39

Before the
Department of the Treasury
Washington, D.C.

In the Matter of	)	**Study on Information-sharing**
Financial Services Modernization Act or	)	**Practices Among Financial**
Gramm-Leach-Bliley Act (GLBA)	)	**Institutions and Their Affiliates**
15 USC § 1608 -- Comment	)	

TO: Regulations and Legislation Division

COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER, THE PRIVACY RIGHTS CLEARINGHOUSE, US PIRG, AND CONSUMERS UNION

May 1, 2002

Pursuant to the notice[1] and request for public comment published by the Secretary of the Department of Treasury on February 15, 2002, requesting comment on the study of information-sharing practices, mandated by 15 USC § 1608, the Electronic Privacy Information Center (EPIC), the Privacy Rights Clearinghouse (PRC), and Consumers Union submit the following comments:

TABLE OF CONTENTS

I. Introduction **3**

A. Purpose of the Study *3*

B. Risks of Weak Privacy Protection in the GLBA *4*

II. Numerous Risks to Customer Privacy Are Raised by Unfettered Information-sharing **5**

A. Unfettered Affiliate Sharing Permits Comprehensive Consumer Profiling. Resulting in Aggressive and Potentially Dangerous Target Marketing *5*

B. Permitting Unfettered Non-Affiliate Sharing Implicates Numerous Privacy Concerns Including Identity Theft, Profiling and Fraud *8*

C. The Joint Marketing Agreement Loophole is a Serious Privacy Risk Allowing Unregulated Information-sharing of the Type the GLBA was Enacted to Restrict *10*

D. Other Risks of Personal Data on the Open Market *11*

1. Identity Theft 11

[1] 67 Fed. Reg. 7213 (Feb. 15, 2002).

2. Personal Information is a Gold Mine for Criminals 12

III. Notices Under the GLBA Fail to Give Consumers Adequate Choice or Notice Necessary to Evaluate the Benefits and Harms of Information-sharing 12

IV. Existing Privacy Law—Based on an Opt-Out Standard—is Inadequate to Protect the Privacy of Customer Information 14

A. Existing Privacy Laws Do Not Protect the Privacy of Customer Information 14

1. Opt-out Frameworks Create a Financial Incentive for the Creation of Confusing Privacy Notices and Obfuscated Opt-Out Mechanisms 14
2. . Effective Choice Is Unattainable Where Broad Exceptions Exist Prohibiting an Individual's Ability to Control the Flow of Sensitive Information 15
3. There is No Privacy for Non-Customer Information 16
4. There is Inadequate Enforcement Under Current Law 16

V. Financial Institutions' Privacy Policy and Privacy Rights Disclosure Are Inadequate Under Existing Law 17

A. Financial Institution Privacy Notices Sent in Compliance with the GLBA Have Failed to Provide Consumers With Notice 17

1. Most Notices Perceived as "Junk Mail" 18
2. Notices Were Confusing and Failed to Provide Basic Information 19
3. Notices Placed an Unfair Burden on Customers to Protect their Privacy 19

B. Regulators Must Place More Stringent Standards on Financial Institutions 20

VI. Opt-In is the Only Feasible Approach to Permit Informed Customer Consent and to Permit Customers to Restrict Use of Personal Information 20

A. There is a Substantial, Protected Interest in Privacy of Personal Information 20

B. Opt-In is the Only Truly Effective Means for Protecting the Privacy Interests of Consumers 21

C. Implementing an Opt-In Approach Serves the Governmental Interest in Customer Privacy 22

VII. Conclusion 22

COMMENTS

I. Introduction

A. Purpose of the Study

The commentators appreciate the opportunity to contribute to the study. Information-sharing practices among financial institutions and individuals' loss of privacy from lack of control over use of sensitive data is a continuing topic of public attention. This study, based as it is on voluntary comments, can be expected to shed little, if any, new light on *actual* information-sharing practices within the financial services industry. However, the study has value in giving ordinary citizens—individuals affected by erosion of privacy—the opportunity to weigh-in on this important issue.

