

109TH CONGRESS
1ST SESSION

H. R. 3374

To provide for the uniform and timely notification of consumers whose sensitive financial personal information has been placed at risk by a breach of data security, to enhance data security safeguards, to provide appropriate consumer mitigation services, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 21, 2005

Mr. LATOURETTE (for himself and Ms. HOOLEY) introduced the following bill;
which was referred to the Committee on Financial Services

A BILL

To provide for the uniform and timely notification of consumers whose sensitive financial personal information has been placed at risk by a breach of data security, to enhance data security safeguards, to provide appropriate consumer mitigation services, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Consumer Notification
5 and Financial Data Protection Act of 2005”.

1 **SEC. 2. DATA SECURITY SAFEGUARDS.**

2 Each financial institution shall have an affirmative
3 and continuing obligation to maintain reasonable policies
4 and procedures to protect the security and confidentiality
5 of sensitive financial personal information of any con-
6 sumer that is maintained or received by or on behalf of
7 such financial institution against any unauthorized use
8 that is reasonably likely to result in harm or substantial
9 inconvenience to such consumer.

10 **SEC. 3. INVESTIGATION AND NOTICE TO REGULATORS AND**
11 **LAW ENFORCEMENT IN CASE OF BREACH OF**
12 **DATA SECURITY.**

13 (a) DUTY TO INVESTIGATE.—

14 (1) IN GENERAL.—Whenever any financial in-
15 stitution determines or becomes aware of informa-
16 tion that would reasonably indicate that a breach of
17 data security may have occurred or is reasonably
18 likely to occur, or receives notice under subsection
19 (c), the financial institution shall immediately con-
20 duct a reasonable investigation to—

21 (A) assess the nature and scope of the
22 breach;

23 (B) identify the sensitive financial personal
24 information involved; and

25 (C) determine if the breach is reasonably
26 likely to result in harm or substantial inconven-

1 ience to any consumer to whom the information
2 relates.

3 (2) FACTORS TO BE CONSIDERED.—In deter-
4 mining, under paragraph (1), the likelihood that
5 harm or substantial inconvenience may be caused to
6 consumers, the financial institution shall consider all
7 available relevant facts, including whether the infor-
8 mation that was subject to the breach was
9 unencrypted, or unredacted, or required technology
10 to use that is not generally commercially available.

11 (b) INVESTIGATION NOTICES.—If a financial institu-
12 tion determines after commencing an investigation under
13 subsection (a) that a potential breach of data security may
14 result in harm or substantial inconvenience to any con-
15 sumer whose sensitive financial personal information was
16 involved in such potential breach, the financial institution
17 shall—

18 (1) promptly notify the appropriate law enforce-
19 ment agencies of the breach;

20 (2) promptly notify the institution’s functional
21 regulator;

22 (3) take reasonable measures to ensure and re-
23 store the security and confidentiality of the sensitive
24 financial personal information involved in the
25 breach;

1 (4) take reasonable measures to prevent further
2 unauthorized access to or disclosure of any sensitive
3 financial personal information and to restore the in-
4 tegrity of the data system; and

5 (5) notify as appropriate and without unreason-
6 able delay all critical third parties—

7 (A) whose involvement is necessary to in-
8 vestigate the breach of data security; or

9 (B) who will be required to undertake fur-
10 ther action with respect to such information to
11 protect such consumers from fraud or identity
12 theft.

13 (c) DUTY OF FINANCIAL CONTRACTORS.—Whenever
14 any financial institution that maintains or receives sen-
15 sitive personal financial information for or on behalf of
16 another party determines, or has reason to believe, that
17 a breach of data security has occurred with respect to such
18 information, the financial institution shall—

19 (1) promptly notify the other party of the
20 breach;

21 (2) conduct a joint investigation with the other
22 party to determine the likelihood that such informa-
23 tion will be misused against the consumers to whom
24 the information relates in a manner that would

1 cause harm or substantial inconvenience to such con-
2 sumer; and

3 (3) unless the financial institution and third
4 party determine, after conducting a reasonable in-
5 vestigation, that it is not reasonably likely that such
6 information will be misused to commit financial
7 fraud against any consumer to whom any of such
8 sensitive financial personal information relates in a
9 manner that would cause harm or substantial incon-
10 venience to such consumer, provide joint notice
11 under section 4 to such consumers.

