriate information on how the consumer may—

"(i) obtain a copy of a consumer report free of charge in accordance with section 612;

"(ii) place a fraud alert in any file relating to the consumer at a consumer reporting agency under section 605A to discourage unauthorized use; and

"(iii) contact the Commission for more detailed information.

"(H) With respect to notices involving sensitive financial identity information, a prominent statement in accordance with subsection (h) that file monitoring will be made available to the consumer free of charge for a period of not less than six months, together with a telephone number for requesting such services, and may also include such additional contact information as a mailing address, e-mail, or Internet website address.

"(I) The approximate date the notice is being issued.

"(4) OTHER TRANSMISSION OF NOTICE.—The notice described in paragraph (3) may be made by other means of transmission (such as electronic or oral) to a consumer only if—

"(A) the consumer has affirmatively consented to such use, has not withdrawn such consent, and with respect to electronic transmissions is provided with the appropriate statements related to such consent as described in section 101(c)(1) of the Electronic Signatures in Global and National Commerce Act; and

"(B) all of the relevant information in paragraph (3) is communicated to such consumer in such transmission.

"(5) DUPLICATIVE NOTICES.—

"(A) IN GENERAL.—A consumer reporter, whether acting directly or in coordination with another entity—

"(i) shall not be required to provide more than 1 notice with respect to any breach of data security to any affected consumer, so long as such notice meets all the applicable requirements of this section, and

"(ii) shall not be required to provide a notice with respect to any consumer if a notice meeting the applicable requirements of this section has already been provided to such consumer by another entity.

"(B) UPDATING NOTICES.—If a consumer notice is provided to consumers pursuant only to subsection (f)(1)(C)(ii) (relating to sensitive financial account information), and the consumer reporter subsequently becomes aware of a reasonable likelihood that sensitive financial personal information involved in the breach is being misused in a manner causing harm or inconvenience against such consumer to commit identity theft, an additional notice shall be provided to such consumers as well any other appropriate parties under this section, including a copy of the Commission's summary of rights and file monitoring mitigation instructions under subparagraphs (G) and (H) of paragraph (3).

"(6) RESPONSIBILITY AND COSTS.—

"(A) IN GENERAL.—Except as otherwise established by written agreement between the consumer reporter and its agents or third party servicers, the entity that suffered a breach of data security shall be—

"(i) primarily responsible for providing any consumer notices and file monitoring required under this section with respect to such breach; and

"(ii) responsible for the reasonable actual costs of any notices provided under this section.

"(B) IDENTIFICATION TO CONSUMERS.—No such agreement shall restrict the ability of a consumer reporter to identify the entity responsible for the breach to consumers

"(C) NO CHARGE TO CONSUMERS.— The cost for the notices and file monitoring described in subparagraph (A) may not be charged to the related consumers.

"(h) FINANCIAL FRAUD MITIGATION.—

"(1) FREE FILE MONITORING.—Any consumer reporter that is required to provide notice to a consumer under subsection (f)(1)(C)(i), or that is deemed to be in compliance with such requirement by operation of subsection (j), if requested by the consumer before the end of the 90-day period beginning on the date of

such notice, shall make available to the consumer, free of charge and for at least a 6-month period—

"(A) a service that monitors nationwide credit activity regarding a consumer from a consumer reporting agency described in section 603(p); or

"(B) a service that provides identity-monitoring to consumers on a nationwide basis that meets the guidelines described in paragraph (2).

"(2) IDENTITY MONITORING NETWORKS.—The regulators described in subsection (k)(1) shall issue guidelines on the type of identity monitoring networks that are likely to detect fraudulent identity activity regarding a consumer on a nationwide basis and would satisfy the requirements of paragraph (1).

"(3) JOINT RULEMAKING FOR SAFE HARBOR.—In accordance with subsection (j), the Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission shall jointly develop standards and guidelines, which shall be issued by all functional regulatory agencies, that, in any case in which—

"(A) free file monitoring is offered under paragraph (1) to a consumer;

"(B) subsequent to the offer, another party misuses sensitive financial identity information on the consumer obtained through the breach of data security (that gave rise to such offer) to commit identity theft against the consumer; and

"(C) at the time of such breach the consumer reporter met the requirements of subsections (a) and (d),

exempts the consumer reporter from any liability for any harm to the consumer resulting from such misuse, other than any direct pecuniary loss or loss pursuant to agreement by the consumer reporter, except that nothing in this paragraph shall be construed as creating any inference with respect to the establishment or existence of any such liability.

"(i) CREDIT SECURITY FREEZE.—

"(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

"(A) SECURITY FREEZE.—The term 'security freeze' means a notice placed in a credit report on a consumer, at the request of the consumer who is a victim of identity theft, that prohibits the consumer reporting agency from releasing all or any part of the credit report, without the express authorization of the consumer, except as otherwise provided in this section.

"(B) REVIEWING THE ACCOUNT; ACCOUNT REVIEW.—The terms 'reviewing the account' and 'account review' include activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

"(2) REQUEST FOR A SECURITY FREEZE.—

"(A) IN GENERAL.—A consumer who has been the victim of identity theft may place a security freeze on the file of such consumer at any consumer reporting agency by—

"(i) making a request in writing by certified mail to the consumer reporting agency;

"(ii) submitting an identity theft report to the consumer reporting agency; and

"(iii) providing such evidence of the identity of the consumer as such consumer reporting agency may require under paragraph (5).

"(B) PROMPT IMPOSITION OF FREEZE.—A consumer reporting agency shall place a security freeze on a credit report on a consumer no later than 5 business days after receiving a written request from the consumer in accordance with subparagraph (A).

"(C) EFFECT OF FREEZE.—

"(i) IN GENERAL.—Except as otherwise provided in this subsection, if a security freeze is in place with respect to any consumer, information from the consumer's credit report may not be released by the consumer reporting agency or reseller to any third party, including another consumer reporting agency or reseller, without the prior express authorization from the consumer or as otherwise permitted in this section.

"(ii) ADVISING OF EXISTENCE OF SECURITY FREEZE.—Clause (i) shall not be construed as preventing a consumer reporting agency or reseller from advising a third party that a security freeze is in effect with respect to the credit report on the consumer.

"(D) CONFIRMATION OF FREEZE; ACCESS CODE.—Any consumer reporting agency that receives a consumer request for a security freeze in accordance with subparagraph (A) shall—

"(i) send a written confirmation of the security freeze to the consumer within 10 business days of placing the freeze; and

"(ii) at the same time, provide the consumer with a unique personal identification number or password (other than the Social Security account number of any consumer) to be used by the consumer when providing authorization for the release of the credit report of the consumer to a specific party or for a specific period of time.

"(3) ACCESS PURSUANT TO CONSUMER AUTHORIZATION DURING SECURITY FREEZE.—

"(A) NOTICE BY CONSUMER.—If the consumer wishes to allow the credit report on the consumer to be accessed by a specific party or for a specific period of time while a freeze is in place, the consumer shall—

"(i) contact the consumer reporting agency in any manner the agency may provide;

"(ii) request that the security freeze be temporarily lifted; and

"(iii) provide—

"(I) proper identification;

"(II) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (2)(D)(ii); and

"(III) the proper information regarding the third party who is to receive the credit report or the time period for which the report shall be available to users of the credit report.

"(B) TIMELY RESPONSE REQUIRED.—A consumer reporting agency that receives a request from a consumer to temporarily lift a security freeze on a credit report in accordance with subparagraph (A) shall comply with the request no later than 3 business days after receiving the request.

"(C) PROCEDURES FOR REQUESTS.—A consumer reporting agency may develop procedures involving the use of telephone, fax, or, upon the consent of the consumer in the manner required by the Electronic Signatures in Global and National Commerce Act for notices legally required to be in writing, by the Internet, e-mail, or other electronic medium to receive and process a request from a consumer to temporarily lift a security freeze on a credit report pursuant to subparagraph (A) in an expedited manner.

"(4) LIFTING OR REMOVING SECURITY FREEZE.—

"(A) IN GENERAL.—A consumer reporting agency may remove or temporarily lift a security freeze placed on a credit report on a consumer only in the following cases:

"(i) Upon receiving a consumer request for a temporary lift of the security freeze in accordance with paragraph (3)(A).

"(ii) Upon receiving a consumer request for the removal of the security freeze in accordance with subparagraph (C).

"(iii) Upon a determination by the consumer reporting agency that the security freeze was imposed on the credit report due to a material misrepresentation of fact by the consumer.

"(B) NOTICE TO CONSUMER OF DETERMINATION.—If a consumer reporting agency makes a determination described in subparagraph (A)(iii) with a respect to a security freeze imposed on the credit report on any consumer, the consumer reporting agency shall notify the consumer of such determination in writing prior to removing the security freeze on such credit report.

"(C) REMOVING SECURITY FREEZE.—

"(i) IN GENERAL.—Except as provided in this subsection, a security freeze shall remain in place until the consumer requests that the security freeze be removed.

"(ii) PROCEDURE FOR REMOVING SECURITY FREEZE.—A consumer reporting agency shall remove a security freeze within 3 business days of receiving a request for removal from the consumer who provides—

"(I) proper identification; and

"(II) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (2)(D)(ii).

"(5) PROPER IDENTIFICATION REQUIRED.—A consumer reporting agency shall require proper identification of any person who makes a request to impose, temporarily lift, or permanently remove a security freeze on the credit report of any consumer under this section.

"(6) THIRD PARTY REQUESTS.—If—

"(A) a third party requests access to a consumer's credit report on which a security freeze is in effect under this section in connection with an application by the consumer for credit or any other use; and

"(B) the consumer does not allow the consumer's credit report to be accessed by that specific party or during the specific period such application is pending,

the third party may treat the application as incomplete.

"(7) CERTAIN ENTITY EXEMPTIONS.—

"(A) AGGREGATORS AND OTHER AGENCIES.—This subsection shall not apply to a consumer reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer reporting agency or multiple consumer reporting agencies, and does not maintain a permanent database of credit information from which new credit reports are produced.

"(B) OTHER EXEMPTED ENTITIES.—The following entities shall not be required to place a security freeze in a credit report:

"(i) An entity which provides check verification or fraud prevention services, including but not limited to, reports on incidents of fraud, verification or authentication of a consumer's identification, or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments.

"(ii) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, automated teller machine abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or other financial institution.

"(8) EXCEPTIONS.—This subsection shall not apply with respect to the use of a consumer credit report by any of the following for the purpose described:

"(A) A person, or any affiliate, agent, or assignee of any person, with whom the consumer has or, prior to an assignment, had an account, contract, or debtor-creditor relationship for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or debt.

"(B) An affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under paragraph (3) for purposes of facilitating the extension of credit or other permissible use of the report in accordance with the consumer's request under such paragraph.

"(C) Any State or local agency, law enforcement agency, trial court, or person acting pursuant to a court order, warrant, or subpoena.

"(D) A Federal, State, or local agency that administers a program for establishing an enforcing child support obligations for the purpose of administering such program.

"(E) A Federal, State, or local health agency, or any agent or assignee of such agency, acting to investigate fraud within the jurisdiction of such agency.

"(F) A Federal, State, or local tax agency, or any agent or assignee of such agency, acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of other statutory responsibility of such agency.

"(G) Any person that intends to use the information in accordance with section 604(c).

"(H) Any person administering a credit file monitoring subscription or similar service to which the consumer has subscribed.

"(I) Any person for the purpose of providing a consumer with a copy of the credit report or credit score of the consumer upon the consumer's request.

"(9) PROHIBITION ON FEE.—A consumer reporting agency may not impose a fee for placing, removing, or removing for a specific party or parties a security freeze on a credit report.

"(10) NOTICE OF RIGHTS.—At any time that a consumer is required to receive a summary of rights required under section 609(c)(1) or 609(d)(1) the following notice shall be included:

"'Consumers Who Are Victims of Identity Theft Have the Right to Obtain a Security Freeze on Your Consumer Report

"'You may obtain a security freeze on your consumer credit report at no charge if you are a victim of identity theft and you submit a copy of an identity theft report you have filed with a law enforcement agency about unlawful use of your personal information by another person.

"'The security freeze will prohibit a credit reporting agency from releasing any information in your consumer credit report without your express authorization. A security freeze must be requested in writing by certified mail.

"'The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gains access to the personal and financial information in your consumer credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transaction, or other services, including an extension of credit at point of sale.

"'When you place a security freeze on your consumer credit report, within 10 business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your consumer credit report or authorize the release of your consumer credit report for a specific party, parties or period of time after the freeze is in place.

"'To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer reporting agency (2) Proper identification to verify your identity (3) The proper information regarding the third party or parties who are trying to receive the consumer credit report or the period of time for which the report shall be available to users of the consumer report.

"'A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a consumer credit report shall comply with the request no later than 3 days after receiving the request.

"'A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity with which you have an existing account that requests information in your consumer credit report for the purposes of reviewing or collecting the account, if you have previously given your consent to this use of your consumer credit report. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account up-grades and enhancements.

"'If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely or temporarily if you are shopping around, or specifically for a certain creditor, a few days before actually applying for new credit.'.

"(j) EFFECT ON GLBA.—

"(1) DEPOSITORY INSTITUTIONS.—The current and any future breach notice regulations and guidelines under section 501(b) of the Gramm-Leach-Bliley Act with respect to depository institutions shall be superseded, as of the effective date of the regulations required under subsection (k)(3)(A), relating to the specific requirements of this section.

"(2) NONDEPOSITORY INSTITUTIONS.—The current and any future data security regulations and guidelines under section 501(b) of the Gramm-Leach-Bliley Act with respect to nondepository institutions shall be superseded as of the effective date of the regulations required under subsection (k)(3)(A), relating to the responsibilities under this section.

"(k) UNIFORM DATA SECURITY SAFEGUARD REGULATIONS.—

"(1) UNIFORM STANDARDS.—The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission shall jointly, and the Federal functional regulatory agencies that have issued guidance on consumer breach notification shall jointly with respect to the entities under their jurisdiction, develop standards and guidelines to implement this section, including—

"(A) prescribing specific standards with respect to subsection (g)(3) setting forth a reasonably unique and, pursuant to paragraph (2)(B), exclusive color and titling of the notice, and standardized formatting of the notice contents described under such subsection to standardize such communications and make them more likely to be reviewed, and understood by, and helpful to consumers, including to the extent possible placing the critical information for consumers in an easily understood and prominent text box at the top of each notice;

"(B) providing in such standards and guidelines that the responsibility of a consumer reporter to provide notice under this section—

"(i) has been satisfied with respect to any particular consumer, even if the consumer reporter is unable to contact the consumer, so long as the consumer reporter has made reasonable efforts to obtain a current

address or other current contact information with respect to such consumer;

"(ii) may be made by public notice in appropriate cases in which—

"(I) such reasonable efforts described in clause (i) have failed; or

"(II) a breach of data security involves a loss or unauthorized acquisition of sensitive financial personal information in paper documents or records that has been determined to be usable, but the identities of specific consumers are not determinable; and

"(iii) with respect to paragraph (3) of subsection (c), may be communicated to entities in addition to those specifically required under such paragraph through any reasonable means, such as through an electronic transmission normally received by all of the consumer reporter's business customers; and

"(C) providing in such standards and guidelines elaboration on how to determine whether a technology is generally commercially available for the purposes of subsection (b), focusing on the availability of such technology to persons who potentially could seek to breach the data security of the consumer reporter, and how to determine whether the information is likely to be usable under subsection (b)(3);

"(D) providing for a reasonable and fair manner of providing required consumer notices where the entity that directly suffered the breach is unavailable to pay for such notices, because for example the entity is bankrupt, outside of the jurisdiction of the United States, or otherwise can not be compelled to provide such notice;

"(E) providing for periodic instead of individual notices to regulators and law enforcement under subsection (c)(1) and (2) where the consumer reporter determines that only a de minimus number of consumers are reasonably likely to be affected;

"(F) providing, to the extent appropriate, notice to the United States Secret Service, a consumer reporter's functional regulator, and the entities described in paragraphs (1) through (3) of subsection (c), whenever the consumer reporter's sensitive financial personal information has been lost or illegally obtained but such loss or acquisition does not result in a breach, for example because the information was sufficiently encrypted or otherwise unusable; and

"(G) establishing what types of accounts might be subject to unauthorized transactions after a breach involving sensitive financial account information, for example because such accounts are open-end credit plans or are described in section 903(2) of the Electronic Fund Transfer Act.

"(2) MODEL NOTICE FORMS.—

"(A) IN GENERAL.—The Secretary of the Treasury, Board of Governors of the Federal Reserve System, and the Commission shall jointly establish and publish model forms and disclosure statements to facilitate compliance with the notice requirements of subsection (g) and to aid the consumer in understanding the information required to be disclosed relating to a breach of data security and the options and services available to the consumer for obtaining additional information, consumer reports, and credit monitoring services.

"(B) USE OPTIONAL.—A consumer reporter may utilize a model notice or any model statement established under this paragraph for purposes of compliance with this section, at the discretion of the consumer reporter.

"(C) EFFECT OF USE.—A consumer reporter that uses a model notice form or disclosure statement established under this paragraph shall be deemed to be in compliance with the requirement to provide the required disclosure to consumers to which the form or statement relates.

"(3) ENFORCEMENT.—

"(A) REGULATIONS.—Each of the functional regulatory agencies shall prescribe such regulations as may be necessary, consistent with the standards in paragraph (1), to ensure compliance with this section with respect to the persons subject to the jurisdiction of such agency under subsection (l).

"(B) MISUSE OF UNIQUE COLOR AND TITLES OF NOTICES.—Any person who uses the unique color and titling adopted under paragraph (1)(A) for notices under subsection (f)(1) in a way that is likely to create a false belief in a consumer that a communication is such a notice shall be liable in the same manner and to the same extent as a debt collector is liable under section 813 for any failure to comply with any provision of the Fair Debt Collection Practices Act.

"(4) PROCEDURES AND DEADLINE.—

"(A) PROCEDURES.—Standards and guidelines issued under this subsection shall be issued in accordance with applicable requirements of title 5, United States Code.

"(B) DEADLINE FOR INITIAL STANDARDS AND GUIDELINES.—The standards and guidelines required to be issued under paragraph (1) shall be published in final form before the end of the 9-month period beginning on the date of the enactment of the Financial Data Protection Act of 2006.

"(C) DEADLINE FOR ENFORCEMENT REGULATIONS.—The standards and guidelines required to be issued under paragraph (2) shall be published in final form before the end of the 6-month period beginning on the date standards and guidelines described in subparagraph (B) are published in final form.

"(D) AUTHORITY TO GRANT EXCEPTIONS.—The regulations prescribed under paragraph (2) may include such additional exceptions to this section as are deemed jointly by the functional regulatory agencies to be consistent with the purposes of this section if such exceptions are necessary because of some unique aspect of the entities regulated or laws governing such entities; and such exemptions are narrowly tailored to protect the purposes of this Act.

"(E) CONSULTATION AND COORDINATION.—The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission shall consult and coordinate with the other functional regulatory agencies to the extent appropriate in prescribing regulations under this subsection.

"(F) FAILURE TO MEET DEADLINE.—Any agency or authority required to publish standards and guidelines or regulations under this subsection that fails to meet the deadline for such publishing shall submit a report to the Congress within 30 days of such deadline describing—

"(i) the reasons for the failure to meet such deadline;

"(ii) when the agency or authority expects to complete the publication required; and

"(iii) the detriment such failure to publish by the required deadline will have on consumers and other affected parties.

"(G) UNIFORM IMPLEMENTATION AND INTERPRETATION.—It is the intention of the Congress that the agencies and authorities described in subsection (l)(1)(G) will implement and interpret their enforcement regulations, including any exceptions provided under subparagraph (D), in a uniform manner.

"(5) APPROPRIATE EXEMPTIONS OR MODIFICATIONS.—The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission, in consultation with the Administrator of the Small Business Administration and the functional regulatory agencies, shall provide appropriate exemptions or modifications from requirements of this section relating to sensitive financial personal information for consumer reporters that do not maintain, service, or communicate a large quantity of such information, taking into account the degree of sensitivity of such information, the likelihood of misuse, and the degree of potential harm or inconvenience to the related consumer.

"(6) COORDINATION.—

"(A) IN GENERAL.—Each functional regulatory agency shall consult and coordinate with each other functional regulatory agency so that, to the extent possible, the regulations prescribed by each agency are consistent and comparable.

"(B) MODEL REGULATIONS.—In prescribing implementing regulations under paragraph (1), the functional regulatory agencies agencies referred to in such paragraph shall use the Gramm-Leach-Bliley Act (including the guidance and regulations issued thereunder) as a base, adding such other consumer protections as appropriate under this section.

"(l) ADMINISTRATIVE ENFORCEMENT.—

"(1) IN GENERAL.—Notwithstanding section 616, 617, or 621, compliance with this section and the regulations prescribed under this section shall be enforced by the functional regulatory agencies with respect to financial institutions and other persons subject to the jurisdiction of each such agency under applicable law, as follows:

"(A) Under section 8 of the Federal Deposit Insurance Act, in the case of—

"(i) national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Comptroller of the Currency;

"(ii) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Fed-

eral branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act, and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Governors of the Federal Reserve System;

"(iii) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Directors of the Federal Deposit Insurance Corporation; and

"(iv) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Director of the Office of Thrift Supervision.