Numerous polls conducted before and during the debate that culminated in the privacy provisions of the GLBA illustrate public attitudes towards loss of privacy.[2] Public trust that a financial institution will keep confidential data private, while once high, is now tarnished. Public concern for loss of privacy was stirred by a series of highly publicized lawsuits brought by state attorneys general around the time Congress was debating legislation to overhaul the financial services industry.[3]

These cases brought to light disturbing practices that included the sale of personal data, including data used to access and charge accounts without either notice or consent of account holders. Recipients of the data, while sharing profits with the originating institution, in turn charged customer accounts through various negative-option marketing schemes.

Largely in response to the public airing of such abhorrent practices, Congress enacted Title V, Subpart A of the GLBA, Disclosure of Nonpublic Personal Information. Principles of notice and consent, universally recognized as elements of fair information practices (FIPs),[4] were incorporated to allow financial institutions to conduct business as

---

[2] *See* EPIC's Polling Data Page, http://www.epic.org/privacy/survey/default.html; New York Senate Majority Task Force on the Invasion of Privacy, Public Attitudes about the Privacy of Information, *at* http://www.privacyrights.org/ar/invasion.htm at 11-12; Beth Givens, What's Missing from this Picture? Privacy Protection in the New Millennium, at http://www.privacyrights.org/ar/naag-mill.htm; Mike Hatch, *The Privatization of Big Brother: Protection Sensitive Personal Information From Commercial Interests in the 21st Century, at* www.ag.state.mn.us/consumer/Privacy?Default.htm, at 20.

[3] Hatch v. US Bank et al, Final Judgment and Order for Injunctive and Consumer Relief (No. 99-872); *see also* Holden Lewis, *Banks are Selling Your Private Information,* http://www.bankrate.com/brm/news/bank/19991008.asp (October 08, 1999), Lori Enos, *FTC Lowers Boom on Net Porn Scammers,* http://www.ecommercetimes.com/perl/story/4233.html, (Sept. 8, 2000) (reporting FTC settlement against porn site brokers who purchased database information from Charter Pacific and used information to charge consumer credit card were charged for visits to porn sites. Many people whose account was charged didn't have a computer. The names and accounts numbers were not even necessarily Charter Pacific's customers. Many of the credit cards belonged to third-party merchants who processed transactions through their own accounts at Charter Pacific).

[4] *See, e.g.,* Privacy Rights Clearinghouse, *A Checklist of Responsible Information-Handling Practices,* http://www.privacyrights.org/fs/fs12-ih2.htm (Apr. 2001)

usual as long as customers were given notice and an opportunity to "opt-out,"—to take affirmative action to restrict information-sharing.

Under the GLBA, companies are required to provide a "clear and conspicuous" (§503 (a)) disclosure regarding a company's information-sharing practices and then consumers could make an informed choice about whether or not to allow information to be shared. Choice was based on the negative rule of "silence as consent," or "opt-out." The opt-out scheme was accepted after regulated institutions argued that opt-in was an unworkable solution that would cause intolerable economic consequences.

Now, over two years after the GLBA became law and nearly a year after the regulations implementing the GLBA took effect, public concerns over loss of privacy have intensified.[5] Last year the Minnesota attorney general made headlines when he brought a lawsuit against Fleet Mortgage for selling sensitive customer data to telemarketers.[6] In addition, the recent settlement of litigation brought by twenty-seven attorneys general against Citibank confirms that the public is justified in its continuing concern.[7] The public has had few recent concrete examples of the darker side of information-sharing practices among financial institutions because these policies are opaque and the GLBA notices are vague. However, neither case was brought under the provisions of the GLBA, a fact that in itself points out the deficiency of privacy protections in this law.

Ideally, a study such as this, mandated by Congress, with views of all interested parties solicited, would elucidate the reality of information-sharing practices within the financial services industry. However, because individuals do not have a statutory right of access to learn more about industry practices, and because the submissions from industry are voluntary, it will be challenging to assess the privacy protections of the Act.

B. Risks of Weak Privacy Protection in the GLBA

The GLBA has failed to provide the adequate protections for consumer privacy in modern financial services. Individuals face a multitude of potential risks through unrestricted and undisclosed information-sharing of personal financial data information under the GLBA. Unfettered affiliate and non-affiliate sharing permits comprehensive profiling, which results in aggressive target marketing techniques, identity theft, profiling and fraud. Consumers have not been adequately informed or been given effective choice to evaluate the benefits of information-sharing against the potential harms causes by unrestricted information-sharing.