12 **SEC. 4. NOTICE TO CONSUMERS OF DATA SECURITY**
13 **BREACH.**

14 (a) NOTICE REQUIRED.—If, after completing a rea-
15 sonable investigation pursuant to section 3, a financial in-
16 stitution or a financial contractor pursuant to section 3(c)
17 becomes aware that a breach of data security is reasonably
18 likely to have occurred, with respect to sensitive financial
19 personal information maintained or received by or on be-
20 half of the institution, that creates a risk of harm or sub-
21 stantial inconvenience to consumers to whom the informa-
22 tion relates, the financial institution shall, without unrea-
23 sonable delay—

24 (1) provide written notice, in accordance with
25 this section, to each consumer whose sensitive finan-

1 cial personal information was involved in the breach
2 of data security; and

3 (2) if the financial institution determines that it
4 is likely to be providing notice under paragraph (1)
5 to 1,000 or more consumers for any breach of data
6 security, provide written notice to—

7 (A) each consumer reporting agency de-
8 scribed in section 603(p) of the Fair Credit Re-
9 porting Act; and

10 (B) any other consumer reporting agency
11 that the financial institution identifies, or ex-
12 pects to identify, in the notice provided to the
13 consumer under paragraph (1).

14 (b) CONTENT OF NOTICE.—The notice provided to
15 any consumer under subsection (a)(1) shall include the
16 following information in a clear and conspicuous manner:

17 (1) A description of the nature and type of in-
18 formation that was, or is reasonably believed to have
19 been, subject to the breach of data security.

20 (2) If known, the date, or a reasonable approxi-
21 mation of the period of time, on or within which sen-
22 sitive financial personal information of the consumer
23 was, or is reasonably believed to have been, acquired
24 by an unauthorized person.

1 (3) A description of the actions taken by the fi-
2 nancial institution to restore the security and con-
3 fidentiality of the data.

4 (4) A toll-free telephone number where a con-
5 sumer whose information was subject of the breach
6 of data security may obtain additional information
7 the breach of data security.

8 (5) A summary of rights of consumer victims of
9 fraud or identity theft, such as that prepared by the
10 Federal Trade Commission under section 609(d) of
11 the Fair Credit Reporting Act, including any addi-
12 tional appropriate information on how the consumer
13 may—

14 (A) obtain a copy of a consumer report
15 free of charge in accordance with section 612 of
16 the Fair Credit Reporting Act;

17 (B) place a fraud alert in any file relating
18 to the consumer at a consumer reporting agen-
19 cy under section 605A of such Act to discour-
20 age unauthorized use; and

21 (C) contact the Federal Trade Commission
22 for more detailed information.

23 (c) NOTICE OF IDENTITY THEFT.—If a financial in-
24 stitution is required to provide a notice under subsection
25 (a)(1) with respect to a breach of data security involving

1 sensitive financial personal information relating to a con-
2 sumer (other than financial account information described
3 in section 9(5)(A)(v)), the notice required in this section
4 with respect to such consumer shall include information
5 on how the consumer may obtain mitigation services free
6 of charge in accordance with section 5.

7 (d) DELAY OF NOTICE FOR LAW ENFORCEMENT
8 PURPOSES.—If a financial institution receives a written
9 request, or an oral request indicating that a written re-
10 quest will be provided, from an appropriate law enforce-
11 ment agency indicating that providing a particular notice
12 to any consumer under this section would impede a crimi-
13 nal or civil investigation by that law enforcement agency,
14 the financial institution shall delay, or in the case of a
15 foreign law enforcement agency may delay, providing such
16 notice until the law enforcement agency informs the finan-
17 cial institution that such notice will no longer impede the
18 investigation or the law enforcement agency fails to con-
19 firm that a continued delay is necessary to avoid impeding
20 such investigation.

21 (e) ELECTRONIC TRANSMISSION OF NOTICE.—The
22 written notice required under this section to any consumer
23 may be made by an electronic transmission only if—

1 (1) the consumer has provided prior consent to
2 receive any such notice by electronic transmission;
3 and

4 (2) the notice is consistent with the provisions
5 permitting electronic transmission of notices under
6 section 101 of the Electronic Signatures in Global
7 and National Commerce Act.