"(B) Under the Federal Credit Union Act, by the Board of the National Credit Union Administration with respect to any federally insured credit union, and any subsidiaries of such an entity.

"(C) Under the Securities Exchange Act of 1934, by the Securities and Exchange Commission with respect to any broker, dealer, or nonbank transfer agent.

"(D) Under the Investment Company Act of 1940, by the Securities and Exchange Commission with respect to investment companies.

"(E) Under the Investment Advisers Act of 1940, by the Securities and Exchange Commission with respect to investment advisers registered with the Commission under such Act.

"(F) Under the provisions of title XIII of the Housing and Community Development Act of 1992, by the Director of the Office of Federal Housing Enterprise Oversight (and any successor to such functional regulatory agency) with respect to the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and any other entity or enterprise or bank (as defined in such title XIII) subject to the jurisdiction of such functional regulatory agency under such title, including any affiliate of any such enterprise.

"(G) Under State insurance law, in the case of any person engaged in the business of insurance, by the applicable State insurance authority of the State in which the person is domiciled.

"(H) Under the Federal Home Loan Bank Act, by the Federal Housing Finance Board (and any successor to such functional regulatory agency) with respect to the Federal home loan banks and any other entity subject to the jurisdiction of such functional regulatory agency, including any affiliate of any such bank.

"(I) Under the Federal Trade Commission Act, by the Commission for any other person that is not subject to the jurisdiction of any agency or authority under subparagraphs (A) through (G) of this subsection, except that for the purposes of this subparagraph a violation of this section shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act regarding unfair or deceptive acts or practices.

"(2) EXERCISE OF CERTAIN POWERS.—For the purpose of the exercise by any agency referred to in paragraph (1) of its powers under any Act referred to in such paragraph, a violation of any requirement imposed under this section shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in paragraph (1), each of the agencies referred to in that paragraph may exercise, for the purpose of enforcing compliance with any requirement imposed under this section, any other authority conferred on it by law.

"(3) USE OF UNDISTRIBUTED FUNDS FOR FINANCIAL EDUCATION.—If—

"(A) in connection with any administrative action under this section, a fund is created or a functional regulatory agency has obtained disgorgement; and

"(B) the functional regulatory agency determines that—

"(i) due to the size of the fund to be distributed, the number of individuals affected, the nature of the underlying violation, or for other reasons, it would be infeasible to distribute such fund or disgorgement to the victims of the violation; or

"(ii) there are excess monies remaining after the distribution of the fund or disgorgement to victims,

the functional regulatory agency may issue an order in an administrative proceeding requiring that the undistributed amount of the fund or disgorgement be used in whole or in part by the functional regulatory agency for education programs and outreach activities of consumer groups, community based groups, and the Financial Literacy and Education Commission established under the Fair and Accurate Credit Transactions Act of 2003 that are consistent with and further the purposes of this title.

"(m) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

"(1) BREACH OF DATA SECURITY.—The term 'breach of data security' or 'data security breach' means any loss, unauthorized acquisition, or misuse of sensitive financial personal information handled by a consumer reporter that could be misused to commit financial fraud (such as identity theft or fraudulent transactions made on financial accounts) in a manner causing harm or inconvenience to a consumer.

"(2) CONSUMER.—The term 'consumer' means an individual.

"(3) CONSUMER REPORTER AND RELATED TERMS.—

"(A) CONSUMER FINANCIAL FILE AND CONSUMER REPORTS.—The term 'consumer financial file and consumer reports' includes any written, oral, or other communication of any information by a consumer reporter bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, personal identifiers, financial account information, or mode of living.

"(B) CONSUMER REPORTER.—The term 'consumer reporter' means any consumer reporting agency or financial institution, or any person which, for monetary fees, dues, on a cooperative nonprofit basis, or otherwise regularly engages in whole or in part in the practice of assembling or evaluating consumer financial file and consumer reports, consumer credit information, or other information on consumers, for the purpose of furnishing consumer reports to third parties or to provide or collect payment for or market products and services, or for employment purposes, and which uses any means or facility of interstate commerce for such purposes.

"(4) FINANCIAL INSTITUTION.—The term 'financial institution' means—

"(A) any person the business of which is engaging in activities that are financial in nature as described in or determined under section 4(k) of the Bank Holding Company Act;

"(B) any person that is primarily engaged in activities that are subject to the Fair Credit Reporting Act; and

"(C) any person that is maintaining, receiving, or communicating sensitive financial personal information on an ongoing basis for the purposes of engaging in interstate commerce.

"(5) FUNCTIONAL REGULATORY AGENCY.—The term 'functional regulatory agency' means any agency described in subsection (l) with respect to the financial institutions and other persons subject to the jurisdiction of such agency.

"(6) HANDLED BY.—The term 'handled by' includes with respect to sensitive financial personal information, any access to or generation, maintenance, servicing, or ownership of such information, as well as any transfer to or allowed access to or similar sharing or servicing of such information by or with a third party on a consumer reporter's behalf.

"(7) NATIONWIDE CONSUMER REPORTING AGENCY.—The term 'nationwide consumer reporting agency' means—

"(A) a consumer reporting agency described in section 603(p);

"(B) any person who notifies the Commission that the person reasonably expects to become a consumer reporting agency described in section 603(p) within a reasonable time; and

"(C) a consumer reporting agency described in section 603(w) that notifies the Commission that the person wishes to receive breach of data security notices under this section that involve information of the type maintained by such agency.

"(8) NEURAL NETWORK.—The term 'neural network' means an information security program that monitors financial account transactions for potential fraud, using historical patterns to analyze and identify suspicious financial account transactions.

"(9) SENSITIVE FINANCIAL ACCOUNT INFORMATION.—The term 'sensitive financial account information' means a financial account number of a consumer, such as a credit card number or debit card number, in combination with any required

security code, access code, biometric code, password, or other personal identification information that would allow access to the financial account.

"(10) SENSITIVE FINANCIAL IDENTITY INFORMATION.—The term 'sensitive financial identity information' means the first and last name, the address, or the telephone number of a consumer, in combination with any of the following of the consumer:

"(A) Social Security number.

"(B) Driver's license number or equivalent State identification number.

"(C) IRS Individual Taxpayer Identification Number.

"(D) IRS Adoption Taxpayer Identification Number.

"(E) The consumer's deoxyribonucleic acid profile or other unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

"(11) SENSITIVE FINANCIAL PERSONAL INFORMATION.—The term 'sensitive financial personal information' means any information that is sensitive financial account information, sensitive financial identity information, or both.

"(12) HARM OR INCONVENIENCE.—The term 'harm or inconvenience', with respect to a consumer, means financial loss to or civil or criminal penalties imposed on the consumer or the need for the consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by consumer reporting agencies, financial institutions, or government entities, in order to avoid the risk of financial loss or increased costs or civil or criminal penalties.

"(n) RELATION TO STATE LAWS.—

"(1) IN GENERAL.—No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any consumer reporter or the functional equivalent of such responsibilities—

"(A) to protect the security or confidentiality of information on consumers maintained by or on behalf of the person;

"(B) to safeguard such information from potential misuse;

"(C) to investigate or provide notices of any unauthorized access to information concerning the consumer, or the potential misuse of such information, for fraudulent purposes;

"(D) to mitigate any loss or harm resulting from such unauthorized access or misuse; or

"(E) involving restricting credit reports from being provided, or imposing any requirement on such provision, for a permissible purpose pursuant to section 604, such as—

"(i) the responsibilities of a consumer reporting agency to honor a request, or withdrawal of such a request, to prohibit the consumer reporting agency from releasing any type of information from the file of a consumer;

"(ii) the process by which such a request or withdrawal of such a request is made, honored, or denied;

"(iii) any notice that is required to be provided to the consumer in connection with such a request or withdrawal of such a request; or

"(iv) the ability of a consumer reporting agency to update or change information in a consumer's file as a result of such a request or withdrawal of such a request; or

"(v) the responsibilities of third parties if information from a consumer's file is unavailable as a result of such a request.

"(2) EXCEPTION FOR CERTAIN STATE LAWS.—Paragraph (1) shall not apply with respect to—

"(A) State laws governing professional confidentiality; or

"(B) State privacy laws limiting the purposes for which information may be disclosed.

"(3) EXCEPTION FOR CERTAIN COVERED ENTITIES.—Paragraph (1) shall not apply with respect to the entities described in subsection (l)(1)(G) to the extent that such entities are acting in accordance with subsection (k)(4)(G) in a manner that is consistent with this section and the implementation of this section by the regulators described in subsection (k)(1).".

(b) CLERICAL AMENDMENT.—The table of sections for the Fair Credit Reporting Act is amended by inserting after the item relating to section 629 the following new item:

"630. Data security safeguards.".

(c) EFFECTIVE DATE.—The provisions of section 630 of the Fair Credit Reporting Act (as added by this section), other than subsection (k) of such section, shall take effect on the date of publication of the regulations required under paragraph (3) of

such subsection, with respect to any person under the jurisdiction of each regulatory agency publishing such regulations.

SEC. 3. NATIONAL SUMMIT ON DATA SECURITY.

Not later than April 30, 2008, the President or the designee of the President shall convene a National Summit on Data Security Safeguards for Sensitive Personal Financial Information in the District of Columbia.

SEC. 4. GAO STUDY.

(a) STUDY REQUIRED.—The Comptroller General shall conduct a study to determine a system that would provide notices of data breaches to consumers in languages other than English and identify what barriers currently exist to the implementation of such a system.

(b) REPORT.—The Comptroller General shall submit a report to the Congress before the end of the 1-year period beginning on the date of the enactment of this Act containing the findings and conclusion of the study under subsection (a) and such recommendations for legislative and administrative action as the Comptroller General may determine to be appropriate.

SEC. 5. ENHANCED DATA COLLECTION ON DATA SECURITY BREACHES AND ACCOUNT FRAUD.

In order to improve law enforcement efforts relating to data security breaches and fighting identity theft and account fraud, the Federal Trade Commission shall compile information on the race and ethnicity of consumers, as defined and volunteered by the consumers, who are victims of identity theft, account fraud, and other types of financial fraud. The Commission shall consult with the various international, national, State, and local law enforcement officers and agencies who work with such victims for the purpose of enlisting the cooperation of such officers and agencies in the compilation of such information. Notwithstanding any other provision of law, such compilation of information shall be made available exclusively to the Commission and law enforcement entities.

SEC. 6. CLARIFICATION RELATING TO CREDIT MONITORING SERVICES.

(a) IN GENERAL.—Section 403 of the Credit Repair Organizations Act (15 U.S.C. 1679a) is amended—

(1) by striking "For purposes of this title" and inserting "(a) IN GENERAL.—For purposes of this title"; and

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

"(b) CLARIFICATION WITH RESPECT TO CERTAIN CREDIT MONITORING SERVICES UNDER CERTAIN CIRCUMSTANCES.—

"(1) IN GENERAL.—Subject to paragraph (2)—

"(A) the provision of, or provision of access to, credit reports, credit monitoring notifications, credit scores and scoring algorithms, and other credit score-related tools to a consumer (including generation of projections and forecasts of such consumer's potential credit scores under various prospective trends or hypothetical or alternative scenarios);

"(B) any analysis, evaluation, and explanation of such actual or hypothetical credit scores, or any similar projections, forecasts, analyses, evaluations or explanations; or

"(C) in conjunction with offering any of the services described in subparagraph (A) or (B), the provision of materials or services to assist a consumer who is a victim of identity theft,

shall not be treated as activities described in clause (i) of subsection (a)(3)(A).

"(2) CONDITIONS FOR APPLICATION OF PARAGRAPH (1).—Paragraph (1) shall apply with respect to any person engaging in any activity described in such paragraph only if—

"(A) the person does not represent, expressly or by implication, that such person—

"(i) will or can modify or remove, or assist the consumer in modifying or removing, adverse information that is accurate and not obsolete in the consumer's credit report; or

"(ii) will or can alter, or assist the consumer in altering, the consumer's identification to prevent the display of the consumer's credit record, history, or rating for the purpose of concealing adverse information that is accurate and not obsolete;

"(B) in any case in which the person represents, expressly or by implication, that it will or can modify or remove, or assist the consumer in modifying or removing, any information in the consumer's credit report, except for a representation with respect to any requirement imposed on the person under section 611 or 623(b) of the Fair Credit Reporting Act, the person discloses, clearly and conspicuously, before the consumer pays or agrees to pay

any money or other valuable consideration to such person, whichever occurs first, the following statement:

"'NOTICE: Neither you nor anyone else has the right to have accurate and current information removed from your credit report. If information in your report is inaccurate, you have the right to dispute it by contacting the credit bureau directly.';

"(C) the person provides the consumer in writing with the following statement before any contract or agreement between the consumer and the person is executed:

"'Your Rights Concerning Your Consumer Credit File

"'You have a right to obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies. To request your free annual credit report, you may go to www.annualcreditreport.com, or call 877–322–8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348–5281. You can obtain additional copies of your credit report from a credit bureau, for which you may be charged a reasonable fee. There is no fee, however, if you have been turned down for credit, employment, insurance, or a rental dwelling because of information in your credit report within the preceding 60 days. The credit bureau must provide someone to help you interpret the information in your credit file. You are entitled to receive a free copy of your credit report if you are unemployed and intend to apply for employment in the next 60 days, if you are a recipient of public welfare assistance, or if you have reason to believe that there is inaccurate information in your credit report due to fraud.

"'You have the right to cancel your contract with a credit monitoring service without fee or penalty at any time, and in the case in which you have prepaid for a credit monitoring service, you are entitled to a pro rata refund for the remaining term of the credit monitoring service.

"'The Federal Trade Commission regulates credit bureaus and credit monitoring services. For more information contact:

"'Federal Trade Commission

"'Washington, D.C. 20580

"'1–877–FTC-HELP

"'www.ftc.gov.'; and

"(D) in any case in which the person offers a subscription to a credit file monitoring program to a consumer, the consumer may cancel the subscription at any time upon written notice to the person without penalty or fee for such cancellation and, in any case in which the consumer is billed for the subscription on other than a monthly basis, within 60 days of receipt of the consumer's notice of cancellation, the person shall make a pro rata refund to the consumer of a subscription fee prepaid by the consumer, calculated from the date that the person receives the consumer's notice of cancellation until the end of the subscription period.".

(b) CLARIFICATION OF NONEXEMPT STATUS.—Section 403(a) of the Credit Repair Organizations Act (15 U.S.C. 1679a) (as so redesignated by subsection (a) of this section) is amended, in paragraph (3)(B)(i), by inserting "and is not for its own profit or for that of its members" before the semicolon at the end.

(c) REVISION OF DISCLOSURE REQUIREMENT.—Section 405(a) of the Credit Repair Organizations Act (15 U.S.C. 1679c) is amended by striking everything after the heading of the disclosure statement contained in such section and inserting the following new text of the disclosure statement:

"'You have a right to dispute inaccurate information in your credit report by contacting the credit bureau directly. However, neither you nor any "credit repair" company or credit repair organization has the right to have accurate, current, and verifiable information removed from your credit report. The credit bureau must remove accurate, negative information from your report only if it is over 7 years old. Bankruptcy information can be reported for 10 years.

"'You have a right to obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies. To request your free annual credit report, you may go to www.annualcreditreport.com, or call 877–322–8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348–5281. You can obtain additional copies of your credit report from a credit bureau, for which you may be charged a reasonable fee. There is no fee, however, if you have been turned down for credit, employment, insurance, or a rental dwelling because of information in your credit report within the preceding 60 days. The credit bureau must provide someone to help you interpret the infor-

mation in your credit file. You are entitled to receive a free copy of your credit report if you are unemployed and intend to apply for employment in the next 60 days, if you are a recipient of public welfare assistance, or if you have reason to believe that there is inaccurate information in your credit report due to fraud.

"'You have a right to sue a credit repair organization that violates the Credit Repair Organization Act. This law prohibits deceptive practices by credit repair organizations.

"'You have the right to cancel your contract with any credit repair organization for any reason within 3 business days from the date you signed it.

"'Credit bureaus are required to follow reasonable procedures to ensure that the information they report is accurate. However, mistakes may occur.

"'You may, on your own, notify a credit bureau in writing that you dispute the accuracy of information in your credit file. The credit bureau must then reinvestigate and modify or remove inaccurate or incomplete information. The credit bureau may not charge any fee for this service. Any pertinent information and copies of all documents you have concerning an error should be given to the credit bureau.

"'If the credit bureau's reinvestigation does not resolve the dispute to your satisfaction, you may send a brief statement to the credit bureau, to be kept in your file, explaining why you think the record is inaccurate. The credit bureau must include a summary of your statement about disputed information with any report it issues about you.

"'The Federal Trade Commission regulates credit bureaus and credit repair organizations. For more information contact:

"'Federal Trade Commission
"'Washington, D.C. 20580
"'1–877–FTC-HELP
"'(877 382–4357)
"'www.ftc.gov.'".

PURPOSE AND SUMMARY

H.R. 3997, the Financial Data Protection Act, would expand the data safeguards requirements of the Fair Credit Reporting Act (FCRA) and build off the implementation of safeguard and consumer notice provisions from the Gramm-Leach-Bliley Act (GLBA) to establish uniform standards for all consumer reporters that possess or maintain sensitive financial account or identity information about consumers.

This bill establishes the policy that consumer reporters have to protect the security and confidentiality of sensitive financial personal information. All consumer reporters are required to maintain reasonable policies and procedures to protect the security and confidentiality of their sensitive financial personal information relating to any consumer. Should a consumer reporter believe a breach has occurred, or is likely to occur, they are required to immediately investigate. If the potential breach of data security may result in harm or inconvenience to any consumer, then the consumer reporter is required to notify the U.S. Secret Service, appropriate regulator(s), and other consumer reporters in the transaction chain. If the potential breach may result in financial fraud against consumers causing harm or inconvenience, then the consumers must be notified through a uniform mailing. Consumer notification involving sensitive financial identity information must include an offer of free credit file monitoring for the consumer. Consumers who are victims of identity theft are also provided with the right to place a security freeze on their credit report.

BACKGROUND AND NEED FOR LEGISLATION

In 2005, there were more than 100 data security breaches involving sensitive information relating to over 50 million consumers. As of March 5, 2006, another 29 breaches had been reported. The growing incidence of data security breaches, the potential impact of these breaches on consumers and the previous focus of Federal data security requirements on specific types of information and specific types of entities has required the Committee to look closely at ways to broaden Federal regulation of sensitive financial personal information in a manner that provides stronger and more comprehensive uniform consumer protections.

In determining the appropriate Congressional response, the Committee has conducted numerous hearings and independent investigations to identify the nature of the problem, the potential risks to consumers and the appropriate remedies. During a typical business transaction, various marketplace participants routinely process sensitive financial personal information relating to consumers. For example, in a typical credit card transaction, a retailer, merchant bank, third-party processors, card association and issuing bank will handle identifying information relating to the cardholder. Data brokers compile information on individuals from a variety of public sources to assist consumer reporters in fraud prevention, marketing and other purposes. A data security breach involving sensitive financial personal information at any of these or other entities risks enabling data thieves seeking to engage in financial identity theft or account fraud.

It is also apparent that different levels of risk to consumers are presented by different types of data security breaches. For example, despite the high-profile media coverage attendant to certain recent breaches, many breaches do not result in any incidence of financial fraud or harm to consumers. In February 2005, Bank of America announced that four backup computer data tapes containing personal information relating to over one million Federal Government employees had been lost in shipping. Nonetheless, the data tapes were unmarked and required software to read that is not generally available, and there is no public evidence to date that any of the information has been misused. ID Analytics, an identity risk management company, studied the level of misuse of identity information relating to approximately 500,000 consumers that was involved in four breaches in 2005. The Company found that the highest rate for fraudulent misuse among the four breaches was 0.098 percent—fewer than one in 1,000 identities. This study and other evidence clearly illustrates that while a number of breaches have occurred, the actual harm to consumers has been relatively low. This has been a factor of breach circumstances (for example, the information is on unreadable software), as well as related to procedures and protections currently in place by the majority of financial institutions. For example, financial institutions use sophisticated internal and third-party identity verification and fraud detection systems to prevent misuse of personal data that can lead to identity theft and other financial fraud.

The Federal response to date to the potential harms in this area has been targeted to a limited subset of financial institutions. The Federal banking agencies, based upon general directives contained

in the 1999 passage of GLBA, have issued broad guidance for banks regarding mandatory internal data security programs, investigation standards for potential breaches and regulatory and consumer breach notification requirements that are predicated on the level of probable consumer harm involved. The Committee generally believes that this has resulted in the establishment of a strong Federal regulatory scheme for banking institutions that adequately protects consumers. Moreover, it provides the Committee with an appropriate working model that may be applied more broadly to additional types of financial information and to other consumer reporters covered under this bill.

The Committee has also based its legislation on the protections for covered information in the FCRA. For example, in 2003 the Committee amended the FCRA in the Fair and Accurate Credit Transactions Act (the FACT Act) to further govern the communication of various identifying information between consumer reporting agencies and retailers and other 3rd party users of such financial information, as well as from consumer reporters to various law enforcement agencies. The FACT Act also gave consumers new rights to block the reporting of fraudulent information to consumer reporting agencies and to require new duties on users and furnishers of consumer reports to ensure the integrity of the consumer reporting system.