---

[5] *See* Harris Interactive, *Privacy On and Off the Internet: What Consumers Want* (Feb. 19, 2002) *available at* http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429.

[6] *See, e.g.*, Hatch v. Fleet Mortgage, Memorandum Opinion and Order No. 01-48, (D. Minn. 2001), *available at* http://www.ag.state.mn.us/consumer/news/pr/fleet%5Fopinion%5F61901.html.

[7] Office of the Attorney General of the State of California, *Citibank Agrees to Curb Deceptive Marketing Practices by Telemarketing Vendors*, http://www.caag.state.ca.us/newsalerts/2002/02-013.htm (Feb. 27, 2002).

Opt-in is the most feasible approach to permit informed customer consent and to permit individuals to restrict use of personal information.[8] The GLBA, because it is based on an opt-out standard, is inadequate to protect the privacy of the nation's financial consumers. In an opt-out regime, effective privacy notices are contrary to industry interests. A year of vague, illusive, and unhelpful notices under the GLBA has frustrated and confused consumers while effectively highlighting the fundamental defects of opt-out regulatory standard.

II. Numerous Risks to Customer Privacy Are Raised by Unfettered Information-Sharing

Individuals face a multitude of potential risks through unrestricted and undisclosed information-sharing of personal financial data information among affiliates and non-affiliates under the GLBA.

A. Unfettered Affiliate Sharing Permits Comprehensive Consumer Profiling, Resulting in Aggressive and Potentially Dangerous Target Marketing

The GLBA allows distinct financial entities of banking, insurance and securities companies to now operate under a single corporate roof. When customer databases from these giant entitles are combined, the result is a mega database containing a vast amount of financial, medical and other sensitive information. When appended with information easily obtainable from outside sources, a comprehensive profile of each individual customer of the financial institution can be compiled with a single keystroke. Such detailed profiles are available to all affiliates to target the individual for an array of products and both financial and non-financial services.

Through the collection of "transaction and experience" information, companies are able to track information totally unrelated to the purchase of any financial service or product. For example, payments by check or credit card can reveal religious and political affiliations, use of high fat foods or alcohol, medical conditions, propensity to gamble, entertainment choices, charitable contributions and much more.[9]

The natural outgrowth of this unlimited collection and sharing of personal data is individual profiling. Profiles can be used to determine the amount one pays for financial services and products obtained from within the "financial supermarket" structure. As just one example, information about health condition or lifestyle can be used to determine interest rates for a credit card or mortgage. Even with a history of spotless credit, an

[8] An opt-in framework would better protect individuals' rights, and is consistent with most United States privacy laws. For instance, the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, the Video Privacy Protection Act, the Driver's Privacy Protection Act, and the Children's Online Privacy Protection Act all empower the individual by specifying that affirmative consent is needed before information is shared. Respectively, at 20 U.S.C. § 1232 g(b)(1), 47 U.S.C. § 551(a)(1), 18 U.S.C. § 2511(2)(c), 18 U.S.C. § 2710(b)(2)(B), 18 U.S.C. § 2721(b)(4)(13), and 15 U.S.C. § 6501(b)(1)(A)(2).

[9] *See* Robert O'Harrow, Jr., "For Sale on the Web: Your Financial Secrets," Washington Post, June 11 1998, at A1.

individual, profiled on undisclosed factors, can end up paying too much for a financial service or product.

Because there are no limits on the sharing of personal data among corporate affiliates, a customer profile can be developed by a financial affiliate of the company and sold or shared with an affiliate that does not fall within the broad definition of "financial institution." A bank, for instance, that has an affiliation with a travel company could share a customer profile resulting in the bank's customer receiving unwanted telephone calls and unsolicited direct mail for offers of memberships in travel clubs or the like that the individual never wanted or requested.

Such affiliate sharing between financial and non-financial companies as well as sharing pursuant to a joint marketing agreement have resulted in aggressive, deceptive negative option sales of memberships that the customer neither wanted nor understood.[10] To compound the problem, non-financial affiliates of financial institutions can sell, share, lease or otherwise trade consumer profiles with other companies, thus increasing the number of privacy invasions on individuals already bombarded with unwanted telemarketing calls and "junk mail."

