AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 109–453
Part 3

FINANCIAL DATA PROTECTION ACT OF 2006

JUNE 2, 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. 4127]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the bill (H.R. 4127) to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach, having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

CONTENTS

	Page
Amendment	2
Purpose and Summary	2
Background and Need for Legislation	3
Hearings	3
Committee Consideration	3
Committee Votes	3
Committee Oversight Findings	3
Performance Goals and Objectives	3
New Budget Authority, Entitlement Authority, and Tax Expenditures	3
Committee Cost Estimate	4
Congressional Budget Office Estimate	4
Federal Mandates Statement	9
Advisory Committee Statement	9
Constitutional Authority Statement	9
Applicability to Legislative Branch	9
Section-by-Section Analysis of the Legislation	9
Changes in Existing Law Made by the Bill, as Reported	10

49–006

Dissenting Views 11

AMENDMENT

The amendments are as follows:

Strike all after the enacting clause and insert the text of H.R. 3997, as reported by the Committee on Financial Services.

Amend the title so as to read:

A bill to amend the Fair Credit Reporting Act to provide for secure financial data, and for other purposes.

For the full text of the amendment in the nature of a substitute adopted to H.R. 4127, see House Report 109–454, Part 1, on H.R. 3997, the Financial Data Protection Act of 2006.

PURPOSE AND SUMMARY

H.R. 4127, as referred to the Committee on Financial Services and as reported with the text of H.R. 3997, the Financial Data Protection Act, builds off of the data safeguards requirements and regulations of the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA). It requires certain entities that possess or maintain sensitive information about consumers to keep the information secure, investigate breaches of the information, and notify consumers of data security breaches.

As amended, H.R. 4127 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.

Notwithstanding the effective date in section 2(c), the requirements of H.R. 4127 shall apply immediately to any Executive agency (as defined in section 105 of title 5, United States Code), including the Veterans Administration, that determines on or after January 1, 2006, that a breach of data security has occurred, is likely to have occurred, or is unavoidable. Such requirements shall include the provisions relating to free credit monitoring, prompt notice to consumers, and data security safeguards as practicable, notwithstanding that the agency made its determination before the date of the enactment of this Act. Any relevant time periods contained in section 630 of the Fair Credit Reporting Act shall be applied with respect to any Executive agency to which such section is applicable as if the determination of the agency were made on the date of the enactment of this Act.

BACKGROUND AND NEED FOR LEGISLATION

For further background information on H.R. 4127, see House Report 109–454, Part 1, on H.R. 3997, the Financial Data Protection Act of 2006.

HEARINGS

No hearings were held on H.R. 4127 by the Committee on Financial Services.

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on May 24, 2006, and ordered H.R. 4127 reported to the House as amended by a voice vote.

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. No record votes were taken with in conjunction with the consideration of this legislation. A motion by Mr. Oxley to report the bill to the House as amended with a favorable recommendation was agreed to by a voice vote. During the consideration of the bill, the following amendments were considered:

An amendment in the nature of a substitute offered by Mr. Bachus, No. 1, consisting of the text of H.R. 3997 as reported by the Committee on Financial Services, was agreed to by a voice vote.

An amendment offered by Ms. Hooley, No. 1(a), regarding the Veterans Administration data breach scope of application, was offered and withdrawn.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held hearings 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:

As amended, H.R. 4127, 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:

MAY 26, 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. 4127, 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 are Melissa Z. Petersen (for federal costs), Sarah Puro (for state and local costs), and Page Piper/Bach (for the impact on the private sector).

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 4127—Financial Data Protection Act of 2006

Summary: H.R. 4127 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. 4127 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. 4127 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. 4127 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. 4127 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. 4127 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. 4127 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. 4127 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. 4127 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. 4127 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 (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 by the FTC, CBO estimates that implementing H.R. 4127 would cost less than $500,000 in 2006 and $5 million over the 2006–2011 period for the 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. 4127 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. 4127 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 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. 4127 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. 4127 would reduce revenues by less than $500,000 a year.

Enacting H.R. 4127 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. 4127 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 information from state and local governments and a review of current legal precedents, CBO expects 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. 4127 would impose private-sector mandates, as defined in UMRA, on financial institu-

tions, 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 sensitive 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, certain mandates in H.R. 4127 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 UMRA 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 he 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 award 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 monitoring. 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 or 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: CBO has provided cost estimates for six pieces of legislation that deal with identity theft or the safeguarding of personal information. Some have different provisions, but all of the pieces of legislation would require private companies and the government to take certain precautions to safeguard personal information. The cost estimates reflect those differences.

• On May 26, 2006, CBO transmitted a cost estimate for H.R. 3997, the Data Accountability and Trust Act (DATA), as ordered reported by the House Committee on Energy and Commerce on May 24, 2006.

• On April 19, 2006, CBO transmitted a cost estimate for S. 1789, the Personal Data Privacy and Security Act of 2005, as reported by the Senate Committee on the Judiciary on November 17, 2005.

• On April 6, 2006, CBO transmitted a cost estimate for H.R. 4127, the Data Accountability and Trust Act, as ordered reported by the House Committee on Energy and Commerce on March 29, 2006, with a subsequent amendment provided by the committee on April 4, 2006.

• On March 30, 2006, CBO transmitted a cost estimate for H.R. 3997, the Financial Data Protection Act, as ordered reported by the House Committee on Financial Services on March 16, 2006.

• On March 10, 2006, CBO transmitted a cost estimate for S. 1326, the Notification of Risk to Personal Data Act, as ordered reported by the Senate Committee on the Judiciary on October 20, 2005.

• On November 3, 2005, CBO transmitted a cost estimate for S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005.

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

For a section-by-section analysis of H.R. 4127, see House Report 109–454, Part 1, on H.R. 3997, the Financial Data Protection Act of 2006.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

The bill was referred to this commitee for consideration of such provisions of the bill and amendment as fall within the jurisdiction of this committee pursuant to clause 1(g) of rule X of the Rules of the House of Representatives. The changes made to existing law by the amendment reported by this committee are shown in the report filed on May 4, 2006 (Rept. 109–454, Part 1).

DISSENTING VIEWS OF RON PAUL

Since the version of H.R. 4127, The Data Accountability and Trust Act, reported out of this Committee, is identical to H.R. 3997, the Financial Data Protection Act, I am resubmitting my dissenting views on H.R. 3997:

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 new costs 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 policies" 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 of 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 polices 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 preempting state laws blatantly violate the Tenth Amendment. I, therefore, urge my colleagues to reject this bill.

RON PAUL.

○