Unfortunately, however, the Committee determined that the directives in GLBA and FCRA to the regulators to ensure the integrity of data security and the consumer reporting system have not been sufficient as implemented in their scope of coverage to prevent the misuse of sensitive financial personal information. For example, until recently, header information from consumer reporting agencies consisting of identifying information such as name, address, social security number, and sometimes mother's maiden name, was being extensively used and sold for marketing purposes in noncompliance with GLBA. In 2002, the United States Court of Appeals for the District of Columbia Circuit rejected arguments by a consumer reporting agency that it was not a "financial institution" subject to the Federal Trade Commission's (FTC) rulemaking authority under the GLBA, and that the regulations' definition of the term "personally identifiable financial information" was overly broad (295 F.2d 42). But according to the FTC in testimony before the Subcommittee on Financial Institutions and Consumer Credit, there are continued concerns about the aggregation of sensitive consumer information and whether this information is protected adequately from misuse to commit financial fraud. Gaps remain or continue to be challenged both with respect to the types of consumer reporters and the types of financial information subject to the various Federal laws. In addition, implementation of Federal safeguard laws by some of the Federal and State regulators has been inadequate. For example, many Federal and State regulators have not yet issued extensive data safeguard and consumer breach notice requirements, and the regulated entities and sensitive information covered are inconsistent.

A particular factor in the Committee's deliberations has been the lack of uniformity in the varied approaches that the state legislatures have taken to data breach regulation. As of the Committee's markup of H.R. 3997, more than twenty states have enacted dif-

ferent, and often-conflicting, data breach laws, with over a hundred additional bills pending. Some of these state initiatives recognize and work in concert with GLBA and FCRA mandates; however, many include requirements that are inconsistent with existing Federal mandates as well as the various mandates of other states. Doing so provides consumers with different levels of protection based solely on where they live, while imposing inconsistent and costly burdens on consumer reporters attempting to comply with this patchwork-quilt of regulation. The Committee believes that the existing regulatory approach makes little sense, and in taking action, has sought to establish a uniform approach to regulation in this area that recognizes the "national" nature of the U.S. economy and the need to establish consistent rules in the marketplace. This ensures that all consumers, regardless of where they live, receive necessary protections from the risks associated with identity theft while promoting efficient nationwide regulation.

An example of the different approaches to state regulation can be seen in the area of consumer notice, and the appropriate circumstances under which notice would be triggered. Some states, for example, have mandated notices where certain consumer information has been subject to unauthorized access, regardless of the level of risk of identity theft that may be present. However, several government agencies have raised concerns about the adverse impact of providing consumers with notice with respect to every such breach. For example, both the FTC and the Office of the Comptroller of the Currency (OCC) have testified before Congress that companies should have to provide prompt notice only when there is actually a significant risk to consumers, since otherwise, consumers would not appreciate and understand when there was a need to act. Unnecessary notification is also costly and time consuming to consumer reporters and an undue burden when there is no benefit, and possibly a negative impact, for the consumer. In fact, the FTC warned that providing consumers with notice in response to every breach, regardless of the likelihood of harm, would lead to consumers becoming "numb to them and failing to spot or act on those risks that truly are significant." [1]

Most existing consumer data breach State notice laws also fail to distinguish between sensitive financial identity information and sensitive financial account information. America's Community Bankers testified before the Committee about the need to differentiate between the two types of financial information and formulate a different remedy distinguishing the differing risks to consumers between identity theft and account fraud. Mrs. Josie Callari elaborated, "for consumers there is a distinct difference between the two risks. Transaction fraud poses minimal risk to consumers because they have no liability for fraudulent credit or debit card transactions, and regulations specify standards for speedy resolution. Transaction fraud generally creates only a temporary inconvenience. However, identity theft can be much more harmful for consumers, and they must take concrete steps to prevent identity theft as quickly as possible if they are at risk. [A] dual notice

[1] Testimony of the Honorable Deborah Majoras, Chairman, Federal Trade Commission, before the Senate Committee on Commerce, Science and Transportation. June 16, 2005.

recognize[s] these differences and provides consumers with the appropriate information to address the risk." [2]

Congress has passed laws establishing data security requirements for specific types of information (health insurance records) and for certain industry sectors (banks), but has not yet established comprehensive data security requirements that apply uniformly to all consumer reporters for all sensitive financial personal information relating to consumers that could be used to commit financial fraud. Several of the most high profile data security breaches last year involved large data brokers that compile files from financial companies on millions of consumers, but who are not subject to current Federal data security breach notification requirements. While many of these businesses assist law-enforcement efforts and create a more efficient and reliable financial services marketplace, most of the witnesses at the Committee's data security hearings expressed concerns about the lack of a uniform national standard governing such services. For this reason, H.R. 3997 seeks to end the challenges over which consumer reporters in the information chain are required to safeguard and notify consumers about breaches in sensitive financial personal information and apply similar data security standards across all entities, rather than to restrict or further regulate the use of such information which is vital as a tool in the fight against identity theft and financial fraud.

HEARINGS

The Subcommittee on Financial Institutions and Consumer Credit held a hearing on November 9, 2005, on H.R. 3997, the "Financial Data Protection Act of 2005." The following witnesses testified:

Mr. Oliver I. Ireland, Partner, Morrison & Foerster LLP, representing the Financial Services Coordinating Council;

Mrs. Josie Callari, Senior Vice President, Astoria Federal S&L Association and Chairman, America's Community Bankers Electronic Banking and Payment Systems Committee, representing America's Community Bankers;

Mr. H. Randy Lively, President & CEO, representing the American Financial Services Association;

Mr. Mark Bohannon, General Counsel and Senior Vice President Public Policy, representing the Software and Information Industry Association;

Ms. Julie Brill, Assistant Attorney General, State of Vermont;

Mr. Evan Hendricks, Publisher, Privacy Times;

Mr. Karl F. Kaufmann, Sidley Austin Brown & Wood LLP, representing the Chamber of Commerce; ARMA International (submitted for the record);

ID Analytics Corporation (submitted for the record);

Mortgage Bankers Association (submitted for the record);

National Association of Insurance Commissioners (submitted for the record);

[2] Testimony of Mrs. Josie Callari, Senior Vice President, Astoria Federal S&L Association and Chairman, America's Community Bankers Electronic Banking and Payment Systems Committee, on behalf of America's Community Bankers, before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit. November 9, 2005.

National Business Coalition on E-Commerce & Privacy (submitted for the record).

The Subcommittee on Oversight and Investigations held a hearing on July 21, 2005, on "Credit Card Data Processing: How Secure Is It?" The following witnesses testified:

Mr. Joshua L. Peirez, Senior Vice President & Associate General Counsel, Law Department, representing MasterCard International;

Mr. Steve Ruwe, Executive Vice President, Operations & Risk Management, representing Visa U.S.A. Inc.;

Mr. Zyg Gorgol, Senior Vice President, Fraud Risk Management, representing American Express;

Mr. Carlos Minetti, Executive Vice President, Cardmember Services, representing Discover Card;

Mr. David B. Watson, Chairman, representing Merrick Bank;

Mr. Mallory Duncan, General Counsel, representing the National Retail Federation;

Mr. John M. Perry, President and Chief Executive Office, representing CardSystems Solutions, Inc.

The Subcommittee on Financial Institutions and Consumer Credit on May 18, 2005, on "Enhancing Data Security: The Regulators' Perspective." The following witnesses testified:

Ms. Lydia B. Parnes, Director, Bureau of Consumer Protection, representing the Federal Trade Commission;

Ms. Sandra Thompson, Deputy Director, Division of Supervision and Consumer Protection, representing the Federal Deposit Insurance Corporation;

Mr. Robert M. Fenner, General Counsel, representing the National Credit Union Administration.

The Full Committee on Financial Services held a hearing on May 4, 2005, on "Assessing Data Security: Preventing Breaches and Protecting Sensitive Information." The following witnesses testified:

Ms. Barbara Desoer, Global Technology, Service & Fulfillment Executive, representing Bank of America;

Mr. Eugene Foley, President & CEO, representing Harvard University Employees Credit Union;

Mr. Don McGuffey, Senior Vice President for Data Acquisition and Strategy, representing ChoicePoint;

Mr. Kurt P. Sanford, President & CEO, U.S. Corporate & Federal Government Markets, representing LexisNexis;

Mr. Bestor Ward, President, representing Safe Archives-Safe Shredding, LLC.

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on March 15 and 16, 2006, and ordered H.R. 3997, the Financial Data Protection Act, reported to the House with an amendment by a record vote of 48 yeas and 17 nays.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. A motion by Mr.

Oxley to report the bill, with an amendment, to the House with a favorable recommendation was agreed to a record vote of 48 yeas and 17 nays (Record vote No. FC–17). The names of Members voting for and against follow:

RECORD VOTE NO. FC–17

Representative	Aye	Nay	Present	Representative	Aye	Nay	Present
Mr. Oxley	X			Mr. Frank (MA)		X	
Mr. Leach	X			Mr. Kanjorski	X		
Mr. Baker	X			Ms. Waters		X	
Ms. Pryce (OH)	X			Mr. Sanders		X	
Mr. Bachus	X			Mrs. Maloney		X	
Mr. Castle	X			Mr. Gutierrez		X	
Mr. Royce	X			Ms. Velázquez			
Mr. Lucas	X			Mr. Watt		X	
Mr. Ney	X			Mr. Ackerman		X	
Mrs. Kelly	X			Ms. Hooley	X		
Mr. Paul		X		Ms. Carson		X	
Mr. Gillmor	X			Mr. Sherman	X		
Mr. Ryun (KS)	X			Mr. Meeks (NY)			
Mr. LaTourette	X			Ms. Lee		X	
Mr. Manzullo	X			Mr. Moore (KS)	X		
Mr. Jones (NC)				Mr. Capuano		X	
Mrs. Biggert	X			Mr. Ford		X	
Mr. Shays	X			Mr. Hinojosa		X	
Mr. Fossella	X			Mr. Crowley	X		
Mr. Gary G. Miller (CA)	X			Mr. Clay		X	
Mr. Tiberi	X			Mr. Israel	X		
Mr. Kennedy (MN)				Mrs. McCarthy	X		
Mr. Feeney	X			Mr. Baca	X		
Mr. Hensarling	X			Mr. Matheson	X		
Mr. Garrett (NJ)	X			Mr. Lynch		X	
Ms. Brown-Waite (FL)	X			Mr. Miller (NC)		X	
Mr. Barrett (SC)	X			Mr. Scott (GA)	X		
Ms. Harris	X			Mr. Davis (AL)	X		
Mr. Renzi	X			Mr. Al Green (TX)		X	
Mr. Gerlach				Mr. Cleaver	X		
Mr. Pearce	X			Ms. Bean	X		
Mr. Neugebauer	X			Ms. Wasserman Schultz	X		
Mr. Price (GA)	X			Ms. Moore (WI)	X		
Mr. Fitzpatrick (PA)	X						
Mr. Davis (KY)	X						
Mr. McHenry	X						
Mr. Campbell	X						

*Mr. Sanders is an independent, but caucuses with the Democratic Caucus.

The following amendments were decided by record votes. The names of Members voting for and against follow:

An amendment to the amendment in the nature of a substitute by Mr. Gutierrez, No. 1a, relating to state action for violations was not agreed to by a record vote of 23 yeas and 40 nays (Record vote No. FC–15).

RECORD VOTE NO. FC–15

Representative	Aye	Nay	Present	Representative	Aye	Nay	Present
Mr. Oxley		X		Mr. Frank (MA)	X		
Mr. Leach	X			Mr. Kanjorski	X		
Mr. Baker		X		Ms. Waters	X		
Ms. Pryce (OH)		X		Mr. Sanders	X		
Mr. Bachus		X		Mrs. Maloney	X		
Mr. Castle		X		Mr. Gutierrez	X		
Mr. Royce		X		Ms. Velázquez			
Mr. Lucas		X		Mr. Watt	X		

RECORD VOTE NO. FC–15—Continued

Representative	Aye	Nay	Present	Representative	Aye	Nay	Present
Mr. Ney		X		Mr. Ackerman	X		
Mrs. Kelly	X			Ms. Hooley		X	
Mr. Paul				Ms. Carson	X		
Mr. Gillmor		X		Mr. Sherman	X		
Mr. Ryun (KS)		X		Mr. Meeks (NY)	X		
Mr. LaTourette		X		Ms. Lee	X		
Mr. Manzullo		X		Mr. Moore (KS)		X	
Mr. Jones (NC)		X		Mr. Capuano	X		
Mrs. Biggert		X		Mr. Ford		X	
Mr. Shays		X		Mr. Hinojosa			
Mr. Fossella		X		Mr. Crowley		X	
Mr. Gary G. Miller (CA)		X		Mr. Clay		X	
Mr. Tiberi		X		Mr. Israel	X		
Mr. Kennedy (MN)				Mrs. McCarthy	X		
Mr. Feeney		X		Mr. Baca			
Mr. Hensarling		X		Mr. Matheson		X	
Mr. Garrett (NJ)		X		Mr. Lynch	X		
Ms. Brown-Waite (FL)		X		Mr. Miller (NC)	X		
Mr. Barrett (SC)		X		Mr. Scott (GA)		X	
Ms. Harris		X		Mr. Davis (AL)	X		
Mr. Renzi		X		Mr. Al Green (TX)	X		
Mr. Gerlach		X		Mr. Cleaver			
Mr. Pearce		X		Ms. Bean		X	
Mr. Neugebauer				Ms. Wasserman Schultz	X		
Mr. Price (GA)		X		Ms. Moore (WI)	X		
Mr. Fitzpatrick (PA)		X					
Mr. Davis (KY)		X					
Mr. McHenry		X					
Mr. Campbell		X					

*Mr. Sanders is an independent, but caucuses with the Democratic Caucus.

An amendment to the amendment in the nature of a substitute by Mr. Frank, No. 1h, relating to a rule of construction was not agreed to by a record vote of 26 yeas and 35 nays (Record vote No. FC–16).

RECORD VOTE NO. FC–16

Representative	Aye	Nay	Present	Representative	Aye	Nay	Present
Mr. Oxley		X		Mr. Frank (MA)	X		
Mr. Leach		X		Mr. Kanjorski		X	
Mr. Baker		X		Ms. Waters	X		
Ms. Pryce (OH)		X		Mr. Sanders	X		
Mr. Bachus		X		Mrs. Maloney	X		
Mr. Castle		X		Mr. Gutierrez	X		
Mr. Royce				Ms. Velázquez	X		
Mr. Lucas		X		Mr. Watt	X		
Mr. Ney		X		Mr. Ackerman	X		
Mrs. Kelly		X		Ms. Hooley		X	
Mr. Paul				Ms. Carson	X		
Mr. Gillmor				Mr. Sherman	X		
Mr. Ryun (KS)		X		Mr. Meeks (NY)			
Mr. LaTourette		X		Ms. Lee	X		
Mr. Manzullo		X		Mr. Moore (KS)		X	
Mr. Jones (NC)				Mr. Capuano	X		
Mrs. Biggert		X		Mr. Ford	X		
Mr. Shays	X			Mr. Hinojosa	X		
Mr. Fossella		X		Mr. Crowley	X		
Mr. Gary G. Miller (CA)		X		Mr. Clay	X		
Mr. Tiberi		X		Mr. Israel		X	
Mr. Kennedy (MN)				Mrs. McCarthy	X		
Mr. Feeney				Mr. Baca	X		
Mr. Hensarling		X		Mr. Matheson		X	

RECORD VOTE NO. FC–16—Continued

Representative	Aye	Nay	Present	Representative	Aye	Nay	Present
Mr. Garrett (NJ)		X		Mr. Lynch			
Ms. Brown-Waite (FL)		X		Mr. Miller (NC)	X		
Mr. Barrett (SC)		X		Mr. Scott (GA)	X		
Ms. Harris		X		Mr. Davis (AL)	X		
Mr. Renzi		X		Mr. Al Green (TX)	X		
Mr. Gerlach				Mr. Cleaver	X		
Mr. Pearce		X		Ms. Bean		X	
Mr. Neugebauer		X		Ms. Wasserman Schultz	X		
Mr. Price (GA)		X		Ms. Moore (WI)	X		
Mr. Fitzpatrick (PA)		X					
Mr. Davis (KY)		X					
Mr. McHenry		X					
Mr. Campbell		X					

*Mr. Sanders is an independent, but caucuses with the Democratic Caucus.

The following other amendments were also considered by the Committee:

An amendment in the nature of a substitute offered by Mr. Castle, No. 1, making various substantive and technical changes, was agreed to, as amended, by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Mr. LaTourette, No. 1b, making miscellaneous improvements in the manager's amendment, was agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Mr. Hinojosa, No. 1c, regarding protection of consumer identity, was withdrawn.

An amendment to the amendment in the nature of a substitute offered by Mr. Baca, No. 1d, improving Latino access to credit reports, was withdrawn.

An amendment to the amendment in the nature of a substitute offered by Mr. Hinojosa, No. 1e, requiring a GAO study, was agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Ms. Lee, No. 1f, regarding public availability of data breach information, was withdrawn.

An amendment to the amendment in the nature of a substitute offered by Mrs. Maloney, No. 1g, providing protection of data through a security freeze, was not agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Mr. Frank, No. 1i, establishing jurisdiction of the Federal functional regulatory agencies, was not agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Ms. Waters, No. 1j, relation to state laws, was not agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Mr. Capuano, No. 1k, establishing reimbursement for costs, was withdrawn.

An amendment to the amendment in the nature of a substitute offered by Mr. Frank, No. 1l, regarding preemption, was not agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Ms. Lee, No. 1m, providing for coordination of consumer notice databases, was agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Mr. Baca, No. 1n, improving consumer complaint information collected by the FTC in the Sentinel Program, was agreed to by a voice vote.

An amendment to the amendment in the nature of a substitute offered by Mr. Ackerman, No. 1o, regarding address changes, was withdrawn.

An amendment to the amendment in the nature of a substitute offered by Mr. Price, No. 1p, enforcement clarification, was withdrawn.

An amendment to the amendment in the nature of a substitute offered by Mr. Royce, No. 1q, providing for clarification to credit monitoring services, was agreed to by a voice vote.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held a hearing and made findings that are reflected in this report.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee establishes the following performance related goals and objectives for this legislation:

H.R. 3997, the Financial Data Protection Act, would expand the data safeguards requirements of the Fair Credit Reporting Act (FCRA) and build off the implementation of safeguard and consumer notice provisions from the Gramm-Leach-Bliley Act (GLBA) to establish uniform standards for all consumer reporters that possess or maintain sensitive financial account or identity information about consumers.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 30, 2006.

Hon. MICHAEL G. OXLEY,
Chairman, Committee on Financial Services,
House of Representatives, Washington DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3997, the Financial Data Protection Act of 2006.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Melissa Z. Petersen.

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 3997—Financial Data Protection Act of 2006

Summary: H.R. 3997 would require private companies with access to consumers' personal information to take certain precautions to safeguard that information. Private companies also would be required to notify consumers and certain authorities whenever there is a breach in the security of a consumer's personal information and to investigate and take steps to repair the breach. Under the bill, consumers would have the option of freezing their credit reports in the event of a threat to the security of their personal information. H.R. 3997 would require the Federal Trade Commission (FTC) and other federal regulatory agencies to enforce the restrictions and requirements in the bill and to issue regulations related to the security of consumers' personal information.

Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 3997 would cost less than $500,000 in 2006 and a total of $5 million over the 2006–2011 period. Enacting the bill would not have a significant impact on direct spending or revenues.

H.R. 3997 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA); but CBO estimates that the aggregate cost of complying with those mandates would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

H.R. 3997 would impose private-sector mandates, as defined in UMRA, on financial institutions, employers, consumer credit-reporting agencies and other entities that engage in assembling or evaluating consumer financial information using any means or facility of interstate commerce. While CBO cannot determine the total direct costs of complying with each mandate, the security standards and notification requirements in H.R. 3997 would impose compliance costs on a large number of private-sector entities. Based on this information, CBO estimates that the aggregate direct cost of mandates in the bill, could exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Estimated Cost to the Federal Government: The estimated budgetary impact of H.R. 3997 is shown in the following table. The costs

of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION [1]						
Estimated Authorization Level	*	1	1	1	1	1
Estimated Outlays	*	1	1	1	1	1

[1] Enacting H.R. 3997 would also have small effects on direct spending and revenues, but those effects would be less than $500,000 a year.

Note.—* = less than $500,000.

Basis of estimate: CBO estimates that implementing H.R. 3997 would cost less than $500,000 in 2006 and about $5 million over the 2006–2011 period to issue regulations and enforce the bill's new provisions regarding the security of consumers' personal information. For this estimate, CBO assumes that the bill will be enacted before the end of 2006, that the estimated amounts will be appropriated for each year, and that outlays will follow historical spending patterns. Enacting the legislation would not have a significant effect on direct spending or revenues.

Spending subject to appropriation

H.R. 3997 would require that private companies take certain steps to safeguard consumers' personal information. Private companies also would be required to investigate and remedy security breaches and to notify consumers and certain authorities in the event of a breach. Under the bill, consumers would have the option to freeze their credit reports in the event of a threat to the security of their personal information. The Federal Trade Commission, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), the Office of Federal Housing Enterprise Oversight (OFHEO), and the Federal Housing Finance Board (FHFB) would enforce the restrictions and requirements under the bill and create regulations related to the security of consumers' personal information.