The customer of the bank or other financial institution that collected the information to begin with has no ability to knowledgeably consent on the sharing of information, no right to know what information is shared and with what company or when, and no right to stop the flow of information forward.[11] Furthermore, the individual has no right to review information that is disclosed or to correct inaccurate or incomplete data.[12] In short, the individual has no ability to control the flow or content of personal information.

Although many large banks now say that information is not shared with third-party non-affiliates, the same bank can share information with an affiliated credit card company. The bank's personal data on its customer then becomes a part of the credit card company's information. The credit card company, gives the customer a privacy notice that includes an opt-out as required by the GLBA, but discloses the information to third-party non-affiliates.

If the customer overlooks the privacy notice from the credit card company and fails to opt-out, the credit card company is free to disclose all information in its files to third-party non-affiliates. This includes information received from the affiliated bank. *This kind of backdoor disclosure poses a major threat to personal privacy.*

Individuals can take no comfort in a financial institution's claim that information is shared only within the "corporate family." In addition, such marketing phrases as "corporate family" not only fail to disclose the extent of information-sharing practices but also create a false sense of confidentiality and misplaced trust.

---

[10] *See supra*, note 3.
[11] *See generally* 15 USC §§1601 *et seq.*
[12] *See id.*

Serious harms have resulted from such information-sharing. NationSecurities obtained data on customers who had recently maturing low-risk securities from its NationsBank affiliate to market high-risk securities to them. The customers, a majority of whom were low-income elderly people, were misled by NationSecurities to believe that the securities carried the same kind of risk. When their investments collapsed, a number of elderly customers lost significant portions of their life savings.[13]

In this instance, the SEC issued a cease-and-desist order to stop the fraudulent securities sales practices. The SEC found that the NationSecurities sales force, encouraged by company management, intentionally blurred the distinctions between the securities broker-dealer and the bank. Thus, unsophisticated investors were led to believe they were dealing with bank employees and that their money was being invested in insured bank products when, in fact, investments were being funneled into mutual funds that included a high-risk component of over-the-counter derivatives.[14] *The sharing of personal information without consent was the practice that triggered the abuses of NationsBank.*

Aggressive sales practices plus commission incentives continually test the limits of information-sharing. While similar instances of abuses have been prosecuted,[15] such abusive practices can only come to light *after* there is significant harm to customers. An opt-in standard for affiliate sharing would help prevent such abuse.

The driving force in this era of mega-mergers among financial services companies is to pool customer data and to cross-sell different products. This trend introduces a second kind of risk to customers: the inability to exercise meaningful control and oversight over personal data. Will information collected to determine insurance premiums also be used to determine mortgage rates? Will a customer's credit card transaction data—several purchases at a liquor store for instance—influence life insurance premiums? Will a brokerage affiliate aggressively sell their wealth management services to a recently bereaved widower who might have received a significant death benefit? Will financially unsophisticated customers be targeted for risky investments as in the NationsBank example? There is no way in the current system for the customer to know how their highly personal and sensitive information might be used or abused.

If there are benefits to information-sharing, the financial services companies can be encouraged to make a compelling case to the customer for why they should agree to share their sensitive data. An opt-in standard for sharing information among affiliates will encourage greater transparency in how personal financial information is used. The lack of transparency not only leads to confusion and inevitable abuse, but also deprives customers of important consumer rights. Consumers want adequate disclosure about a company's information collection and use policies. Customers do not want to reveal more information than is needed for a transaction. Information collected for one purpose

[13] *See* In the Matter of Nations Securities and Nations Bank, Securities Act Release No. 7532 (May 4, 1998).
[14] *See id.*
[15] *See, e.g.*, Hatch, *supra* note 3; *see also* Enos, *supra* note 3.

should not be used for other purposes without the informed affirmative consent of the consumer.

Financial services companies should comply with fair information practices that (a) give consumers the right to opt-in for all information-sharing for secondary purposes, whether to affiliates or to third parties; (b) give consumers clear notice and full disclosure of a bank's privacy policies for both affiliate and third party sharing and of the consumer's right to choose; (c) give consumers full access to all of records containing information about them and a right to dispute and correct errors; and (d) provide consumers with enforceable legal rights against violators.