8 **SEC. 5. MITIGATION PROCEDURES.**

9 (a) **FREE FILE MONITORING.**—Any financial institu-
10 tion that is required to provide notice to a consumer under
11 section 4(a)(1) with respect to a breach of data security
12 described in section 4(c) shall, if requested by the con-
13 sumer before the end of the 90-day period beginning on
14 the date of such notice, make available to the consumer,
15 free of charge and for a 12-month period, a service that
16 monitors nationwide credit activity regarding the con-
17 sumer from a consumer reporting agency described in sec-
18 tion 603(p) of the Fair Credit Reporting Act.

19 (b) **JOINT RULEMAKING FOR SAFE HARBOR.**—The
20 Federal Trade Commission, in consultation with the regu-
21 latory agencies described in section 8, shall develop regula-
22 tions, which shall be prescribed by all functional regu-
23 latory agencies, that, in any case in which—

24 (1) free file monitoring is offered under sub-
25 section (a) to a consumer;

1 (2) subsequent to the offer, another party mis-
2 uses sensitive financial identity information on the
3 consumer obtained through the breach of data secu-
4 rity (that gave rise to such offer) to commit identity
5 theft against the consumer; and

6 (3) at the time of such breach the financial in-
7 stitution maintained reasonable policies and proce-
8 dures to comply with subsection (a),
9 exempts the financial institution from any liability under
10 State common law for any loss or harm to the consumer
11 occurring after the end of a reasonable period beginning
12 on the date of such offer, other than any direct pecuniary
13 loss provided under such law, resulting from such misuse.

14 **SEC. 6. PROPER DISPOSAL OF PERSONAL INFORMATION.**

15 (a) IN GENERAL.—Before the end of the 6-month pe-
16 riod beginning on the date of the enactment of this Act,
17 the Federal Trade Commission shall prescribe regulations
18 in final form requiring any financial institution which
19 maintains or otherwise possesses sensitive financial per-
20 sonal information, or any compilation of such information,
21 for a business purpose to properly dispose of any such in-
22 formation or compilation so that such information or com-
23 pilation cannot practicably be read or reconstructed.

24 (b) RULE OF CONSTRUCTION.—No provision of this
25 section shall be construed—

1 (1) as requiring, or authorizing the Federal
2 Trade Commission to require, any person to main-
3 tain or destroy any sensitive financial personal infor-
4 mation that is not required to be maintained or de-
5 stroyed under any other provision of Federal or
6 State law; or

7 (2) as altering or affecting any requirement im-
8 posed under any other provision of Federal or State
9 law to maintain or destroy sensitive financial per-
10 sonal information.

11 **SEC. 7. RELATION TO STATE LAW.**

12 The provisions of this Act shall supersede any law,
13 rule, or regulation of any State or political subdivision of
14 any State that relates in any way to—

15 (1) information security standards of financial
16 institutions; or

17 (2) the notification of consumers by financial
18 institutions with respect to any breach of the con-
19 fidentiality or security of information maintained or
20 received by or on behalf of the financial institutions.

21 **SEC. 8. ADMINISTRATIVE ENFORCEMENT.**

22 This Act and any regulation prescribed under this
23 Act shall be enforced with respect to financial institutions
24 and other persons to which this Act applies exclusively by
25 the functional financial regulators, and by the chief law

1 enforcement officer of a State, or an official or agency des-
2 igned by a State (with respect to persons within the ju-
3 risdiction of such officer, official, or agency), as follows:

4 (1) Under section 8 of the Federal Deposit In-
5 surance Act, in the case of—

6 (A) national banks, Federal branches and
7 Federal agencies of foreign banks, and any sub-
8 sidiaries of such entities (except brokers, deal-
9 ers, persons providing insurance, investment
10 companies, and investment advisers), by the
11 Comptroller of the Currency;

12 (B) member banks of the Federal Reserve
13 System (other than national banks), branches
14 and agencies of foreign banks (other than Fed-
15 eral branches, Federal agencies, and insured
16 State branches of foreign banks), commercial
17 lending companies owned or controlled by for-
18 eign banks, organizations operating under sec-
19 tion 25 or 25A of the Federal Reserve Act, and
20 bank holding companies and their nonbank sub-
21 sidiaries or affiliates (except brokers, dealers,
22 persons providing insurance, investment compa-
23 nies, and investment advisers), by the Board of
24 Governors of the Federal Reserve System;

1 (C) banks insured by the Federal Deposit
2 Insurance Corporation (other than members of
3 the Federal Reserve System), insured State
4 branches of foreign banks, and any subsidiaries
5 of such entities (except brokers, dealers, per-
6 sons providing insurance, investment compa-
7 nies, and investment advisers), by the Board of
8 Directors of the Federal Deposit Insurance Cor-
9 poration; and

10 (D) savings associations the deposits of
11 which are insured by the Federal Deposit In-
12 surance Corporation, and any subsidiaries of
13 such savings associations (except brokers, deal-
14 ers, persons providing insurance, investment
15 companies, and investment advisers), by the Di-
16 rector of the Office of Thrift Supervision.