Based on information provided the FTC, CBO estimates that implementing H.R. 3997 would cost less than $500,000 in 2006 and $5 million over the 2006–2011 period for FTC to develop and issue regulations and to enforce the bill's provisions related to information security. Those costs would be subject to the availability of appropriated funds. CBO estimates that implementing the bill would not have a significant impact on spending subject to appropriation for the other regulatory agencies.

Direct spending and revenues

Enacting H.R. 3997 would affect direct spending and revenues because of provisions affecting financial regulatory agencies and civil penalties. CBO estimates that any such effects would not be significant.

H.R. 3997 would require several financial regulatory agencies to enforce the regulations on the security of consumers' personal information as they apply to financial institutions: OCC, FDIC, the

Federal Reserve, the NCUA, and OTS. Any additional direct spending by NCUA, OCC, and OTS to implement the bill would have no net budgetary impact because those agencies charge annual fees to cover all of their administrative expenses. In contrast, the FDIC's sources of income—primarily intragovernmental interest earnings and insurance premiums—do not change in tandem with in its annual expenditures; as a result, any added costs would increase direct spending unless and until the FDIC raised insurance premiums to offset those expenses. Budgetary effects on the Federal Reserve are recorded as changes in revenues (governmental receipts).

According to FDIC officials, enacting H.R. 3997 would not have a significant effect on their workload or budgets. For this estimate, CBO assumes that the FDIC would not assess additional premiums to cover the small costs associated with implementing this bill. Thus, CBO estimates that enacting this bill would increase direct spending and offsetting receipts of the NCUA, OTS, OCC, and FDIC by less than $500,000 a year. Based on information from the Federal Reserve, CBO estimates that enacting H.R. 3997 would reduce revenues by less than $500,000 a year.

Enacting H.R. 3997 could increase Federal revenues as a result of the collection of additional civil penalties assessed for violation of laws related to information security. Collections of civil penalties are recorded in the budget as revenues. CBO estimates, however, that any additional revenues that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved.

Estimated impact on State, local, and tribal governments: H.R. 3997 contains intergovernmental mandates as defined in UMRA because it would require state entities that regulate insurance to enforce certain administrative rules and would explicitly preempt laws in about 20 states that regulate the protection and use of certain personal data. Based on conversations with state and local governments and a review of current legal precedents, CBO assumes that intergovernmental entities would not be required to comply with new data security and notification requirements contained in the bill. CBO estimates, therefore, that the aggregate cost to intergovernmental entities of complying with the mandates in the bill would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

Estimated impact on the private sector: H.R. 3997 would impose private-sector mandates, as defined in UMRA, on financial institutions, employers, consumer credit-reporting agencies, and other entities that engage in assembling or evaluating consumer financial information using any means or facility of interstate commerce. Each entity would be required to protect "sensitive financial personal information" relating to any consumer against unauthorized access that is reasonably likely to result in harm or inconvenience and to provide notice to consumers of data security breaches. The legislation defines sensitive financial personal information as a combination of sensitive financial identity information (name, address, or phone number with Social Security number, driver's license number, or other personal identification information), or sen-

sitive financial account information (financial account number with information allowing access to the account), or both.

In addition, the bill would require the Secretary of the Treasury, the Federal Reserve System, the Federal Trade Commission, and certain other federal regulatory agencies to jointly develop standards and guidelines to implement data security safeguards. Because those standards and regulations have not been issued, CBO cannot determine the total direct costs of complying with those mandates, however, mandates in H.R. 3997 would impose compliance costs on a large number of private-sector entities. Based on this information, CBO estimates that the aggregate direct cost of the mandates could exceed the annual threshold established by UMBRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Protection of sensitive financial personal information

Section 2 would require certain private companies to implement and maintain reasonable measures to protect the security and confidentiality of sensitive financial personal information, including the proper disposal of such information. Such companies would include consumer reporting agencies, financial institutions, businesses, employers, and other entities that assemble or evaluate sensitive financial personal information using any means or facility of interstate commerce. The cost of this mandate would depend on both the number of covered entities and the average cost to an entity of complying with the mandates. According to industry sources, generally all consumer reporting entities have some measure of security in place. But because standards and regulations have not been issued, CBO does not have enough information to determine the incremental cost for such entities to comply with the mandate.

Notification of security breach

Section 2 also would require certain private entities to comply with certain procedures for notifying the Secret Service, regulatory agencies, affected third parties, and consumers if a security breach involving sensitive financial personal information has occurred, is likely to have occurred, or is unavoidable. In addition, the bill would require consumer reporters to:

- Investigate any suspected breach of security;
- Notify credit reporting agencies if the breach affects 1,000 or more consumers;
- Take prompt and reasonable measures to repair a breach of security and restore the integrity of the security safeguards; and
- Delay the release of any security breach notification if requested by law enforcement.

If an entity becomes aware that a security breach is reasonably likely to have occurred or is unavoidable, they would be required to provide a specific notification to any affected consumer. Any entity required to provide such notification also would be required to offer affected consumers free credit-file monitoring and identity-monitoring services for at least six months.

The cost of this mandate depends on the number of security breaches that occur, the average number of persons affected by a breach, and the cost per person for notification and credit-file moni-

toring. According to several industry sources, over 100 security breaches involving sensitive information occurred in 2005, but generally only the largest of breaches are noticed and recorded. Nevertheless, available information suggests that security breaches are not rare. Although the cost to notify individuals and other entities in the event of a security breach may be small per person, the potentially large number of people in data systems maintained by some private companies would make the cost of notification and monitoring associated with one breach significant. Furthermore, certain companies do not maintain the mailing addresses of customers for whom they have name and credit card information. It would be costly for those entities to begin keeping that information. While the regulations regarding consumer notification have not been issued, CBO expects that the cost imposed on consumer reporting entities by the notification requirements could be large relative to the annual threshold established by UMRA for private-sector mandates.

Credit report security freeze

Section 2 also would allow consumers who have been the victim of identity theft to place a security freeze on their credit report by making a request to a consumer credit-reporting agency. The consumer reporting agency would be prevented from releasing the credit report to any third parties without a prior express authorization from the consumer. The agency also would be required to send a written confirmation of the security freeze to the consumer within 10 business days and provide a unique personal identification number of password to be used to authorize the release of any reports. According to industry sources, the major credit-reporting agencies currently provide a security freeze for consumers and have the systems and procedures in place to accept, impose, and release freezes on credit reports. Therefore, CBO expects that the incremental cost to comply with this mandate would be minimal.

Previous CBO estimates: On November 3, 2005, CBO transmitted a cost estimate for S. 1408, the Identify Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005. On March 10, 2006, CBO transmitted a cost estimate for S. 1326, the Notification of Risk to Personal Data Act, as reported by the Senate Committee on the Judiciary on October 20, 2005. H.R. 3997, S. 1408, and S. 1326 would require private companies to take certain precautions to safeguard the personal information of consumers. S. 1326 contains similar requirements for government agencies. S. 1408 would specifically authorize the appropriation of $5 million over the 2006–2010 period for the FTC to enforce the restrictions and requirements under that bill, while H.R. 3997 would not specifically authorize appropriations for the FTC. However, based on information provided by the FTC, we estimate that spending subject to appropriation would be similar under H.R. 3997 and S. 1408. Because S. 1326 also would require government agencies to comply with provisions related to data security, we estimate that spending subject to appropriation would be higher under S. 1326 as compared to the other bills. None of the bills would have a significant impact on direct spending or revenues.

S. 1408 would impose private-sector mandates on certain private entities and consumer credit-reporting agencies that acquire, maintain, or utilize sensitive personal information. S. 1326 would impose private-sector mandates on certain private entities that own or license computerized data containing sensitive personal information. S. 1408 also includes a provision to allow consumers to place a security freeze on their credit report. Since the bills would impose security standards and notification requirements on a large number of private-sector entities, CBO estimated that the total direct cost of mandates in those bills would exceed the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Estimate prepared by: Federal Costs: Melissa Z. Petersen and Kathleen Gramp. Impact on State, Local, and Tribal Governments: Sarah Puro. Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional Authority of Congress to enact this legislation is provided by Article 1, section 8, clause 1 (relating to the general welfare of the United States) and clause 3 (relating to the power to regulate interstate commerce).

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title; findings

This section sets forth the short title of this legislation—the "Financial Data Protection Act of 2006." This section also provides the findings of Congress regarding why a uniform Federal data security safeguard law is necessary and what consumer reporters are supposed to do when handling sensitive financial personal information. Specifically in this section, Congress finds that better data security safeguards are necessary to protect consumer from account fraud and identity theft. Congress believes that there is a need to extend data security safeguards, breach investigation and breach notification requirements, similar to those required by the Federal

banking agencies under the Gramm-Leach-Bliley Act (GLBA), to all other entities that act as consumer reporters and handle sensitive financial personal information. It is the intent of the Committee that the functional regulatory agencies should use these GLBA requirements as a base model when issuing implementing standards and guidelines and enforcement regulations.

In this section Congress further finds that to establish appropriate data security safeguards, consumer reporters handling sensitive financial personal information should protect the information, investigate potential breaches of the information, provide breach notices as appropriate to the U.S. Secret Service and the consumer reporter's functional regulator, provide breach notice to consumers to help them protect themselves against financial identity theft and account fraud where the breach is reasonably likely to result in harm or inconvenience, to restore information security and safeguards after a breach, and provide free file monitoring to consumers for breaches involving theft of sensitive financial identity information to help them limit the risk of identity theft.

Section 2. Data security safeguards

This section amends the Fair Credit Reporting Act (FCRA) by adding a new section 630 with its own unique definitions and enforcement scheme. This section amends the FCRA to require consumer reporters to: (1) protect sensitive financial personal information relating to consumers; (2) investigate data security breaches; (3) notify regulators, law enforcement and other third parties of certain breaches; (4) notify consumers if sensitive financial personal information involved in a breach is reasonably likely to be misused to commit financial fraud causing the consumers harm or inconvenience; and provide free file monitoring to consumers for breaches involving theft of sensitive financial identity information to help them limit the risk of identity theft. A specific description of section 630 is set forth below.

FCRA Section 630(a). Protection of sensitive financial personal information

This subsection states that it is the policy of Congress that each consumer reporter has an affirmative obligation to protect the security and confidentiality of sensitive personal financial information handled by the consumer reporter.

This subsection also provides that a consumer reporter has an affirmative obligation to implement, and a continuing obligation to maintain, reasonable policies and procedures to protect sensitive financial personal information handled by the consumer reporter from loss, unauthorized access or misuse that would be reasonably likely to result in harm or inconvenience to the consumers to whom the information relates.

The Committee recognizes the data security vulnerabilities can result from improper disposal of sensitive financial personal information, including but not limited to Social Security and drivers license numbers as well as bank account and credit card numbers. Identity theft violations, as well as the number of ways these unlawful acts are carried out, are increasing in number. Common identity theft approaches are often committed by extracting information from used computers or by so-called "dumpster divers" who

uncover and misuse sensitive documents after they have been discarded. There have been reported incidents of thousands of files containing sensitive individual information being discarded in a dumpster or left behind office buildings for trash pick up. H.R. 3997 would require covered entities to properly dispose of sensitive financial personal information after its useful life. The Committee expects the regulators should take all necessary steps to spell out the disposal and destruction procedures consumer reporters are to follow, taking into account the nature of the media on which the information is maintained, and to closely monitor the implementation by consumer reporters. The functional regulatory agencies should also ensure that any standards, guidelines or regulations implementing this disposal requirement are in accordance section 628 of the FCRA governing disposal of records.

FCRA Section 630(b). Investigation requirements

This subsection requires a consumer reporter to immediately conduct an investigation if it becomes aware of any information indicating a reasonable likelihood that a data security breach has occurred or is unavoidable. This provision is not intended to require a consumer reporter to investigate a data security breach that occurs at an unrelated third party, even if the breach involves information with the same content as information handled by the consumer reporter. For example, a credit union would not be required to investigate a data security breach involving sensitive financial account information relating to financial account provided by the credit union if the breach occurred at a merchant that was not providing services or otherwise handling the information on behalf of the credit union. The merchant, however, would be required to conduct an investigation and fulfill the obligations of this section.

In addition, this subsection requires a consumer reporter to immediately conduct an investigation if it becomes aware of unusual patterns of misuse of sensitive financial personal information (such as an analytic report evidencing a pattern of fraud that suggests a potential breach). An immediate investigation would also be required if the consumer reporter receives a breach notification by a third party handling sensitive financial personal information for or on behalf of the consumer reporter.

The scope of the investigation required under this subsection will depend on the nature and amount of the information involved in the breach. The consumer reporter must assess the nature and scope of the potential breach and identify the sensitive financial personal information that may have been involved in the breach. Then the consumer reporter must determine if such information is usable by the parties that caused the breach to commit identity theft or to make fraudulent transactions, and the likelihood that the information has been or will be misused in a manner that may cause harm or inconvenience to the affected consumers.

This subsection requires the Secretary of the Treasury (Treasury), the Board of Governors of the Federal Reserve System (Board), and the Federal Trade Commission (FTC), and the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA), to jointly develop standards and guidelines to identify appropriate

technology safeguards that, if used, will allow a consumer reporter to conclude that sensitive financial personal information is unusable.

These standards and guidelines are entirely voluntary, and serve only as a non-exclusive safe harbor under the legislation. Failure to adhere to the standards and guidelines is not evidence that sensitive financial personal information is usable. This subsection specifies that consumer reporters may use safeguarding technology that is not specifically identified by the regulators to render sensitive information unusable (in some cases that may be even more advanced), and may factor the use of these safeguards into determining whether the information is unusable and thus whether a breach has occurred.

Use of the safeguards identified by the regulators, however, creates a presumption allowing a consumer reporter to affirmatively conclude that a breach has not occurred absent evidence reasonably indicating that the information was in fact usable. Specifically, in determining whether a data security breach has occurred, a consumer reporter would be permitted to rely on these standards in determining whether the information involved in the breach was unusable because it was encrypted, redacted, required technology to use that is not generally commercially available or was otherwise rendered unreadable. However, a consumer reporter would not be permitted to rely on this safe harbor if an encryption code has been compromised, the entities that caused the potential breach have the technology necessary to access the information or there is an unusual pattern of misuse that is indicative of financial fraud.

The appropriate level of encryption will vary with the nature and amount of the information. Consumer reporters with relatively small amounts of sensitive financial personal information are not required to use the same level of safeguard as consumer reporters with large quantities of information or databases of such information that present a more target rich environment for financial fraudsters.

In developing and updating these standards and guidelines, the regulators must consider the encryption standards adopted by the National Institute of Standards and Technology (NIST) for use by the Federal Government. The regulators must also consider the appropriate management and protection of encryption keys and codes so that the safeguards used to prevent the information from being usable would not be compromised.

FCRA Section 630(c). Breach notices

This subsection requires a consumer reporter to notify specified third parties of certain data security breaches, and provides the order in which these parties must be notified. Specifically, if a consumer reporter conducts an investigation pursuant to subsection (b) and determines that a data security breach has occurred, is likely to have occurred or is unavoidable, the consumer reporter would be required first to promptly notify the U.S. Secret Service. The consumer reporter would then be required to promptly notify its functional regulatory agency. Next, if applicable, the consumer reporter would be required to notify without unreasonable delay, but not in any particular order: (1) any third party that owns or is obligated

on a financial account to which sensitive financial account information involved in the breach relates; and (2) any other appropriate third parties whose involvement is critical and necessary to investigate the breach.

Notification to the U.S. Secret Service is required first in order to allow law enforcement the opportunity to request a delay in the other notices in order to further an important criminal or civil investigation related to a breach. This may be critical in order to avoid tipping off the involved fraudsters that a breach has been discovered, allowing law enforcement working with the U.S. Secret Service to monitor the affected information systems or breached information to detect continued illegal activity.

After the other breach notifications have been completed, if a breach notice is required to the affected consumers under subsection (f), those notices must be provided without unreasonable delay. In addition, if breach notices are being provided to consumers, notices must also be provided to the nationwide consumer reporting agencies (if the breach involves sensitive financial identity information relating to at least 1,000 consumers) and to appropriate critical third parties who will be required to take further action with respect to the information involved in the breach to protect the consumers from account fraud or identity theft. This latter group would include, for example, entities that may need to close or adjust the safeguards with respect to the information or financial accounts involved in a breach.

The Committee expects the consumer and additional third party notices to be provided in an order most appropriate to the circumstances. In many instances notice should be provided to the nationwide consumer reporting agencies before consumers in order to allow the nationwide consumer reporting agencies to take appropriate measures to respond to consumer calls. These investigation and notice priority provisions are intended to establish a mechanism for quickly informing important law and enforcement and other credit system actors. However, the Committee does not intend consumer reporters to be able to use these provisions to create an unreasonable delay in notifying consumers.

FCRA Section 630(d). System restoration requirements

This subsection requires a consumer reporter to conduct specified system restoration activities. Specifically, if a consumer reporter conducts an investigation pursuant to subsection (b) and determines that a data security breach has occurred, is likely to have occurred or is unavoidable, the consumer reporter would be required to take reasonable measures to repair the breach and restore the security and confidentiality of the sensitive financial personal information involved in the breach in order to limit unauthorized misuse of such information. In addition, the consumer reporter would be required to restore the integrity of the affected data security safeguards and make improvements to its data security policies and procedures required under subsection (a).

FCRA Section 630(e). Third party duties

This subsection imposes specified requirements on a consumer reporter that handles sensitive financial personal information for, or on behalf of, another party. If such a consumer reporter deter-

mines that an investigation would be required under subsection (b) with respect to sensitive financial personal information that the consumer reporter handles for, or on behalf of, another party, the consumer reporter would be required to promptly notify the other party of the potential breach. In addition, the consumer reporter would be required to conduct a coordinated investigation with the other party and to ensure that appropriate notices are provided to consumers if required under subsection (f).

The Committee does not intend a coordinated investigation to mean joint involvement in all parts of a breach investigation (which would be particularly inappropriate in cases involving potential malfeasance by one of the parties). Rather, it may not be possible for either party to fully investigate a potential breach without the cooperation of both entities, so both parties must coordinate their efforts as necessary to ensure an appropriate investigation and notice. The requirement to ensure consumer notices are provided does not override the primary responsibility of the breached entity to provide consumer notices as provided in subsection (g)(6) nor does it affect the ability to contractually agree who provides and bears the costs of such notices. Rather, the requirement provides a fallback responsibility if the notice duty is contractually shifted to another party and the other party does not fulfill its noticing obligation (for example the other party is outside of the jurisdiction of the United States and refuses to provide the required notices).

This subsection also prohibits a consumer reporter from providing sensitive financial personal information to a third party unless the third party agrees to comply with specified requirements of section 630 where it is handling the information on the consumer reporter's behalf, including the information safeguard requirements in subsection (a). In addition, a consumer reporter is prohibited from providing sensitive financial personal information to a third party unless the third party agrees to fulfill the third party obligations of this section. The provision in this paragraph is not intended to create a duplicative or additional requirement on the duties of a consumer reporter regarding a breach, but rather is intended to ensure that consumer reporters do not provide sensitive financial personal information to other entities that may not be covered as consumer reporters under this section or that are outside of the jurisdiction of the United States unless those entities agree to abide by the pertinent provisions of this section safeguarding the covered information.

FCRA Section 630(f). Consumer notice

This subsection establishes a risk-based notification standard that requires a consumer reporter to provide notice to consumers of certain data security breaches where the consumer should take proactive steps to avoid being the victim of account fraud or identity theft, such as steps to avoid fraudulent charges to the consumer's account or to protect his or her credit history. Specifically, a consumer reporter is required to provide notice to consumers if the consumer reporter: (1) determines that a data security breach is reasonably likely to have occurred or is unavoidable with respect to sensitive financial personal information handled by the consumer reporter; (2) becomes aware of information reasonably iden-

tifying the nature and scope of the breach; and (3) determines that the sensitive information involved in the breach is reasonably likely to have been or to be misused in a manner causing harm or inconvenience to the consumers to whom the information relates to commit identity theft (with respect to sensitive financial identity information) or to make fraudulent transactions on the financial accounts of consumers (in the case of sensitive financial account information).

This risk-based notification standard is intended to ensure that consumers receive security breach notifications where the consumers need to take steps to protect themselves from harm resulting from identity theft or account fraud. This provision is not intended to require a consumer reporter to provide notice to consumers of a data security breach that occurs at an unrelated third party.

This subsection requires the Treasury, Board, FTC, OCC, OTS, FDIC, and NCUA to issue guidelines concerning the types of neural networks and security programs that are likely to detect fraudulent account activity. A consumer reporter would be permitted to rely on its neural network pursuant to these guidelines to conclude that notice to consumers is not required where no fraud is detected or fraud can be prevented by such security programs or no harm or inconvenience is likely to occur. Specifically, in determining whether notice would be required to consumers with respect to a breach involving sensitive financial account information, a consumer reporter would be permitted to consider whether any neural network or security program that is used by, or on behalf of, the consumer reporter would be likely to detect fraudulent transactions resulting from the breach.