B. Permitting Unfettered Non-Affiliate Sharing Implicates Numerous Privacy Concerns Including Identity Theft, Profiling and Fraud

A typical privacy notice from a company that discloses information to third-party non-affiliates reads as follows:

> We disclose nonpublic personal information about you to the following types of third parties:
>
> **Financial service providers** such as mortgage bankers, securities broker-dealers, and insurance agents
> **Non-financial companies**, such as retailers, direct marketers, airlines and publishers
> **Others**, such as non-profit organizations.

All-inclusive notices such as this, and variations adopted from federal regulations, do nothing to answer the primary question of how information is used. Statements such as this do no more than to satisfy a financial institution's obligation to give a general disclosure. Although companies have spent millions to draft, print, and mail the notices, individuals who receive the notice, if they even see it, can only assume that personal information may be disclosed, for a price, to any outside entity. This important disclosure and all the implications that flow from it—and the right to opt-out—is almost always at the end of the privacy statement. Rather than notice to individuals about how personal information is used, these disclosures serve only to raise additional questions about how information is used and how much the financial institution profits from the use of the information.[16]

Sharing personal information with non-affiliates raises significant risks for customers. Such information-sharing leads to increased incidents of identity theft, profiling, and fraud. Most of the abuses come from cases where financial institutions entered into agreements to sell data and then profit from the sales generated by the receiving party – without regard to the character of the recipient or the products being marketed.

[16] *See* Interagency Public Workshop, *Get Noticed: Effective Financial Privacy Notices* (Dec. 4, 2001) *available at* http://www.ftc.gov/bcp/workshops/glb/.

For example, in 1999, Pacific Charter Bank sold customer credit card account numbers—without obtaining consent—to a person who subsequently committed credit card fraud on thousands of those individuals. The Attorney General of Minnesota sued U.S. Bancorp for selling customer data to third parties without obtaining customer consent, after customers were telemarketed by a firm that was able to directly debit customer bank accounts for the services purchased.[17]

The New York Attorney General targeted the Chase Manhattan bank, which was sharing personal information about its credit card holders and mortgagers with third party marketers without disclosing this fact to customers. The types of information shared with marketers included: the type of credit card and card number; last transaction date; credit line and whether it was delinquent or had exceeded the credit amount; number and amount of purchases per year and number and amount of purchases for year-to-date; cash advances; the amount of finance charges per year; and the consumer's card balance. Chase had contractual agreements with marketers to receive a percentage commission of any sales generated through the telemarketing and direct marketing campaigns. Over 22 million customers might have been affected. Chase agreed to settle the suit and changed its privacy policy to allow information-sharing with non-affiliates only with express written consent (opt-in).[18]

The Washington and Connecticut Attorney Generals pursued BrandDirect, a merchandiser of discount buying clubs partly owned by Reader's Digest and Federated Department Stores, for privacy violations. BrandDirect used information provided by some of the nation's largest financial institutions, including First USA Bank, Citibank, Chase Manhattan Bank and others, to develop lists of consumers who were then called by telemarketers. BrandDirect obtained consumers' charge card information from the banks, and in some instances used the information to make unauthorized charges against consumers' accounts. The banks, without the consent of their customers, shared their customers' credit card information with an over-zealous marketing firm, which misled, overcharged and deceived consumers.[19]

In February 2002, Citibank agreed to settle with 27 state Attorney Generals to remedy their deceptive telemarketing practices. Since the mid-1990s, Citibank had shared personal data with telemarketers to offer its customers products and services (including dental plans and credit card loss-protection programs), for which Citibank received a percentage of the sales. Customers were often deceptively billed for products and services without their express affirmative consent and were not able to easily cancel their membership in these programs.[20]

---

[17] *See* Hatch v. US Bank, *supra* note 3.
[18] *See* –In the Matter of Chase Manhattan Bank USA, (2000), *available at* http://www.oag.state.ny.us/internet/litigation/chase.pdf.
[19] Office of the Washington State Attorney General, "*Settlement with Discount Buying Club Highlights Privacy Concerns*," http://www.wa.gov/ago/releases/rel-branddirect.080400.html.
[20] *See* Office of the Attorney General of the State of California, *Citibank Agrees to Curb Deceptive Marketing Practices by Telemarketing Vendors*, *supra* note 6.