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

21 (3) Under the Securities Exchange Act of 1934,
22 by the Securities and Exchange Commission with re-
23 spect to any broker or dealer.

1 (4) Under the Investment Company Act of
2 1940, by the Securities and Exchange Commission
3 with respect to investment companies.

4 (5) Under the Investment Advisers Act of 1940,
5 by the Securities and Exchange Commission with re-
6 spect to investment advisers registered with the
7 Commission under such Act.

8 (6) Under State insurance law, in the case of
9 any person engaged in the business of insurance, by
10 the applicable State insurance authority of the State
11 in which the person is domiciled.

12 (7) Under the Federal Trade Commission Act,
13 by the Federal Trade Commission for any other per-
14 son that is not subject to the jurisdiction of any
15 agency or authority under paragraphs (1) through
16 (6) of this subsection.

17 **SEC. 9. DEFINITIONS.**

18 For purposes of this Act, the following definitions
19 shall apply:

20 (1) **BREACH OF DATA SECURITY.**—The term
21 “breach of data security” means, with respect to
22 sensitive financial personal information that is main-
23 tained, received, or communicated by or on behalf of
24 any financial institution—

1 (A) an unauthorized acquisition of such in-
2 formation that could be used to commit finan-
3 cial fraud; or

4 (B) an unusual pattern of misuse of such
5 information to commit financial fraud.

6 (2) CONSUMER.—The term “consumer” means
7 an individual.

8 (3) FINANCIAL INSTITUTION.—The term “fi-
9 nancial institution” means—

10 (A) any person the business of which is en-
11 gaging in activities that are financial in nature
12 as described in or determined under section
13 4(k) of the Bank Holding Company Act;

14 (B) any entity that is primarily engaged in
15 activities that are subject to the Fair Credit Re-
16 porting Act; and

17 (C) any person that is maintaining, receiv-
18 ing, or communicating sensitive financial per-
19 sonal information on an ongoing basis for the
20 purposes of engaging in interstate commerce.

21 (4) FUNCTIONAL FINANCIAL REGULATOR.—The
22 term “functional financial regulator”—

23 (A) has the same meaning as in section
24 509(2) of the Gramm-Leach-Bliley Act; and

1 (B) in the case of any financial institution
2 that is described in paragraph (3)(B) that is
3 not subject to the Gramm-Leach-Bliley Act, in-
4 cludes the appropriate regulator for such finan-
5 cial institution under section 621 of the Fair
6 Credit Reporting Act.

7 (5) SENSITIVE FINANCIAL PERSONAL INFORMA-
8 TION.—

9 (A) IN GENERAL.—The term “sensitive fi-
10 nancial personal information” means informa-
11 tion that is personal, sensitive, and nonpublic
12 and contains an individual’s first and last name
13 and either the individual’s address or telephone
14 number and appears in combination with any of
15 the following:

16 (i) Social Security number.

17 (ii) Driver’s license number or an
18 equivalent State-issued identification num-
19 ber.

20 (iii) Taxpayer identification number.

21 (iv) Any credit card or debit card ac-
22 count number.

23 (v) Any bank, savings association,
24 credit union, or investment account num-
25 ber, other than an account number de-

1 scribed in clause (iv), in combination with
2 any required security code, biometric code,
3 password, or other means that would per-
4 mit access to a consumer’s financial ac-
5 count.

6 (B) EXCLUSIONS.—The term “sensitive fi-
7 nancial personal information” shall not in-
8 clude—

9 (i) any list, description or other
10 grouping of individuals (and publicly avail-
11 able information pertaining to them) that
12 is derived without using any sensitive per-
13 sonal information; or

14 (ii) publicly available information that
15 is lawfully made available to the general
16 public from Federal, State or local govern-
17 ment records.

○