As with the encryption standard discussed above, this security program safeguard provision is a non-exclusive safe harbor intended solely for purposes of this legislation. Use of a neural network that differs from the guidelines is not evidence that the neural network does not provide the intended protections, unless precluded by or similarly inconsistent with the guidelines. In fact, the Committee is aware that neural networks are likely to evolve faster or differently than the agencies' guidance. In addition, a consumer reporter would be permitted to consider whether no harm or inconvenience is reasonably likely to have occurred because of alternative safeguard steps taken by the consumer reporter. For example, if a consumer reporter suffers a data security breach with respect to sensitive financial account information, but the related account is closed or has its number or access code changed, notice to consumers would not be required because the consumer reporter could conclude that no harm or inconvenience is reasonably likely to occur.

This subsection provides that a notice that is provided to a consumer of a data security breach is not to be considered a communication under the Fair Debt Collection Practices Act or otherwise an attempt to collect a debt, but only to the extent that the notice pertains to the issues regulated under this section. If a consumer reporter were to include additional content in a notice, for example, demanding repayment of a debt, then this exception would not apply.

This subsection directs the FTC to work with the other regulators and entities described in this section to create a publicly available list of data security breaches that have triggered a notice to consumers within the last twelve months. The publicly available list shall include (to the extent described in the notices or as further summarized by the regulators and entities to improve usefulness): the identity of the party responsible, a general description of the nature and scope of the breach, and any financial fraud mitigation or other services provided by the party responsible (including a telephone number and other appropriate contact information to obtain the mitigation services). The list is intended by the Committee to provide another means for consumers to determine if their information is breached and how to respond appropriately. The Committee further intends that, in implementing this consumer notice database requirement, the FTC should attempt to provide publicly available information on each breach within a reasonable time frame to help protect consumers, and to make the list available at minimum on the FTC's website with links to appropriate information for consumers on preventing identity theft and account fraud and the rights of consumers under the FCRA and other applicable law. If during the 12 month listing for a data security breach, the party responsible provides updated information on any financial fraud mitigation or other such services available to consumers, the Committee intends the FTC to correspondingly update its publicly available listing for the breach to the extent possible.

FCRA Section 630(g). Timing, content, and manner of notices

This subsection governs the timing, content, and manner of breach of security notices required to be provided under subsection (f). A consumer reporter is required to delay providing notice of a data security breach to consumers and certain third parties upon a written request (or oral request indicating that a written request will be provided within two business days) made by a domestic law enforcement agency indicating that notice would impede a criminal or civil investigation. A consumer reporter only may delay providing such notice until the law enforcement agency indicates that notice will no longer impede the investigation. If the law enforcement agency has made only an oral request and fails to follow-up with a written request within two business days, then the consumer reporter must go forward with providing the consumer notice. If the agency provides a written request, breach notice to the consumer must be provided after 10 more days, unless a law enforcement agency provides an additional written request to continue a delay that is approved by a legal court with jurisdiction over the request. A consumer reporter receiving a court approved delay request must abide by the terms of the request for the period specified.

During any delay requested by a law enforcement agency, the consumer reporter may take security measures that are consistent with the law enforcement request, such as system restoration efforts described in subsection (d) that do not interfere with the agency's investigation or are otherwise inconsistent with the delay request. To the extent it is unclear what system restoration activities would be inconsistent with a delay request, the consumer re-

porter may contact the agency for further clarification and act accordingly.

A consumer reporter generally will not be liable for any fraud mitigation costs or any losses that would not have occurred but for the provision of notice to law enforcement, provision of sensitive financial personal information to law enforcement, or delay of notice upon the request of law enforcement. An exception to this safe harbor is when a consumer reporter is required to undertake system restoration requirements under subsection (d), does not perform reasonable system restoration actions in compliance with subsection (d), and was not asked to delay system restoration by a law enforcement agency—in which case the safe harbor shall not apply with respect to costs or losses that would not have occurred had such system restoration been completed as required. However, these provisions should not be read to create an inference that any liability otherwise would exist. This subsection is not intended to create any inference that any right of action in court exists under state or federal law.

Additionally, this subsection requires a consumer reporter to provide notice to consumers of a data security breach in a standardized and exclusively colored envelope (that may not be used for any other purposes) to help consumers recognize these notices. If the notice is provided by electronic means (such as email) in compliance with this section, then the transmission still must be a special standardized transmission to alert consumers to the importance of the notice.

This subsection also requires that consumer breach notices include certain information in a clear and conspicuous manner, in order to make them helpful to consumers and more likely to be reviewed and understood. The most critical information must additionally be put in an easily understood and prominent text box at the top of each notice to highlight for the consumer the most important items to be aware of. The information that must be included in the notice include in a standardized format: an appropriate heading or notice title; a description of the nature and type of information that was subject to the breach; an identification of the party suffering the breach (if known), including an explanation of the relationship of the party to the consumer (for example, if the breached party is a third party processor for a credit card issuer that issues a private label credit card for a retailer, the notice must identify the processor that had the breach, that the processor handles information for the particular credit card issuer holding the consumer's account, that the credit card issuer issues the private label credit card that carries the names of the retailer and that is used by the consumer, and the name of the retailer); if known, the date, or a reasonable approximation of the range of dates when the breach may have occurred; a general description of the actions taken by the consumer reporter to restore the security and confidentiality of the information involved in the breach; a telephone number that the consumer can call free of charge to obtain additional information concerning the breach and how to respond (additional contact information may also be included); and the approximate date that the notice is being issued.

If a data security breach involves sensitive financial identity information, the notice to the affected consumers must also include

the summary of rights of identity theft victims prepared by the FTC and, as appropriate, additional information on how the consumer can obtain a free copy of a consumer report, place a fraud alert on any consumer file relating to the consumer (as provided under section 605A to prevent identity theft), and contact the FTC for more detailed information on the consumer's rights and options. The Committee recognizes that some of this information may be contained in and provided through the inclusion of the copy of the FTC's summary of rights. A consumer breach notice involving sensitive financial identity information must also include a prominent statement (so that consumers will see it and understand what they need to do) explaining to the consumer how to obtain free file monitoring free of charge for at least 6 months, including a telephone number and additional contact information to request the monitoring.

A consumer reporter may provide notice to consumers of a data security breach in a number of manners, including in writing, orally, or electronically. However, a consumer reporter may only provide notice by means other than a written mailed notice if the consumer has previously agreed to receive notices by the specific alternative manner and has not subsequently withdrawn the agreement. Additionally, the alternative notice is only valid if all statutorily required content is included in the communication. So for example, if a breach notice is being provided to a consumer by telephone pursuant to prior agreement, the phone notice is only valid once all of the information is directly communicated to the consumer, and would not be valid if the consumer did not actually receive the call with all of the required information being presented. If a consumer reporter provides notice electronically, the consumer reporter must provide a specified disclosure related to consent that is described in the Electronic Signatures in Global and National Commerce Act.

With one exception, this section does not require that more than one notice be provided to consumers with respect to the same data security breach. For example, this subsection provides that a consumer reporter is not required to provide notice to consumers if another entity has already provided a notice with respect to a breach that includes the statutorily required information. In addition, this subsection provides that a consumer reporter is not required to provide more than one notice to a consumer with respect to the same breach of data security.

However, if a consumer reporter provides notice concerning a data security breach involving sensitive financial account information and the consumer reporter then becomes aware of a reasonable likelihood that sensitive financial personal information involved in the breach is being misused in a manner causing harm or inconvenience to commit identity theft, the consumer reporter would be required to provide an additional notice to consumers and to other specified parties. The new updated notice to consumers must include the additional information required for breaches involving sensitive financial identity information, including a copy of the FTC's summary of rights and information concerning obtaining free file monitoring. Nothing in this section prohibits a consumer reporter from voluntarily providing additional notices concerning a

breach, or providing a notice through an additional manner (such as a telephone call in addition to a written notice).

This subsection provides that, except as otherwise established by agreement, a consumer reporter that suffers a data security breach shall be primarily responsible for providing notice to consumers and making available any required file monitoring, and shall be responsible for the reasonable, actual costs of any notices required under this section. For example, a consumer reporter and its service provider can enter into an agreement to contractually allocate the requirements of this section, so long as the requirements of this section are actually fulfilled. In addition, this subsection provides that a consumer reporter may not charge consumers for a breach notice or for file monitoring that is required under this section.

FCRA Section 630(h). Financial fraud mitigation

This subsection requires that a consumer reporter make a free file-monitoring service available to consumers in specified circumstances. Specifically, if a consumer reporter is required to provide notice to consumers of a data security breach involving sensitive financial identity information, the consumer reporter must make available a free file-monitoring service if a consumer makes a request within 90 days from the date that the consumer reporter provided notice to consumers. The free file-monitoring service must be for duration of at least 6 months and must be from a consumer reporting agency described in section 603(p) of the FCRA or from an identity-monitoring service that qualifies pursuant to guidelines from the standard-setting regulators as likely to detect fraudulent identity activity regarding a consumer on a nationwide basis.

This subsection directs the Treasury, Board and FTC to jointly develop standards and guidelines that exempt a consumer reporter from liability for harm (other than any direct pecuniary loss or loss pursuant to agreement) resulting from the misuse of sensitive financial identity information to commit identity theft that occurs after the consumer reporter has made available a free file monitoring service, if the consumer reporter meets specified requirements such as having compliant data security safeguards and system restoration actions. This safe harbor shall not be construed to create any inference with respect to the establishment or existence of any such liability. For example, this subsection is not intended to create any inference that any right of action exists under State or Federal law. Consumer reporters may offer additional services for a fee to consumers, including extended file monitoring after the free service has expired, but must obtain a specific and express consumer approval for any non-free service. Consumer reporters should not use the free service to unfairly direct consumers into a pay service.

FCRA Section 630(i). Credit security freeze

This subsection provides consumers who have been victims of identity theft with the ability to place (and remove or temporarily remove) a security freeze on his or her credit file at a consumer reporting agency. This provision is modeled on the security freeze law in the State of Vermont as of March 15, 2006. While H.R. 3997 creates a new federal standard for consumers to freeze their credit, the Committee does not intend those consumer freezes in place on

the effective date of this subsection to be prematurely terminated—the subsection goes to the placement of new freezes, not the duration of existing ones. Furthermore, the credit security freeze is intended to act in a complementary manner to the rights of consumers pursuant to section 605A and B to obtain a fraud alert or block information resulting from identity theft. A consumer who has a good faith suspicion that he or she has been or is about to become a victim of a financial crime such as identity theft may request a fraud alert under section 605A. If a consumer subsequently files an identity theft report (as defined in section 603 in part as filed with an appropriate government agency alleging that the consumer is a victim of identity theft), then the consumer may use that report to either block specific fraudulent information reported about the consumer under section 605B or use that report under this subsection to freeze any credit report on the consumer from being released without the consumer's express authorization.

Specifically under this subsection, a security freeze prohibits a consumer reporting agency from releasing all or any part of a credit report relating to a consumer unless the consumer authorizes such release or an exception permits the release. To place a security freeze, a consumer who has been the victim of identity theft must make a written request by certified mail, including an identity theft report and any reasonable identification information required by the consumer reporting agency.

Upon receipt of a consumer's request that complies with the requirements of this subsection, a consumer reporting agency must place a security freeze free of charge within 5 business days. In addition, the consumer reporting agency must, within 10 business days of placing the freeze, send written confirmation of the security freeze to the consumer, and additionally, provide the consumer with a unique personal identification number (PIN) or password to be used by the consumer to authorize the release of his or her consumer report.

A consumer may lift a security freeze so that he or she can enter into new credit transactions or for other purposes. For example, a consumer may lift a security freeze to engage in transactions with a specific party or during a specific period of time, by contacting the consumer reporting agency in a manner provided by such agency in accordance with this subsection, requesting that the freeze be temporarily lifted and providing proper identification, the unique PIN or password described above, and proper information regarding the specific party or period of time that the consumer wishes the freeze to be lifted for. If a consumer reporting agency receives a consumer's request that meets the applicable requirements, the consumer reporting agency must temporarily lift a freeze within 3 business days. The Committee hopes that over time, consumer reporting agencies may develop additional appropriate procedures to allow for the use of telephone, fax, the Internet, e-mail or other electronic form to receive and process consumer requests to lift a security freeze.

A consumer reporting agency may only remove or temporarily lift a security freeze upon a consumer's request that meets the applicable requirements or if the consumer reporting agency determines that the freeze resulted from a material misrepresentation of fact by the consumer. If a consumer reporting agency makes a deter-

mination described above, then it shall notify the consumer in writing of its determination prior to removing the security freeze on the credit report of the consumer.

This subsection permits an entity to treat a consumer's application as incomplete if the entity is unable to obtain a credit report with respect to the consumer because of a security freeze. For example, if an entity receives a consumer's application and requests a consumer report relating to the consumer but a security freeze is in place, the entity may treat the consumer's application as incomplete. In addition, a consumer reporting agency or reseller may tell a third party requesting a credit report that a security freeze is in effect for that report.

This subsection does not apply to specified entities, including resellers, entities providing check verification or fraud prevention services and certain deposit account information service companies. As a result, these entities are not required to comply with any consumer requests relating to security freezes. The Committee does not intend for the security freeze provisions to allow wrongdoers to freeze relevant fraud information to hinder anti-fraud and similar databases, including those used to prevent identity theft.

This subsection also permits the release of a consumer report in specified circumstances, even if the consumer to whom the report relates has requested a security freeze. For example, a security freeze does not apply to a person (or the person's affiliate, agent or assignee) with whom a consumer has or had (prior to an assignment) an account, contract or debtor-creditor relationship if person intends to use the consumer report for the purpose of reviewing the account or collecting a financial obligation owing for the account, contract or debt. A security freeze also does not apply to an affiliate, agent, assignee or prospective assignee of a person who has been granted access to a consumer report by a consumer under this subsection. In addition, a security freeze does not apply to any person who intends to use a consumer report for prescreening, who administers a credit file monitoring subscription or similar service to which the consumer has subscribed, or for the purpose of providing the consumer with a copy of his or her consumer report upon the consumer's request.

In addition, this subsection does not restrict authorized government entities from obtaining credit reports on consumers notwithstanding a security freeze. For example, a security freeze does not apply with respect to the request or use of a credit report on a consumer: by any Federal, State or local agency, law enforcement agency, trial court, or person acting pursuant to court order, warrant or subpoena; by any Federal, State or local agency that administers a program for establishing and enforcing child support obligations for the purpose of administering such program; by any Federal, State or local health agency (or agent or assignee of such agency) acting to investigate fraud; or by any Federal, State or local tax agency (or agent or assignee of such agency) acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any statutory responsibility of such agency.

This subsection prohibits a consumer reporting agency from imposing a fee on a credit freeze provided pursuant to this subsection, including for placing, removing, or temporarily removing the credit freeze. This subsection and this prohibition on fees do not apply,

however, to credit freezes voluntarily offered by consumer reporting agencies outside of this section (for example to people other than victims of identity theft that comply with the requirements of this subsection).

This subsection requires that at any time the FCRA requires that a consumer be provided with a copy of the FTC's model summary of rights to obtain and dispute information in consumer reports and to obtain credit scores (section 609(c)(1)) or summary of rights of identity theft victims (Section 609(d)(1)), the consumer also must provided with a specific notice concerning the right of victims of identity theft to obtain a security freeze to help the consumer understand the effect of the security freeze. The subsection sets forth the specific language that must be included with the summaries.

FCRA Section 630(j). Effect on GLBA

This subsection would supersede any current and future breach notice regulations and guidelines issued under section 501(b) of the GLBA with respect to depository institutions, and any data security regulations or guidelines issued under section 501(b) of the GLBA with respect to non-depository institutions as of the effective date of regulations required under this section. As a result, the data security notice regulations issued by the Board, OCC, OTS, FDIC and NCUA under section 501(b) of the GLBA would be superseded. Thus, for example, a bank would not be subject to such notice guidance, but would be subject only to the requirements of this section; however, this subsection would not supersede the safeguards requirements of section 501(b) of the GLBA with respect to banks and their affiliates and subsidiaries. Nor does it pertain to any other provision of the GLB Act.

FCRA Section 630(k). Uniform security regulations

This subsection directs the Treasury, Board, and FTC jointly to develop implementing standards and guidelines for entities that are not under the jurisdiction of the Federal banking agencies under subsection (l), and the Board, OCC, OTS, FDIC, and NCUA jointly to develop implementing standards and guidelines for entities under their jurisdiction under subsection (l), in a consistent manner. These implementing standards and guidelines must be issued within 9 months following enactment of this Act. In developing implementing standards and guidelines, the Treasury, Board and FTC must consult and coordinate with the functional regulatory agencies. All the regulators are required to implement this section in a consistent and comparable manner, with the intention of the Committee to create a relatively uniform enforcement regime governing data security for the entire chain of use of financial information.

This subsection further requires that the implementing standards and guidelines must include a number of specified standards. For example, these standards and guidelines must prescribe a reasonably unique and exclusive color and titling for a notice to consumers of a data security breach. These notices must use a standardized format for the notice content, to make them more likely to be reviewed by, understood by, and helpful to consumers. These notices must also place the critical information for consumers, to the

extent possible, in a prominent text box at the top of each notice, so that consumers can quickly understand the pertinent details of how the breach affects them and what actions they need to take.

These standards and guidelines also must address other aspects of providing notice to consumers, including what to do if a consumer reporter is unable after reasonable efforts to contact a consumer, when public notice is allowed instead of mailed consumer breach notices where reasonable efforts to obtain the consumer contact information has failed or the identities of specific consumers affected by a breach are not determinable, and additional guidance regarding when and how consumer reporters can communicate breaches to other critical third parties using reasonable means such as electronic transmissions commonly used by the consumer reporter's business customers.

In addition, the standards and guidelines must elaborate on how to determine whether a technology is generally commercially available for purposes of investigating and determining whether a data security breach has occurred. The standards and guidelines also must address how notice will be provided to consumers in the rare instances where the consumer reporter that suffered the breach is unavailable to pay for such notices, because for example they are bankrupt or outside the jurisdiction of the U.S and refusing to comply. The standards and guidelines also must provide for periodic notice to certain entities, including law enforcement, when a consumer reporter determines that a data security breach will impact only a de minimis number of consumers or to the extent the regulators deem appropriate where information has been lost or illegally obtained but does not result in a breach. Finally, the standards and guidelines also must establish what types of accounts can be subject to unauthorized transactions after a breach involving sensitive financial account information, such as certain open-end credit plans where additional account fraud is relatively more likely.

The Treasury, Board and FTC must jointly establish and publish model forms and disclosure statements to facilitate compliance with the notice requirements of subsection (g) and to aid consumer in understanding the information disclosed and the options and services available to them, such as file monitoring services or consumer reports. A consumer reporter may choose to use these model forms and disclosures in order to comply with the corresponding requirements of this section, and shall be deemed to be in compliance with such requirements if the model forms are used.

This subsection requires the functional regulatory agencies, after consultation and coordination, to prescribe enforcement regulations to ensure compliance with this section. These regulations and the enforcement of this section are required and only allowed to the extent consistent with the corresponding implementing standards and guidelines. The enforcement regulations issued by a functional regulatory agency will apply to any person subject to the enforcement jurisdiction of such agency under subsection (l). These enforcement regulations must be issued within 6 months following the date on which the corresponding implementing standards and guidelines are issued, so that the provisions of this section become enforceable no later than 15 months total after the date of enactment. If any of the entities fail to meet their applicable 9 month

or additional 6 month deadline for their standards, guidelines, or regulations, then those entities must report to Congress explaining why the deadline was missed, when the requirements will be fulfilled, and how consumers and other affected parties will be harmed by the delay.

In prescribing these enforcement regulations, the functional regulatory agencies are directed to use the GLBA requirements pertaining to data safeguards as a base, including the regulations and guidelines issued under GLBA, adding such other consumer protections as appropriate under this section. This provision is intended to direct the regulators to build off of their work on GLBA while clarifying the appropriate expanded and adjusted coverage and more detailed and refined requirements. These enforcement regulations may include narrowly tailored exceptions to the requirements of this section that the functional regulatory agencies jointly deem to be consistent with the purposes of this section where the exceptions are narrowly tailored and related to a special aspect of the regulated entities or the laws and other requirements they are subject to. It is the intent of Congress that the State insurance regulators will implement and interpret their enforcement regulations in a uniform manner with each other and the other functional regulators, to avoid any inconsistent treatment of entities subject to their jurisdiction.

This subsection directs the Treasury, Board and FTC, in consultation with the Administrator of the Small Business Administration and the functional regulatory agencies, to provide appropriate exemptions or modifications from the requirements of this section for consumer reporters that do not handle large quantities of sensitive financial personal information. In providing these exemptions or modifications, the regulators shall take into account the degree of sensitivity of the information, the likelihood of misuse, and the risk and degree of harm to the related consumers. The Committee intends that the regulators will provide more flexibility for entities whose databases or information storage systems are less target-rich environments for fraudsters and that would cause relatively damage if breached.

Any agency or authority that is required to issue standards and guidelines or enforcement regulations under this subsection and that fails to meet the deadlines prescribed under this subsection must report to Congress within 30 days of the deadline explaining such failure.

This subsection provides that any person who uses the unique color and titling of a consumer notice adopted under this subsection in a way that is likely to create a false belief in a consumer that a communication is a notice of a data security breach shall be liable for such use. The liability shall be to the same extent as a debt collector failing to comply with 15 U.S.C. 1692k (imposing civil liability on intentional violations of the Fair Debt Collection Practices Act). This provision is intended to ensure that the unique color and transmission titling used for consumer breach notices is not misused for other purposes, so that consumers will not be confused or misled.