Although, under the GLBA, companies were prohibited from disclosing account numbers or access codes, in many circumstances, Citibank provided its marketing partner with an encrypted version of customer identifying information. When the individual agreed to a purchase, by failing to respond to a negative option, encrypted information was then transmitted to Citibank and the customer's account was charged.

Companies mask the profound implications of third-party sharing by suggesting that information is "shared," or "disclosed," or "provided" to outside companies. Instead, common sense says that information under these circumstances is either "sold," or "leased," or "traded" in some manner that means a profit to the company with no reciprocal benefit to the subject of the data. This endless string of information-sharing is deceptively presented to the public in marketing terms, couched as benefiting individuals, not the company that controls the information.

C. The Joint Marketing Agreement Loophole is a Serious Privacy Risk Allowing Unregulated Information-Sharing of the Type the GLBA was Enacted to Restrict

Although the GLBA generally requires that consumers be given notice and an opt-out choice as to whether their nonpublic personal information may be disclosed to nonaffiliated third parties, there is an exception for information disclosed to a nonaffiliated third party in connection with a joint marketing agreement. This exception, set forth in Section 502(b)(2) of the GLBA, applies to customer information that is disclosed to a nonaffiliated third party for purposes of marketing the financial institution's own products and services, or for purposes of marketing financial products and services offered pursuant to a joint agreement between two or more financial institutions. If disclosure of customer information fits within this marketing exception, the consumer is given no opportunity to opt out.[21] Nor is the individual entitled to any notice about the type of information shared, when it is shared, or with what joint marketer. This loophole is a serious privacy risk because it allows for precisely the kind of behavior the GLBA is supposed to restrict. This loophole is particularly troubling given the broad definitions of "financial institution" and "financial service or product" adopted for purposes of the GLBA.

The products and services offered pursuant to financial institutions' marketing agreements with third-party vendors are typically sold by telemarketers, using a script that characterizes the sale as a "free trial offer." Use of the terms, "free" and "trial offer," combined with the fact that the consumer is not required to provide his or her credit card or other account number, will likely lead the consumer to believe that he or she has not made a purchase or incurred any obligation.

Telemarketers do nothing to correct this misapprehension and their scripts generally do not require the telemarketer to obtain a clear and unequivocal consent from the consumer for the purchase of the products and services, or for the consumer's credit card or other account to be charged. They don't need this consent because in fact the financial

[21] 18 USC 6802(b)(2).

institution provides its customers' names and credit card numbers to the marketing company in order to make the solicitation. Financial institutions must be prevented from allowing such deceptive marketing practices to continue.

Third parties do not have the same accountability and audit protections for personal data as do the financial institutions that receive personal information directly from its customers. Although the GLBA places weak restrictions on the further use of data by joint marketers, the restrictions only apply insofar as the originating company could use the data. For example, a credit card company may send its customers a privacy notice saying that information may be disclosed to third-party non-affiliates and, and in compliance with the GLBA, gives the customer an opt-out. More often than not, the customer overlooks the notice entirely, does not give an opt-out, and the credit card company then discloses the information.

Then, if that same credit card company enters into a joint marketing agreement with another company to sell, for example, insurance against loss of the credit card, the joint marketer is then free to sell, share or otherwise disclose the information because the customer of the credit card company did not opt-out. The flow of personal data that results has no discernible end and the subject individual has no right to limit disclosure and no means to stop its onward transfer.

D. Other Risks of Personal Data on the Open Market

1. Identity Theft

Identity theft is the fastest growing white collar crime in America. Identity theft costs financial institutions over a billion dollars a year, which is then passed on to consumers through higher fees and interest rates. This does not account for the staggering financial and emotional costs that identity theft victims have to bear to clear their good name.[22]

Information-sharing practices of financial institutions increase the risk of identity theft by expanding the number of points where crooked employees or companies might compromise sensitive information.[23] The Privacy Rights Clearinghouse and the Federal Trade Commission have both seen an increase in identity theft cases that occur because dishonest "insiders" are able to gain access to personal information such as the Social Security number.[24]

---

[22] *See* Linda Foley, Executive Director, Identity Theft Resource Center, Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, Identity Theft and Legislative Solutions, (Mar. 20, 2002) *available at* http://www.idtheftcenter.org/html/s1742.htm; *See also* "Nowhere to Turn: Victims Speak Out about Identity Theft," by Privacy Rights Clearinghouse and CALPIRG (May 2000), *available at* http://www.privacyrights.org/ar/idtheft2000.htm.