FCRA Section 630(l). Administrative enforcement

This subsection provides for an administrative enforcement scheme based on the enforcement scheme of Title V of the GLBA. Specifically, this subsection establishes that the provisions of section 630 shall be enforced only by the functional regulatory agencies. A violation of section 630 will be treated as a violation of the statute under which each functional regulatory agency has enforcement authority, as delineated in this subsection. As a result, section 630 is not subject to administrative enforcement under section 621, including enforcement by State Attorneys General. In addition, section 630 is not subject to private rights of action under section 616 or 617. The FTC is also granted additional enforcement authority to be able to impose fines on entities subject to its jurisdiction by treating noncompliance by such entities with this section as an unfair and deceptive act or practice in violation of the Federal Trade Commission Act.

This subsection permits the functional regulatory agencies to use certain undistributed funds resulting from an action brought under section 630 for educational programs and outreach activity that are consistent with, and further the purposes of, the FCRA.

FCRA Section 630(m). Definitions

This subsection establishes definitions for the following terms: "breach of data security" and "data security breach;" "consumer;" "consumer financial file and consumer reports;" "consumer reporter;" "financial institution;" "functional regulatory agency;" "handled by;" "nationwide consumer reporting agency;" "neural network;" "sensitive financial account information;" "sensitive financial identity information;" "sensitive financial personal information;" and "harm or inconvenience." These definitions shall apply only with respect to the use of these terms within section 630, and shall not apply to any other section of the FCRA.

This subsection defines the term "handled by" in an intentionally broad manner, and the Committee intends such term to be interpreted broadly, to capture all the entities in the information chain for a transaction involving sensitive financial personal information to capture all masters and servants in the process, for example because a party maintains, services, or communicates such information by or on behalf of a consumer reporter.

This subsection also defines the term "harm or inconvenience" to mean a financial loss to, or civil or criminal penalties imposed on, a consumer or the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, in order to avoid the risk of financial loss or increased costs or civil or criminal penalties. This definition limits notices to consumers to situations where a consumer needs to take significant or meaningful action to protect himself or herself from financial loss or civil or criminal penalties. The term "financial loss" is intended to mean financial liability to another party or the loss of funds from a financial account or similar direct loss as a result of identity theft or account fraud. Although in most cases consumers have no liability for unauthorized transactions on their accounts, where consumers are held liable for such losses or need to expend significant time and effort to avoid such liability, they should receive notice of a data security breach that is likely to lead to such liability.

Similarly, where consumers need to check or monitor their files at consumer reporting agencies to detect and correct erroneous financial information due to identity theft, consumers should receive notice. The term "financial loss" is not intended to mean any insignificant or minimal funds spent by a consumer to address identity theft or account fraud, such as the cost of postage or telephone calls.

FCRA Section 630(n). Relation to state laws

This subsection establishes uniform national consumer protection standards preempting state requirements and prohibitions. Specifically, this subsection provides that no requirement or prohibition may be imposed under State law with respect to the responsibilities of any person to: (1) protect the security and confidentiality of information relating to consumers; (2) safeguard information relating to consumers from misuse; (3) investigate or provide notices of the unauthorized access to, or the potential misuse of, information relating to consumers for fraudulent purposes; and (4) mitigate any loss or harm resulting from such unauthorized access or misuse. In addition, this subsection provides that no requirement or prohibition may be imposed under State law that restrict consumer reports from being provided, or impose any requirements on such provision, for a permissible purpose under section 604, including, for example, any State security freeze law. State laws are also preempted if they are the functional equivalent of any of the above items. This functional equivalency test is intended by the Committee to ensure, for example, that States don't try to create an artificial distinction in creating a law that would undermine the uniform Federal standard governing the responsibilities of consumer reporters in these areas.

The uniform standards provided under this subsection do not preempt State laws governing professional confidentiality. In addition, the uniform standards provided under this subsection do not preempt State privacy laws limiting the purposes for which information may be disclosed. The legislation does not address the relationship between the rest of the FCRA, or other federal laws, and state law. In addition, the uniform standards provided under this subsection do not preempt any enforcement regulations required under this section with respect to persons engaging in the business of insurance that are issued by the State insurance authorities, to the extent that the insurance enforcement regulations are promulgated, enforced, and interpreted in a manner consistent with this section and the implementation of this section by the entities issuing the standards and guidelines under subsection (k)(1).

Section 2(b). Clerical amendment

This subsection amends the table of contents in the FCRA.

Section 2(c). Effective date

This subsection generally makes the provisions of section 630 effective upon the publication of each functional regulator's enforcement regulation, with respect to persons under the regulator's jurisdiction. However, the provisions of section 630 that require the development and issuance of standards and guidelines and regula-

tions (subsection (k)) shall become effective immediately upon enactment of this Act.

Section 3. National summit on data security

This section calls for the establishment of a National Summit on Data Security to be convened no later than April 30, 2008. The Committee intends that the summit shall serve as a national forum for sharing best practices in data security, both between government agencies and with the private sector. The summit should be modeled on the SAVER summit on retirement security and represent a broad variety of opinion and experience. The summit shall also highlight the importance of data security to the general public. The summit shall coordinate with other government and private sector bodies (including the Financial Literacy and Education Commission (FLEC)) on ways to improve knowledge about data security as part of financial literacy efforts.

Section 4. GAO study

This section requires the Comptroller General to conduct a study to determine the feasibility of a system that would provide notices of data security breaches in languages other than English and to identify any existing barriers to implementing such a system. The Comptroller General is required to report to Congress within one year after the date of enactment of this Act. Specifically, the Committee is concerned that individuals who communicate in languages other than English may not understand the notices they may receive about data breaches. Consequently, these individuals may remain unaware of any of their rights or mitigation options and as a result may not take any of the appropriate actions necessary to protect themselves in the event of a data security breach—for example obtaining file monitoring, placing a fraud alert, blocking fraudulent charges, freezing their credit file, or taking other actions necessary to limit potential harm from financial account fraud and identity theft. The Committee intends that Section 4 will require the GAO to research and provide recommendations that will help Congress consider the facilitation of a system that will provide notices of data breaches in languages other than English. The Committee further intends that, as part of the study, the GAO will provide recommendations for legislative and administrative actions, after consulting all interested parties, including those representing the interests of consumers, communities, minorities, data furnishers, federal agencies, credit reporting agencies, related business interests and others they deem appropriate.

Section 5. Enhanced data collection on data security breaches and account fraud

This section addresses enhanced data collection on data security breaches and account fraud by directing the FTC to compile information about race and ethnicity that is volunteered by victims of identity theft, account fraud and other types of financial fraud, in order to improve law enforcement efforts relating to data security breaches and fighting identity theft and account fraud. This information will be available exclusively to the FTC and to law enforcement entities. It is the intent of the Committee that the FTC will enhance its data collection on data security breaches and account

fraud by compiling information on victims of identity theft, account fraud, and other types of financial fraud, by ethnic group and race, to the extent that the victims have volunteered their race or ethnicity, and in accordance with how such victims have defined their race or ethnicity. In carrying out this section, the Committee intends that the FTC shall consult with the various international, national, State, and local law enforcement officers and agencies who work with such victims to break down the complaints that it receives by race and ethnicity to the extent practicable and voluntarily provided, to help law enforcement ascertain whether these victims have greater susceptibility of identity theft because of cultural and language factors, for example because of the commonality of surnames.

Section 6. Clarification relating to credit monitoring services

This section amends the definition of a "credit repair organization" in the Credit Repair Organization Act (CROA) to establish that certain activities—including providing access to credit reports, credit monitoring notifications, credit scores and other tools related to credit scores, or providing any analysis, evaluation and explanation of actual or hypothetical credit scores or any similar projections, forecasts, analyses, evaluations or explanations—are not included as activities that are considered as "improving any consumer's credit record, credit history or credit rating" in determining whether a person is a credit repair organization.

The intent of CROA is to rein in fraudulent credit repair organizations, not to stop the sale of legitimate products and services, such as credit monitoring products and similar consumer educational tools. Additionally, under this section, only those credit monitoring services complying with the statute would be eligible for the CROA exemption.

As this legislation provides for credit monitoring as a remedy for certain data breach victims, this section resolves these matters by clarifying the scope of exempt activities under CROA. Specifically, this section requires that in order to qualify for the exemption, consumers must be provided with specified disclosures and the opportunity to cancel the credit monitoring services without penalty or fee. In addition, the section narrows the exemption from CROA for non-profit organizations in a manner that will enhance the regulator's ability to challenge claims of exemption from CROA. Finally, the section updates the required disclosures under section 405 of CROA to reflect the right to obtain annual free credit reports under the FCRA provided by passage of the FACT Act in 2003.

This section is effective upon enactment, and reflects the intent of Congress to clarify the long-standing definition of a credit repair organization.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

FAIR CREDIT REPORTING ACT

TITLE VI—CONSUMER CREDIT REPORTING

Sec.
601. Short title.

* * * * * * *

630. Data security safeguards.

§ 601. Short title

This title may be cited as the "Fair Credit Reporting Act".

* * * * * * *

SEC. 630. DATA SECURITY SAFEGUARDS.

(a) PROTECTION OF SENSITIVE FINANCIAL PERSONAL INFORMATION.—

(1) DATA SECURITY OBLIGATION POLICY.—It is the policy of the Congress that each consumer reporter has an affirmative and continuing obligation to protect the security and confidentiality of sensitive financial personal information.

(2) SECURITY POLICIES AND PROCEDURES.—Each consumer reporter shall have an affirmative obligation to implement, and a continuing obligation to maintain, reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information relating to any consumer that is handled by such consumer reporter against any loss, unauthorized access, or misuse that is reasonably likely to result in harm or inconvenience to such consumer.

(3) DATA DESTRUCTION AND DATA DISPOSAL POLICIES AND PROCEDURES.—The policies and procedures described in paragraph (2) shall include providing for the proper disposal of sensitive financial personal information in accordance with the standards, guidelines, or regulations issued pursuant to this title.

(b) INVESTIGATION REQUIREMENTS.—

(1) INVESTIGATION TRIGGER.—A consumer reporter shall immediately conduct a data security breach investigation if it—

(A) becomes aware of any information indicating a reasonable likelihood that a data security breach has occurred or is unavoidable;

(B) becomes aware of information indicating an unusual pattern of misuse of sensitive financial personal information handled by a consumer reporter indicative of financial fraud; or

(C) receives a notice under subsection (e).

(2) SCOPE OF INVESTIGATION.—Such investigation shall be conducted in a manner commensurate with the nature and the amount of the sensitive financial personal information that is subject to the breach of data security, including appropriate actions to—

(A) assess the nature and scope of the potential breach;

(B) identify the sensitive financial personal information potentially involved;

(C) determine whether such information is usable by the parties causing the breach; and

(D) determine the likelihood that such information has been, or will be, misused in a manner that may cause harm or inconvenience to the related consumer.

(3) ENCRYPTION AND OTHER SAFEGUARDS.—

(A) SUGGESTED SAFEGUARDS.—The regulators described in subsection (k)(1) shall jointly develop standards and guidelines to identify and regularly update appropriate technology safeguards for making consumer reporter's sensitive financial personal information unusable in a manner commensurate with the nature and the amount of such information, including—

(i) consideration of the encryption standards adopted by the National Institute of Standards and Technology for use by the Federal Government; and

(ii) appropriate management and protection of keys or codes necessary to protect the integrity of encrypted information.

(B) SAFEGUARD FACTORS.—In determining the likelihood of a data security breach, a consumer reporter may consider whether the information subject to the potential breach is unusable because it is encrypted, redacted, requires technology to use that is not generally commercially available, or has otherwise similarly been rendered unreadable.

(C) SAFE HARBOR FOR PROTECTED DATA.—As set forth in the standards and guidelines issued pursuant to subparagraph (A), a consumer reporter may reasonably conclude that a data security breach is not likely to have occurred where the sensitive personal financial information involved has been encrypted, redacted, requires technology to use that is not generally commercially available, or is otherwise unlikely to be usable

(D) EXCEPTION.—Subparagraphs (B) and (C) shall not apply if the consumer reporter becomes aware of information that would reasonably indicate that the information that was the subject of the potential breach is usable by the entities causing the breach or potentially misusing the information, for example because—

(i) an encryption code is potentially compromised,

(ii) the entities are believed to have the technology to access the information; or

(iii) there is an unusual pattern of misuse of such information indicative of financial fraud.

(c) BREACH NOTICES.—If a consumer reporter determines that a breach of data security has occurred, is likely to have occurred, or is unavoidable, the consumer reporter shall in the order listed—

(1) promptly notify the United States Secret Service;

(2) promptly notify the appropriate functional regulatory agency for the consumer reporter;

(3) notify as appropriate and without unreasonable delay—

(A) any third party entity that owns or is obligated on an affected financial account as set forth in the standards or guidelines pursuant to subsection (k)(1)(G), including in such notification information reasonably identifying the na-

ture and scope of the breach and the sensitive financial personal information involved; and

(B) any other appropriate critical third parties whose involvement is necessary to investigate the breach; and

(4) without unreasonable delay notify any affected consumers to the extent required in subsection (f), as well as—

(A) each nationwide consumer reporting agency, in the case of a breach involving sensitive financial identity information relating to 1,000 or more consumers; and

(B) any other appropriate critical third parties who will be required to undertake further action with respect to such information to protect such consumers from resulting fraud or identity theft.

(d) SYSTEM RESTORATION REQUIREMENTS.—If a consumer reporter determines that a breach of data security has occurred, is likely to have occurred, or is unavoidable, the consumer reporter shall take prompt and reasonable measures to—

(1) repair the breach and restore the security and confidentiality of the sensitive financial personal information involved to limit further unauthorized misuse of such information; and

(2) restore the integrity of the consumer reporter's data security safeguards and make appropriate improvements to its data security policies and procedures.

(e) THIRD PARTY DUTIES.—

(1) COORDINATED INVESTIGATION.—Whenever any consumer reporter that handles sensitive financial personal information for or on behalf of another party becomes aware that an investigation is required under subsection (b) with respect to such information, the consumer reporter shall—

(A) promptly notify the other party of the breach;

(B) conduct a coordinated investigation with the other party as described in subsection (b); and

(C) ensure that the appropriate notices are provided as required under subsection (f).

(2) CONTRACTUAL OBLIGATION REQUIRED.—No consumer reporter may provide sensitive financial personal information to a third party, unless such third party agrees to fulfill the obligations imposed by subsections (a), (d), and (h), as well as that whenever the third party becomes aware that a breach of data security has occurred, is reasonably likely to have occurred, or is unavoidable, with respect to such information, the third party shall be obligated—

(A) to provide notice of the potential breach to the consumer reporter;

(B) to conduct a coordinated investigation with the consumer reporter to identify the sensitive financial personal information involved and determine if the potential breach is reasonably likely to result in harm or inconvenience to any consumer to whom the information relates; and

(C) provide any notices required under this section, except to the extent that such notices are provided by the consumer reporter in a manner meeting the requirements of this section.

(f) CONSUMER NOTICE.—

(1) POTENTIAL IDENTITY THEFT RISK AND FRAUDULENT TRANSACTION RISK.—A consumer reporter shall provide a consumer notice if, at any point the consumer reporter becomes aware—

(A) that a breach of data security is reasonably likely to have occurred or be unavoidable, with respect to sensitive financial personal information handled by the consumer reporter;

(B) of information reasonably identifying the nature and scope of the breach; and

(C) that such information is reasonably likely to have been or to be misused in a manner causing harm or inconvenience against the consumers to whom such information relates to—

(i) commit identity theft if the information is sensitive financial identity information, or

(ii) make fraudulent transactions on such consumers' financial accounts if the information is sensitive financial account information.

(2) SECURITY PROGRAM SAFEGUARDS AND REGULATIONS.—

(A) STANDARDS FOR SAFEGUARDS.—The regulators described in subsection (k)(1) shall issue guidelines relating to the types of sophisticated neural networks and security programs that are likely to detect fraudulent account activity and at what point detection of such activity is sufficient to avoid consumer notice under this subsection.

(B) ALTERNATIVE SAFEGUARDS.—In determining the likelihood of misuse of sensitive financial account information and whether a notice is required under paragraph (1), the consumer reporter may additionally consider—

(i) consistent with any standards promulgated under subparagraph (A), whether any neural networks or security programs used by, or on behalf of, the consumer reporter have detected, or are likely to detect on an ongoing basis over a reasonable period of time, fraudulent transactions resulting from the breach of data security; or

(ii) whether no harm or inconvenience is reasonably likely to have occurred, because for example the related consumer account has been closed or its number has been changed.

(3) COORDINATION WITH THE FAIR DEBT COLLECTION PRACTICES ACT.—The provision of a notice to the extent such notice and its contents are required under this section shall not be considered a communication under the Fair Debt Collection Practices Act.

(4) COORDINATION OF CONSUMER NOTICE DATABASE.—

(A) IN GENERAL.—The Commission shall coordinate with the other government entities identified in this section to create a publicly available list of data security breaches that have triggered a notice to consumers under this subsection within the last 12 months.

(B) LISTED INFORMATION.—The publicly available list described in subparagraph (A) shall include the following:

(i) The identity of the party responsible that suffered the breach.

(ii) A general description of the nature and scope of the breach.

(iii) Any financial fraud mitigation or other services provided by such party to the affected consumers, including the telephone number and other appropriate contact information for accessing such services.

(g) TIMING, CONTENT, AND MANNER OF NOTICES.—

(1) DELAY OF NOTICE FOR LAW ENFORCEMENT PURPOSES.—If a consumer reporter receives a written request from an appropriate law enforcement agency indicating that the provision of a notice under subsection (c)(3) or (f) would impede a criminal or civil investigation by that law enforcement agency, or an oral request from an appropriate law enforcement agency indicating that such a written request will be provided within 2 business days—

(A) the consumer reporter shall delay, or in the case of a foreign law enforcement agency may delay, providing such notice until—

(i) the law enforcement agency informs the consumer reporter that such notice will no longer impede the investigation; or

(ii) the law enforcement agency fails to—

(I) provide within 10 days a written request to continue such delay for a specific time that is approved by a court of competent jurisdiction; or

(II) in the case of an oral request for a delay, provide a written request within 2 business days, and if such delay is requested for more than 10 additional days, such request must be approved by a court of competent jurisdiction; and

(B) the consumer reporter may—

(i) conduct appropriate security measures that are not inconsistent with such request; and

(ii) contact such law enforcement agency to determine whether any such inconsistency would be created by such measures.

(2) HOLD HARMLESS PROVISION.—A consumer reporter shall not be liable for any fraud mitigation costs or for any losses that would not have occurred but for notice to or the provision of sensitive financial personal information to law enforcement, or the delay provided for under this subsection, except that—

(A) nothing in this subparagraph shall be construed as creating any inference with respect to the establishment or existence of any such liability; and

(B) this subparagraph shall not apply if the costs or losses would not have occurred had the consumer reporter undertaken reasonable system restoration requirements to the extent required under subsection (d), or other similar provision of law, except to the extent that such system restoration was delayed at the request of law enforcement.

(3) CONTENT OF CONSUMER NOTICE.—Any notice required to be provided by a consumer reporter to a consumer under subsection (f)(1), and any notice required in accordance with subsection (e)(2)(A), shall be provided in a standardized trans-

mission or exclusively colored envelope, and shall include the following in a clear and conspicuous manner:

(A) An appropriate heading or notice title.

(B) A description of the nature and types of information and accounts as appropriate that were, or are reasonably believed to have been, subject to the breach of data security.

(C) A statement identifying the party responsible, if known, that suffered the breach, including an explanation of the relationship of such party to the consumer.

(D) If known, the date, or the best reasonable approximation of the period of time, on or within which sensitive financial personal information related to the consumer was, or is reasonably believed to have been, subject to a breach.

(E) A general description of the actions taken by the consumer reporter to restore the security and confidentiality of the breached information.

(F) A telephone number by which a consumer to whom the breached information relates may call free of charge to obtain additional information about how to respond to the breach.

(G) With respect to notices involving sensitive financial identity information, a copy of the summary of rights of consumer victims of fraud or identity theft prepared by the Commission under section 609(d), as well as any additional appropriate information on how the consumer may—

(i) obtain a copy of a consumer report free of charge in accordance with section 612;

(ii) place a fraud alert in any file relating to the consumer at a consumer reporting agency under section 605A to discourage unauthorized use; and

(iii) contact the Commission for more detailed information.

(H) With respect to notices involving sensitive financial identity information, a prominent statement in accordance with subsection (h) that file monitoring will be made available to the consumer free of charge for a period of not less than six months, together with a telephone number for requesting such services, and may also include such additional contact information as a mailing address, e-mail, or Internet website address.

(I) The approximate date the notice is being issued.

(4) OTHER TRANSMISSION OF NOTICE.—The notice described in paragraph (3) may be made by other means of transmission (such as electronic or oral) to a consumer only if—

(A) the consumer has affirmatively consented to such use, has not withdrawn such consent, and with respect to electronic transmissions is provided with the appropriate statements related to such consent as described in section 101(c)(1) of the Electronic Signatures in Global and National Commerce Act; and

(B) all of the relevant information in paragraph (3) is communicated to such consumer in such transmission.

(5) DUPLICATIVE NOTICES.—

(A) IN GENERAL.—A consumer reporter, whether acting directly or in coordination with another entity—

(i) shall not be required to provide more than 1 notice with respect to any breach of data security to any affected consumer, so long as such notice meets all the applicable requirements of this section, and

(ii) shall not be required to provide a notice with respect to any consumer if a notice meeting the applicable requirements of this section has already been provided to such consumer by another entity.

(B) UPDATING NOTICES.—If a consumer notice is provided to consumers pursuant only to subsection (f)(1)(C)(ii) (relating to sensitive financial account information), and the consumer reporter subsequently becomes aware of a reasonable likelihood that sensitive financial personal information involved in the breach is being misused in a manner causing harm or inconvenience against such consumer to commit identity theft, an additional notice shall be provided to such consumers as well any other appropriate parties under this section, including a copy of the Commission's summary of rights and file monitoring mitigation instructions under subparagraphs (G) and (H) of paragraph (3).

(6) RESPONSIBILITY AND COSTS.—

(A) IN GENERAL.—Except as otherwise established by written agreement between the consumer reporter and its agents or third party servicers, the entity that suffered a breach of data security shall be—

(i) primarily responsible for providing any consumer notices and file monitoring required under this section with respect to such breach; and

(ii) responsible for the reasonable actual costs of any notices provided under this section.

(B) IDENTIFICATION TO CONSUMERS.—No such agreement shall restrict the ability of a consumer reporter to identify the entity responsible for the breach to consumers

(C) NO CHARGE TO CONSUMERS.— The cost for the notices and file monitoring described in subparagraph (A) may not be charged to the related consumers.

(h) FINANCIAL FRAUD MITIGATION.—

(1) FREE FILE MONITORING.—Any consumer reporter that is required to provide notice to a consumer under subsection (f)(1)(C)(i), or that is deemed to be in compliance with such requirement by operation of subsection (j), if requested by the consumer before the end of the 90-day period beginning on the date of such notice, shall make available to the consumer, free of charge and for at least a 6-month period—

(A) a service that monitors nationwide credit activity regarding a consumer from a consumer reporting agency described in section 603(p); or

(B) a service that provides identity-monitoring to consumers on a nationwide basis that meets the guidelines described in paragraph (2).

(2) IDENTITY MONITORING NETWORKS.—The regulators described in subsection (k)(1) shall issue guidelines on the type of identity monitoring networks that are likely to detect fraudulent identity activity regarding a consumer on a nationwide basis and would satisfy the requirements of paragraph (1).

(3) JOINT RULEMAKING FOR SAFE HARBOR.—In accordance with subsection (j), the Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission shall jointly develop standards and guidelines, which shall be issued by all functional regulatory agencies, that, in any case in which—

(A) free file monitoring is offered under paragraph (1) to a consumer;

(B) subsequent to the offer, another party misuses sensitive financial identity information on the consumer obtained through the breach of data security (that gave rise to such offer) to commit identity theft against the consumer; and

(C) at the time of such breach the consumer reporter met the requirements of subsections (a) and (d),

exempts the consumer reporter from any liability for any harm to the consumer resulting from such misuse, other than any direct pecuniary loss or loss pursuant to agreement by the consumer reporter, except that nothing in this paragraph shall be construed as creating any inference with respect to the establishment or existence of any such liability.

(i) CREDIT SECURITY FREEZE.—

(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) SECURITY FREEZE.—The term "security freeze" means a notice placed in a credit report on a consumer, at the request of the consumer who is a victim of identity theft, that prohibits the consumer reporting agency from releasing all or any part of the credit report, without the express authorization of the consumer, except as otherwise provided in this section.

(B) REVIEWING THE ACCOUNT; ACCOUNT REVIEW.—The terms 'reviewing the account' and 'account review' include activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(2) REQUEST FOR A SECURITY FREEZE.—

(A) IN GENERAL.—A consumer who has been the victim of identity theft may place a security freeze on the file of such consumer at any consumer reporting agency by—

(i) making a request in writing by certified mail to the consumer reporting agency;

(ii) submitting an identity theft report to the consumer reporting agency; and

(iii) providing such evidence of the identity of the consumer as such consumer reporting agency may require under paragraph (5).

(B) PROMPT IMPOSITION OF FREEZE.—A consumer reporting agency shall place a security freeze on a credit report on a consumer no later than 5 business days after receiving a written request from the consumer in accordance with subparagraph (A).

(C) EFFECT OF FREEZE.—

(i) IN GENERAL.—Except as otherwise provided in this subsection, if a security freeze is in place with respect to any consumer, information from the con-

sumer's credit report may not be released by the consumer reporting agency or reseller to any third party, including another consumer reporting agency or reseller, without the prior express authorization from the consumer or as otherwise permitted in this section.

(ii) ADVISING OF EXISTENCE OF SECURITY FREEZE.—Clause (i) shall not be construed as preventing a consumer reporting agency or reseller from advising a third party that a security freeze is in effect with respect to the credit report on the consumer.

(D) CONFIRMATION OF FREEZE; ACCESS CODE.—Any consumer reporting agency that receives a consumer request for a security freeze in accordance with subparagraph (A) shall—

(i) send a written confirmation of the security freeze to the consumer within 10 business days of placing the freeze; and

(ii) at the same time, provide the consumer with a unique personal identification number or password (other than the Social Security account number of any consumer) to be used by the consumer when providing authorization for the release of the credit report of the consumer to a specific party or for a specific period of time.

(3) ACCESS PURSUANT TO CONSUMER AUTHORIZATION DURING SECURITY FREEZE.—

(A) NOTICE BY CONSUMER.—If the consumer wishes to allow the credit report on the consumer to be accessed by a specific party or for a specific period of time while a freeze is in place, the consumer shall—

(i) contact the consumer reporting agency in any manner the agency may provide;

(ii) request that the security freeze be temporarily lifted; and

(iii) provide—

(I) proper identification;

(II) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (2)(D)(ii); and

(III) the proper information regarding the third party who is to receive the credit report or the time period for which the report shall be available to users of the credit report.

(B) TIMELY RESPONSE REQUIRED.—A consumer reporting agency that receives a request from a consumer to temporarily lift a security freeze on a credit report in accordance with subparagraph (A) shall comply with the request no later than 3 business days after receiving the request.

(C) PROCEDURES FOR REQUESTS.—A consumer reporting agency may develop procedures involving the use of telephone, fax, or, upon the consent of the consumer in the manner required by the Electronic Signatures in Global and National Commerce Act for notices legally required to be in writing, by the Internet, e-mail, or other electronic medium to receive and process a request from a consumer

to temporarily lift a security freeze on a credit report pursuant to subparagraph (A) in an expedited manner.

(4) LIFTING OR REMOVING SECURITY FREEZE.—

(A) IN GENERAL.—A consumer reporting agency may remove or temporarily lift a security freeze placed on a credit report on a consumer only in the following cases:

(i) Upon receiving a consumer request for a temporary lift of the security freeze in accordance with paragraph (3)(A).

(ii) Upon receiving a consumer request for the removal of the security freeze in accordance with subparagraph (C).

(iii) Upon a determination by the consumer reporting agency that the security freeze was imposed on the credit report due to a material misrepresentation of fact by the consumer.

(B) NOTICE TO CONSUMER OF DETERMINATION.—If a consumer reporting agency makes a determination described in subparagraph (A)(iii) with a respect to a security freeze imposed on the credit report on any consumer, the consumer reporting agency shall notify the consumer of such determination in writing prior to removing the security freeze on such credit report.

(C) REMOVING SECURITY FREEZE.—

(i) IN GENERAL.—Except as provided in this subsection, a security freeze shall remain in place until the consumer requests that the security freeze be removed.

(ii) PROCEDURE FOR REMOVING SECURITY FREEZE.—A consumer reporting agency shall remove a security freeze within 3 business days of receiving a request for removal from the consumer who provides—

(I) proper identification; and

(II) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (2)(D)(ii).

(5) PROPER IDENTIFICATION REQUIRED.—A consumer reporting agency shall require proper identification of any person who makes a request to impose, temporarily lift, or permanently remove a security freeze on the credit report of any consumer under this section.

(6) THIRD PARTY REQUESTS.—If—

(A) a third party requests access to a consumer's credit report on which a security freeze is in effect under this section in connection with an application by the consumer for credit or any other use; and

(B) the consumer does not allow the consumer's credit report to be accessed by that specific party or during the specific period such application is pending,

the third party may treat the application as incomplete.

(7) CERTAIN ENTITY EXEMPTIONS.—

(A) AGGREGATORS AND OTHER AGENCIES.—This subsection shall not apply to a consumer reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer reporting agency or multiple consumer re-

porting agencies, and does not maintain a permanent database of credit information from which new credit reports are produced.

(B) OTHER EXEMPTED ENTITIES.—The following entities shall not be required to place a security freeze in a credit report:

(i) An entity which provides check verification or fraud prevention services, including but not limited to, reports on incidents of fraud, verification or authentication of a consumer's identification, or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments.

(ii) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, automated teller machine abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or other financial institution.

(8) EXCEPTIONS.—This subsection shall not apply with respect to the use of a consumer credit report by any of the following for the purpose described:

(A) A person, or any affiliate, agent, or assignee of any person, with whom the consumer has or, prior to an assignment, had an account, contract, or debtor-creditor relationship for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or debt.

(B) An affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under paragraph (3) for purposes of facilitating the extension of credit or other permissible use of the report in accordance with the consumer's request under such paragraph.

(C) Any State or local agency, law enforcement agency, trial court, or person acting pursuant to a court order, warrant, or subpoena.

(D) A Federal, State, or local agency that administers a program for establishing an enforcing child support obligations for the purpose of administering such program.

(E) A Federal, State, or local health agency, or any agent or assignee of such agency, acting to investigate fraud within the jurisdiction of such agency.

(F) A Federal, State, or local tax agency, or any agent or assignee of such agency, acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of other statutory responsibility of such agency.

(G) Any person that intends to use the information in accordance with section 604(c).

(H) Any person administering a credit file monitoring subscription or similar service to which the consumer has subscribed.

(I) Any person for the purpose of providing a consumer with a copy of the credit report or credit score of the consumer upon the consumer's request.

(9) PROHIBITION ON FEE.—A consumer reporting agency may not impose a fee for placing, removing, or removing for a specific party or parties a security freeze on a credit report.

(10) NOTICE OF RIGHTS.—At any time that a consumer is required to receive a summary of rights required under section 609(c)(1) or 609(d)(1) the following notice shall be included:

"Consumers Who Are Victims of Identity Theft Have the Right to Obtain a Security Freeze on Your Consumer Report

"You may obtain a security freeze on your consumer credit report at no charge if you are a victim of identity theft and you submit a copy of an identity theft report you have filed with a law enforcement agency about unlawful use of your personal information by another person.

"The security freeze will prohibit a credit reporting agency from releasing any information in your consumer credit report without your express authorization. A security freeze must be requested in writing by certified mail.

"The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gains access to the personal and financial information in your consumer credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transaction, or other services, including an extension of credit at point of sale.

"When you place a security freeze on your consumer credit report, within 10 business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your consumer credit report or authorize the release of your consumer credit report for a specific party, parties or period of time after the freeze is in place.

"To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer reporting agency (2) Proper identification to verify your identity (3) The proper information regarding the third party or parties who are trying to receive the consumer credit report or the period of time for which the report shall be available to users of the consumer report.

"A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a consumer credit report shall comply with the request no later than 3 days after receiving the request.

"A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the

person or entity with which you have an existing account that requests information in your consumer credit report for the purposes of reviewing or collecting the account, if you have previously given your consent to this use of your consumer credit report. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account up-grades and enhancements.

"If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely or temporarily if you are shopping around, or specifically for a certain creditor, a few days before actually applying for new credit.".

(j) EFFECT ON GLBA.—

(1) DEPOSITORY INSTITUTIONS.—The current and any future breach notice regulations and guidelines under section 501(b) of the Gramm-Leach-Bliley Act with respect to depository institutions shall be superseded, as of the effective date of the regulations required under subsection (k)(3)(A), relating to the specific requirements of this section.

(2) NONDEPOSITORY INSTITUTIONS.—The current and any future data security regulations and guidelines under section 501(b) of the Gramm-Leach-Bliley Act with respect to nondepository institutions shall be superseded as of the effective date of the regulations required under subsection (k)(3)(A), relating to the responsibilities under this section.

(k) UNIFORM DATA SECURITY SAFEGUARD REGULATIONS.—

(1) UNIFORM STANDARDS.—The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission shall jointly, and the Federal functional regulatory agencies that have issued guidance on consumer breach notification shall jointly with respect to the entities under their jurisdiction, develop standards and guidelines to implement this section, including—

(A) prescribing specific standards with respect to subsection (g)(3) setting forth a reasonably unique and, pursuant to paragraph (2)(B), exclusive color and titling of the notice, and standardized formatting of the notice contents described under such subsection to standardize such communications and make them more likely to be reviewed, and understood by, and helpful to consumers, including to the extent possible placing the critical information for consumers in an easily understood and prominent text box at the top of each notice;

(B) providing in such standards and guidelines that the responsibility of a consumer reporter to provide notice under this section—

(i) has been satisfied with respect to any particular consumer, even if the consumer reporter is unable to contact the consumer, so long as the consumer reporter has made reasonable efforts to obtain a current address or other current contact information with respect to such consumer;

(ii) may be made by public notice in appropriate cases in which—

(I) such reasonable efforts described in clause (i) have failed; or

(II) a breach of data security involves a loss or unauthorized acquisition of sensitive financial personal information in paper documents or records that has been determined to be usable, but the identities of specific consumers are not determinable; and

(iii) with respect to paragraph (3) of subsection (c), may be communicated to entities in addition to those specifically required under such paragraph through any reasonable means, such as through an electronic transmission normally received by all of the consumer reporter's business customers; and

(C) providing in such standards and guidelines elaboration on how to determine whether a technology is generally commercially available for the purposes of subsection (b), focusing on the availability of such technology to persons who potentially could seek to breach the data security of the consumer reporter, and how to determine whether the information is likely to be usable under subsection (b)(3);

(D) providing for a reasonable and fair manner of providing required consumer notices where the entity that directly suffered the breach is unavailable to pay for such notices, because for example the entity is bankrupt, outside of the jurisdiction of the United States, or otherwise can not be compelled to provide such notice;

(E) providing for periodic instead of individual notices to regulators and law enforcement under subsection (c)(1) and (2) where the consumer reporter determines that only a de minimus number of consumers are reasonably likely to be affected;

(F) providing, to the extent appropriate, notice to the United States Secret Service, a consumer reporter's functional regulator, and the entities described in paragraphs (1) through (3) of subsection (c), whenever the consumer reporter's sensitive financial personal information has been lost or illegally obtained but such loss or acquisition does not result in a breach, for example because the information was sufficiently encrypted or otherwise unusable; and

(G) establishing what types of accounts might be subject to unauthorized transactions after a breach involving sensitive financial account information, for example because such accounts are open-end credit plans or are described in section 903(2) of the Electronic Fund Transfer Act.

(2) MODEL NOTICE FORMS.—

(A) IN GENERAL.—The Secretary of the Treasury, Board of Governors of the Federal Reserve System, and the Commission shall jointly establish and publish model forms and disclosure statements to facilitate compliance with the notice requirements of subsection (g) and to aid the consumer in understanding the information required to be disclosed relating to a breach of data security and the options and services available to the consumer for obtaining addi-

tional information, consumer reports, and credit monitoring services.

(B) USE OPTIONAL.—A consumer reporter may utilize a model notice or any model statement established under this paragraph for purposes of compliance with this section, at the discretion of the consumer reporter.

(C) EFFECT OF USE.—A consumer reporter that uses a model notice form or disclosure statement established under this paragraph shall be deemed to be in compliance with the requirement to provide the required disclosure to consumers to which the form or statement relates.

(3) ENFORCEMENT.—

(A) REGULATIONS.—Each of the functional regulatory agencies shall prescribe such regulations as may be necessary, consistent with the standards in paragraph (1), to ensure compliance with this section with respect to the persons subject to the jurisdiction of such agency under subsection (l).

(B) MISUSE OF UNIQUE COLOR AND TITLES OF NOTICES.—Any person who uses the unique color and titling adopted under paragraph (1)(A) for notices under subsection (f)(1) in a way that is likely to create a false belief in a consumer that a communication is such a notice shall be liable in the same manner and to the same extent as a debt collector is liable under section 813 for any failure to comply with any provision of the Fair Debt Collection Practices Act.

(4) PROCEDURES AND DEADLINE.—

(A) PROCEDURES.—Standards and guidelines issued under this subsection shall be issued in accordance with applicable requirements of title 5, United States Code.

(B) DEADLINE FOR INITIAL STANDARDS AND GUIDELINES.—The standards and guidelines required to be issued under paragraph (1) shall be published in final form before the end of the 9-month period beginning on the date of the enactment of the Financial Data Protection Act of 2006.

(C) DEADLINE FOR ENFORCEMENT REGULATIONS.—The standards and guidelines required to be issued under paragraph (2) shall be published in final form before the end of the 6-month period beginning on the date standards and guidelines described in subparagraph (B) are published in final form.

(D) AUTHORITY TO GRANT EXCEPTIONS.—The regulations prescribed under paragraph (2) may include such additional exceptions to this section as are deemed jointly by the functional regulatory agencies to be consistent with the purposes of this section if such exceptions are necessary because of some unique aspect of the entities regulated or laws governing such entities; and such exemptions are narrowly tailored to protect the purposes of this Act.

(E) CONSULTATION AND COORDINATION.—The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission shall consult and coordinate with the other functional regulatory agencies to the extent appropriate in prescribing regulations under this subsection.

(F) FAILURE TO MEET DEADLINE.—Any agency or authority required to publish standards and guidelines or regulations under this subsection that fails to meet the deadline for such publishing shall submit a report to the Congress within 30 days of such deadline describing—

(i) the reasons for the failure to meet such deadline;

(ii) when the agency or authority expects to complete the publication required; and

(iii) the detriment such failure to publish by the required deadline will have on consumers and other affected parties.

(G) UNIFORM IMPLEMENTATION AND INTERPRETATION.—It is the intention of the Congress that the agencies and authorities described in subsection (l)(1)(G) will implement and interpret their enforcement regulations, including any exceptions provided under subparagraph (D), in a uniform manner.

(5) APPROPRIATE EXEMPTIONS OR MODIFICATIONS.—The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commission, in consultation with the Administrator of the Small Business Administration and the functional regulatory agencies, shall provide appropriate exemptions or modifications from requirements of this section relating to sensitive financial personal information for consumer reporters that do not maintain, service, or communicate a large quantity of such information, taking into account the degree of sensitivity of such information, the likelihood of misuse, and the degree of potential harm or inconvenience to the related consumer.

(6) COORDINATION.—

(A) IN GENERAL.—Each functional regulatory agency shall consult and coordinate with each other functional regulatory agency so that, to the extent possible, the regulations prescribed by each agency are consistent and comparable.

(B) MODEL REGULATIONS.—In prescribing implementing regulations under paragraph (1), the functional regulatory agencies agencies referred to in such paragraph shall use the Gramm-Leach-Bliley Act (including the guidance and regulations issued thereunder) as a base, adding such other consumer protections as appropriate under this section.

(l) ADMINISTRATIVE ENFORCEMENT.—

(1) IN GENERAL.—Notwithstanding section 616, 617, or 621, compliance with this section and the regulations prescribed under this section shall be enforced by the functional regulatory agencies with respect to financial institutions and other persons subject to the jurisdiction of each such agency under applicable law, as follows:

(A) Under section 8 of the Federal Deposit Insurance Act, in the case of—

(i) national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Comptroller of the Currency;

(ii) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act, and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Governors of the Federal Reserve System;

(iii) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Directors of the Federal Deposit Insurance Corporation; and

(iv) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Director of the Office of Thrift Supervision.

(B) Under the Federal Credit Union Act, by the Board of the National Credit Union Administration with respect to any federally insured credit union, and any subsidiaries of such an entity.

(C) Under the Securities Exchange Act of 1934, by the Securities and Exchange Commission with respect to any broker, dealer, or nonbank transfer agent.

(D) Under the Investment Company Act of 1940, by the Securities and Exchange Commission with respect to investment companies.

(E) Under the Investment Advisers Act of 1940, by the Securities and Exchange Commission with respect to investment advisers registered with the Commission under such Act.

(F) Under the provisions of title XIII of the Housing and Community Development Act of 1992, by the Director of the Office of Federal Housing Enterprise Oversight (and any successor to such functional regulatory agency) with respect to the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and any other entity or enterprise or bank (as defined in such title XIII) subject to the jurisdiction of such functional regulatory agency under such title, including any affiliate of any such enterprise.

(G) Under State insurance law, in the case of any person engaged in the business of insurance, by the applicable State insurance authority of the State in which the person is domiciled.

(H) Under the Federal Home Loan Bank Act, by the Federal Housing Finance Board (and any successor to such

functional regulatory agency) with respect to the Federal home loan banks and any other entity subject to the jurisdiction of such functional regulatory agency, including any affiliate of any such bank.

(I) Under the Federal Trade Commission Act, by the Commission for any other person that is not subject to the jurisdiction of any agency or authority under subparagraphs (A) through (G) of this subsection, except that for the purposes of this subparagraph a violation of this section shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act regarding unfair or deceptive acts or practices.

(2) EXERCISE OF CERTAIN POWERS.—For the purpose of the exercise by any agency referred to in paragraph (1) of its powers under any Act referred to in such paragraph, a violation of any requirement imposed under this section shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in paragraph (1), each of the agencies referred to in that paragraph may exercise, for the purpose of enforcing compliance with any requirement imposed under this section, any other authority conferred on it by law.

(3) USE OF UNDISTRIBUTED FUNDS FOR FINANCIAL EDUCATION.—If—

(A) in connection with any administrative action under this section, a fund is created or a functional regulatory agency has obtained disgorgement; and

(B) the functional regulatory agency determines that—

(i) due to the size of the fund to be distributed, the number of individuals affected, the nature of the underlying violation, or for other reasons, it would be infeasible to distribute such fund or disgorgement to the victims of the violation; or

(ii) there are excess monies remaining after the distribution of the fund or disgorgement to victims,

the functional regulatory agency may issue an order in an administrative proceeding requiring that the undistributed amount of the fund or disgorgement be used in whole or in part by the functional regulatory agency for education programs and outreach activities of consumer groups, community based groups, and the Financial Literacy and Education Commission established under the Fair and Accurate Credit Transactions Act of 2003 that are consistent with and further the purposes of this title.

(m) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

(1) BREACH OF DATA SECURITY.—The term "breach of data security" or "data security breach" means any loss, unauthorized acquisition, or misuse of sensitive financial personal information handled by a consumer reporter that could be misused to commit financial fraud (such as identity theft or fraudulent transactions made on financial accounts) in a manner causing harm or inconvenience to a consumer.

(2) CONSUMER.—The term "consumer" means an individual.

(3) CONSUMER REPORTER AND RELATED TERMS.—

(A) CONSUMER FINANCIAL FILE AND CONSUMER REPORTS.—The term "consumer financial file and consumer reports" includes any written, oral, or other communication of any information by a consumer reporter bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, personal identifiers, financial account information, or mode of living.

(B) CONSUMER REPORTER.—The term "consumer reporter" means any consumer reporting agency or financial institution, or any person which, for monetary fees, dues, on a cooperative nonprofit basis, or otherwise regularly engages in whole or in part in the practice of assembling or evaluating consumer financial file and consumer reports, consumer credit information, or other information on consumers, for the purpose of furnishing consumer reports to third parties or to provide or collect payment for or market products and services, or for employment purposes, and which uses any means or facility of interstate commerce for such purposes.

(4) FINANCIAL INSTITUTION.—The term "financial institution" means—

(A) any person the business of which is engaging in activities that are financial in nature as described in or determined under section 4(k) of the Bank Holding Company Act;

(B) any person that is primarily engaged in activities that are subject to the Fair Credit Reporting Act; and

(C) any person that is maintaining, receiving, or communicating sensitive financial personal information on an ongoing basis for the purposes of engaging in interstate commerce.

(5) FUNCTIONAL REGULATORY AGENCY.—The term "functional regulatory agency" means any agency described in subsection (l) with respect to the financial institutions and other persons subject to the jurisdiction of such agency.

(6) HANDLED BY.—The term "handled by" includes with respect to sensitive financial personal information, any access to or generation, maintenance, servicing, or ownership of such information, as well as any transfer to or allowed access to or similar sharing or servicing of such information by or with a third party on a consumer reporter's behalf.

(7) NATIONWIDE CONSUMER REPORTING AGENCY.—The term "nationwide consumer reporting agency" means—

(A) a consumer reporting agency described in section 603(p);

(B) any person who notifies the Commission that the person reasonably expects to become a consumer reporting agency described in section 603(p) within a reasonable time; and

(C) a consumer reporting agency described in section 603(w) that notifies the Commission that the person wishes to receive breach of data security notices under this section that involve information of the type maintained by such agency.

(8) NEURAL NETWORK.—The term "neural network" means an information security program that monitors financial account transactions for potential fraud, using historical patterns to analyze and identify suspicious financial account transactions.

(9) SENSITIVE FINANCIAL ACCOUNT INFORMATION.—The term "sensitive financial account information" means a financial account number of a consumer, such as a credit card number or debit card number, in combination with any required security code, access code, biometric code, password, or other personal identification information that would allow access to the financial account.

(10) SENSITIVE FINANCIAL IDENTITY INFORMATION.—The term "sensitive financial identity information" means the first and last name, the address, or the telephone number of a consumer, in combination with any of the following of the consumer:

(A) Social Security number.

(B) Driver's license number or equivalent State identification number.

(C) IRS Individual Taxpayer Identification Number.

(D) IRS Adoption Taxpayer Identification Number.

(E) The consumer's deoxyribonucleic acid profile or other unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

(11) SENSITIVE FINANCIAL PERSONAL INFORMATION.—The term "sensitive financial personal information" means any information that is sensitive financial account information, sensitive financial identity information, or both.

(12) HARM OR INCONVENIENCE.—The term "harm or inconvenience", with respect to a consumer, means financial loss to or civil or criminal penalties imposed on the consumer or the need for the consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by consumer reporting agencies, financial institutions, or government entities, in order to avoid the risk of financial loss or increased costs or civil or criminal penalties.

(n) RELATION TO STATE LAWS.—

(1) IN GENERAL.—No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any consumer reporter or the functional equivalent of such responsibilities—

(A) to protect the security or confidentiality of information on consumers maintained by or on behalf of the person;

(B) to safeguard such information from potential misuse;

(C) to investigate or provide notices of any unauthorized access to information concerning the consumer, or the potential misuse of such information, for fraudulent purposes;

(D) to mitigate any loss or harm resulting from such unauthorized access or misuse; or

(E) involving restricting credit reports from being provided, or imposing any requirement on such provision, for a permissible purpose pursuant to section 604, such as—

(i) the responsibilities of a consumer reporting agency to honor a request, or withdrawal of such a request, to

prohibit the consumer reporting agency from releasing any type of information from the file of a consumer;

(ii) the process by which such a request or withdrawal of such a request is made, honored, or denied;

(iii) any notice that is required to be provided to the consumer in connection with such a request or withdrawal of such a request; or

(iv) the ability of a consumer reporting agency to update or change information in a consumer's file as a result of such a request or withdrawal of such a request; or

(v) the responsibilities of third parties if information from a consumer's file is unavailable as a result of such a request.

(2) EXCEPTION FOR CERTAIN STATE LAWS.—Paragraph (1) shall not apply with respect to—

(A) State laws governing professional confidentiality; or

(B) State privacy laws limiting the purposes for which information may be disclosed.

(3) EXCEPTION FOR CERTAIN COVERED ENTITIES.—Paragraph (1) shall not apply with respect to the entities described in subsection (l)(1)(G) to the extent that such entities are acting in accordance with subsection (k)(4)(G) in a manner that is consistent with this section and the implementation of this section by the regulators described in subsection (k)(1).

CREDIT REPAIR ORGANIZATIONS ACT

TITLE IV—CREDIT REPAIR ORGANIZATIONS

* * * * * * *

SEC. 401. SHORT TITLE.

This title may be cited as the "Credit Repair Organizations Act".

* * * * * * *

SEC. 403. DEFINITIONS.

[For purposes of this title] *(a) IN GENERAL.—For purposes of this title*, the following definitions apply:

(1) * * *

* * * * * * *

(3) CREDIT REPAIR ORGANIZATION.—The term "credit repair organization"—

(A) * * *

(B) does not include—

(i) any nonprofit organization which is exempt from taxation under section 501(c)(3) of the Internal Revenue Code of 1986 *and is not for its own profit or for that of its members*;

* * * * * * *

(b) CLARIFICATION WITH RESPECT TO CERTAIN CREDIT MONITORING SERVICES UNDER CERTAIN CIRCUMSTANCES.—

(1) IN GENERAL.—Subject to paragraph (2)—

(A) the provision of, or provision of access to, credit reports, credit monitoring notifications, credit scores and scoring algorithms, and other credit score-related tools to a consumer (including generation of projections and forecasts of such consumer's potential credit scores under various prospective trends or hypothetical or alternative scenarios);

(B) any analysis, evaluation, and explanation of such actual or hypothetical credit scores, or any similar projections, forecasts, analyses, evaluations or explanations; or

(C) in conjunction with offering any of the services described in subparagraph (A) or (B), the provision of materials or services to assist a consumer who is a victim of identity theft,

shall not be treated as activities described in clause (i) of subsection (a)(3)(A).

(2) CONDITIONS FOR APPLICATION OF PARAGRAPH (1).—Paragraph (1) shall apply with respect to any person engaging in any activity described in such paragraph only if—

(A) the person does not represent, expressly or by implication, that such person—

(i) will or can modify or remove, or assist the consumer in modifying or removing, adverse information that is accurate and not obsolete in the consumer's credit report; or

(ii) will or can alter, or assist the consumer in altering, the consumer's identification to prevent the display of the consumer's credit record, history, or rating for the purpose of concealing adverse information that is accurate and not obsolete;

(B) in any case in which the person represents, expressly or by implication, that it will or can modify or remove, or assist the consumer in modifying or removing, any information in the consumer's credit report, except for a representation with respect to any requirement imposed on the person under section 611 or 623(b) of the Fair Credit Reporting Act, the person discloses, clearly and conspicuously, before the consumer pays or agrees to pay any money or other valuable consideration to such person, whichever occurs first, the following statement:

"NOTICE: Neither you nor anyone else has the right to have accurate and current information removed from your credit report. If information in your report is inaccurate, you have the right to dispute it by contacting the credit bureau directly.'";

(C) the person provides the consumer in writing with the following statement before any contract or agreement between the consumer and the person is executed:

"Your Rights Concerning Your Consumer Credit File

"You have a right to obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies. To request your free annual credit report, you may go to www.annualcreditreport.com, or call 877–322–8228, or complete the Annual Credit Report Request Form and

mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348–5281. You can obtain additional copies of your credit report from a credit bureau, for which you may be charged a reasonable fee. There is no fee, however, if you have been turned down for credit, employment, insurance, or a rental dwelling because of information in your credit report within the preceding 60 days. The credit bureau must provide someone to help you interpret the information in your credit file. You are entitled to receive a free copy of your credit report if you are unemployed and intend to apply for employment in the next 60 days, if you are a recipient of public welfare assistance, or if you have reason to believe that there is inaccurate information in your credit report due to fraud.

"You have the right to cancel your contract with a credit monitoring service without fee or penalty at any time, and in the case in which you have prepaid for a credit monitoring service, you are entitled to a pro rata refund for the remaining term of the credit monitoring service.

"The Federal Trade Commission regulates credit bureaus and credit monitoring services. For more information contact:

"Federal Trade Commission
"Washington, D.C. 20580
"1–877–FTC-HELP
"www.ftc.gov"; and

(D) in any case in which the person offers a subscription to a credit file monitoring program to a consumer, the consumer may cancel the subscription at any time upon written notice to the person without penalty or fee for such cancellation and, in any case in which the consumer is billed for the subscription on other than a monthly basis, within 60 days of receipt of the consumer's notice of cancellation, the person shall make a pro rata refund to the consumer of a subscription fee prepaid by the consumer, calculated from the date that the person receives the consumer's notice of cancellation until the end of the subscription period.

* * * * * * *

SEC. 405. DISCLOSURES.

(a) DISCLOSURE REQUIRED.—Any credit repair organization shall provide any consumer with the following written statement before any contract or agreement between the consumer and the credit repair organization is executed:

"Consumer Credit File Rights Under State and Federal Law

["You have a right to dispute inaccurate information in your credit report by contacting the credit bureau directly. However, neither you nor any "credit repair" company or credit repair organization has the right to have accurate, current, and verifiable informa-

tion removed from your credit report. The credit bureau must remove accurate, negative information from your report only if it is over 7 years old. Bankruptcy information can be reported for 10 years.

[“You have a right to obtain a copy of your credit report from a credit bureau. You may be charged a reasonable fee. There is no fee, however, if you have been turned down for credit, employment, insurance, or a rental dwelling because of information in your credit report within the preceding 60 days. The credit bureau must provide someone to help you interpret the information in your credit file. You are entitled to receive a free copy of your credit report if you are unemployed and intend to apply for employment in the next 60 days, if you are a recipient of public welfare assistance, or if you have reason to believe that there is inaccurate information in your credit report due to fraud.

[“You have a right to sue a credit repair organization that violates the Credit Repair Organization Act. This law prohibits deceptive practices by credit repair organizations.

[“You have the right to cancel your contract with any credit repair organization for any reason within 3 business days from the date you signed it.

[“Credit bureaus are required to follow reasonable procedures to ensure that the information they report is accurate. However, mistakes may occur.

[“You may, on your own, notify a credit bureau in writing that you dispute the accuracy of information in your credit file. The credit bureau must then reinvestigate and modify or remove inaccurate or incomplete information. The credit bureau may not charge any fee for this service. Any pertinent information and copies of all documents you have concerning an error should be given to the credit bureau.

[“If the credit bureau’s reinvestigation does not resolve the dispute to your satisfaction, you may send a brief statement to the credit bureau, to be kept in your file, explaining why you think the record is inaccurate. The credit bureau must include a summary of your statement about disputed information with any report it issues about you.

[“The Federal Trade Commission regulates credit bureaus and credit repair organizations. For more information contact:

[“The Public Reference Branch

[“Federal Trade Commission

[“Washington, D.C. 20580”.]

“You have a right to dispute inaccurate information in your credit report by contacting the credit bureau directly. However, neither you nor any ‘credit repair’ company or credit repair organization has the right to have accurate, current, and verifiable information removed from your credit report. The credit bureau must remove accurate, negative information from your report only if it is over 7 years old. Bankruptcy information can be reported for 10 years.

“You have a right to obtain a free copy of your credit report once every 12 months from each of the nationwide consumer re-

porting agencies. To request your free annual credit report, you may go to www.annualcreditreport.com, or call 877–322–8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348–5281. You can obtain additional copies of your credit report from a credit bureau, for which you may be charged a reasonable fee. There is no fee, however, if you have been turned down for credit, employment, insurance, or a rental dwelling because of information in your credit report within the preceding 60 days. The credit bureau must provide someone to help you interpret the information in your credit file. You are entitled to receive a free copy of your credit report if you are unemployed and intend to apply for employment in the next 60 days, if you are a recipient of public welfare assistance, or if you have reason to believe that there is inaccurate information in your credit report due to fraud.

"You have a right to sue a credit repair organization that violates the Credit Repair Organization Act. This law prohibits deceptive practices by credit repair organizations.

"You have the right to cancel your contract with any credit repair organization for any reason within 3 business days from the date you signed it.

"Credit bureaus are required to follow reasonable procedures to ensure that the information they report is accurate. However, mistakes may occur.

"You may, on your own, notify a credit bureau in writing that you dispute the accuracy of information in your credit file. The credit bureau must then reinvestigate and modify or remove inaccurate or incomplete information. The credit bureau may not charge any fee for this service. Any pertinent information and copies of all documents you have concerning an error should be given to the credit bureau.

"If the credit bureau's reinvestigation does not resolve the dispute to your satisfaction, you may send a brief statement to the credit bureau, to be kept in your file, explaining why you think the record is inaccurate. The credit bureau must include a summary of your statement about disputed information with any report it issues about you.

"The Federal Trade Commission regulates credit bureaus and credit repair organizations. For more information contact:

"Federal Trade Commission
"Washington, D.C. 20580
"1–877–FTC-HELP
"(877 382–4357)
"www.ftc.gov".

* * * * * * *

DISSENTING VIEWS

H.R. 3997, the Financial Data Protection Act, is neither a constitutional nor an effective solution to the problems surrounding data security. In fact, H.R. 3997 may provide consumers with a lower level of protection than they could obtain in the market. H.R. 3997 also imposes newcosts on small businesses that could deprive consumers of desired goods and services. Finally, but most importantly, H.R. 3997 exceeds the constitutional limits on Congress's power by dictating data security standards and procedures for every business in the nation and by preempting states' data security laws related to data security.

H.R. 3997 mandates that every business in the nation maintain "reasonable policies and procedures" to protect the security and confidentiality of its data. The bill also requires all businesses to notify consumers of data breaches that cause "substantial harm or inconvenience" to consumers.

The drafters of H.R. 3997 believe that federal bureaucrats can craft regulations defining "reasonable polices" and "sustainable harm" that will be both easily adaptable by every business and satisfy every consumer's demand for security. However, the authors of H.R. 3997 overlooked the fact that views differ regarding what is a "reasonable" policy or a "substantial" harm. Some consumers who have a higher tolerance of risk than others are willing to accept a greater chance of a data breach in exchange for other benefits, such as lower prices. Other consumers are willing to forgo certain benefits in exchange for greater protection than H.R. 3997 provides.

Businesses have different definitions of "reasonable." What is "reasonable" security for Wal-Mart or amazon.com may be too costly for a small "mom-and-pop" business. Thus, by imposing a one-size-fits-all model on the country, H.R. 3997 will make it cost prohibitive for some businesses to compete in certain markets. Driving businesses out the market ultimately harms consumers who are deprived of goods and services.

If Congress allowed the market to operate, consumers would have the ability to demand the amount, and type, of data protection that suits their needs, and businesses could use their data security policies as a means of attracting consumers. Each consumer could then pick the business that offers the combination of price, security, and other services that meets the individual's unique needs. Once a federal standard is imposed, most businesses will not devote time and effort to creating their own data security policies, especially considering it would violate federal law to adopt policies that conflict in any way with H.R. 3997 would be a violation of federal law.

Similarly, H.R. 3997's preemption of state laws prohibits states from developing innovative ways to help consumers harmed by negligent failure to adequately protect their data. Proponents of H.R.

3997 claim that the differences among states' laws cause hardships on businesses and consumers that justify the federal government pre-empting state laws and imposing a one-size-fits-all regulatory framework. However, there are two flaws with this argument. First, differences among states' regulations in no way justify violating the Tenth Amendment prohibition on Congress legislating on issues, such as consumer protection, not explicitly placed under congressional jurisdiction in Article I, Section 8. In fact, one of the Founders' purposes in preserving state autonomy was to foster diversity among states' laws so the states can experiment to determine what laws best promote their citizens' interests.

Second, states and businesses are quite capable of developing uniform standards without being forced to do so by the federal government. For example, the Uniform Commercial Code, which governs commercial contracts in most states, was drawn up by private attorneys and voluntarily adopted by the states. Similarly, many states have adopted the model law governing corporations without prodding from Congress. "Model laws" reflecting the experiences of the states and the people with a diversity of laws and regulations are bound to be superior to laws Washington imposes.

H.R. 3997 appears on its surface to be a pro-consumer bill. However, it actually makes it more difficult, if not impossible, for consumers to obtain the data services they need or desire. H.R. 3997 also imposes costs on small business that will deprive consumers of desired goods and services. However, the main reason my colleagues should reject this bill is that Congress has no constitutional authority to dictate to every business in the nation the manner of protecting data security. Furthermore, the provisions of this bill pre-empting state laws blatantly violate the Tenth Amendment. I, therefore, urge my colleagues to reject this bill.

RON PAUL.

DISSENTING VIEWS OF HON. BARNEY FRANK

Unfortunately this legislation is not strong enough to justify its preemption of state law. Although the reported bill is an improvement over the earlier drafts, and now includes a better "trigger" provision for notifying consumers when their data is lost or stolen and safeguards the Gramm-Leach-Bliley Act, the bill is undermined by weak enforcement and federal preemption.

Rather than restricting enforcement only to narrow functional regulators whose resources are often utilized pursuing other goals (e.g., safety and soundness), our system would be much better served if entities closer to our citizens were not prohibited by Congress from protecting them. State Attorneys General, in particular, have played a valuable consumer protection role and should not be pushed aside in this important area.

The bill is similarly weak with regard to consumers' ability to "freeze" their consumer report information (particularly by limiting this ability to individuals who have already been the victim of identity theft). This weakness could be addressed either by establishing a stronger federal freeze law that gives all consumers the right to place a freeze on their consumer report information or by permitting the states to enact stronger laws on this topic. Unfortunately the bill does neither. Instead, it establishes a low federal standard and makes that standard a ceiling above which states cannot go.

Freezes are a potentially important tool that consumers can use to protect themselves before they become the victim of identity theft. It is particularly valuable for at-risk consumers, like the very young or old, who may not want new credit for long periods and do not monitor their credit reports regularly. It is a profound mistake to create a weak law and preempt states from improving it.

Although some proponents of the bill's weak standard contend that freezing a credit file is not in the consumer's interest (e.g., because the consumer will need to take more steps should they desire new/instant credit), the large minority of the Committee that voted against preemption here reject that argument. Consumers are routinely trusted to make far more dangerous decisions about their finances than whether to place a freeze on their consumer report information. Congress never stands in the way of a consumer making a bad purchase or engaging in a complicated, high-risk transaction. It does not prohibit consumers from risking their homes by refinancing with a variable-rate interest-only loan laden with penalties

and fees. Yet, in this case, when faced with the possibility that states might give consumers the choice to protect themselves by temporarily turning the credit spigot off before they are the victim of identity theft, this Committee steps in to pass a law to prohibit it.

BARNEY FRANK.

○