[23] *See, e.g.*, Marc Rotenberg, Executive Director, EPIC, Written Testimony for Joint Hearing on SSNs and Identity Theft, Subcommittee on Oversight and Investigations, Committee on Financial Services and Subcommittee on Social Security Committee on Ways and Means, U.S. House of Representatives, (Nov. 8, 2001) *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html.

[24] *See, e.g.*, EPIC's Social Security Number and Privacy Archive, http://www.epic.org/privacy/ssn/.

Financial institutions might invest in good security practices and rigorously oversee their employees' work, but they have no control over the practices of third party entities. Although customers have a weak opt-out right from non-affiliated third party sharing (but none at all vis-à-vis the joint-marketing loophole), they have no means of assessing what might make a third party "trustworthy," as the financial institutions typically represent. Customers should, at a minimum, be able to find out who has had access to their personal information. Moreover, there are no restrictions placed on the use of information by the third party vendors once they have obtained the information. If an individual does not opt-out, joint marketers are then free to share information in the same manner as the originating institution.

Sensitive financial information should, for similar reasons, be restricted from sharing with affiliated non-financial entities. Almost all conglomerates have financial affiliates and non-financial affiliates. Under the current law, non-financial affiliates can obtain sensitive financial information on their customers without the customer's knowledge. Apart from increasing the risk of identity theft, the law fails to give consumers a choice in having their personal financial information used to market products and services to them.

2. Personal Information is a Gold Mine for Criminals

Easy access to the kinds of personal data stored in the databases of financial institutions creates an endless array of possibilities for criminals. What financial institutions describe as a "target marketing list" becomes a "sucker list" in the hands of criminals.

Information that characterizes an individual as deeply in debt, for example, makes that person a prime target for fraudulent credit repair services. Combine a poor credit rating with information that shows an individual is unemployed or on public assistance to make that person attractive for fraudulent work-at-home schemes. Add to this, the fact that the individual's home may be in foreclosure, and that person then becomes a prime target for a company that specializes in scams that assist personal bankruptcy.

An individual whose "experience and transaction" history reveals a propensity to give to numerous charities leaves open the likelihood of contact by fraudulent charities–especially in times of national disasters. The Federal Trade Commission's web site and history of consumer litigation contain numerous scenarios that involve fraud upon consumers. In a great number of cases involving consumer fraud, the initial contact is made by a company that already has in hand personal information about the victim.[25]

III. Notices Under the GLBA Fail to Give Consumers Adequate Choice or Notice Necessary to Evaluate the Benefits and Harms of Information-sharing

Information shared with the consent of the consumer for an identifiable benefit is not a source of public concern. Benefits of information-sharing, such as frequent-flyer programs, would continue to be available under an opt-in system. Customers should be

[25] Federal Trade Commission, *Privacy Initiatives*, http://www.ftc.gov/privacy/index.html (April 23, 2002).

able to make the decision whether actual benefits outweigh the invasion of privacy. What is a source of concern is an example in which a credit card company sells "transaction and experience" information to a third-party conglomerate that represents hotels, airlines, resorts and the like without a meaningful choice on the part of the consumer.

An exemption already exists in the GLBA to permit information-sharing where it is absolutely necessary. For most of the claims that opt-in would prevent crucial forms of information-sharing, an exemption is already included under the GLBA. For example, information can be shared for law enforcement purposes, to effect transactions, to service accounts, to protect the company's interest against fraud, and to report to credit reporting agencies.[26]

Company profit underlies all of the arguments in favor of taking control of information away from the consumer. Privacy is a fundamental individual right; companies' interest in profit must be subjugated to protection of this right. The result is the same whether the profit comes when a company uses sensitive data to market its own products and services, the products and services of a joint marketer or those of a financial or non-financial affiliate. All these instances of information-sharing practices, in the words of financial companies to individuals, are to "offer you an opportunity for new products and services."

Similar "goodwill" marketing language is used when a financial company says it "shares" information with third-party non-affiliates. Here, an intelligent public is expected to believe that financial conglomerates made up of insurance, brokerage and banking entities, would "share" the vast accumulation of customer data, the lifeblood of any company, for the benefit of the customer. Companies that disclose, by whatever means, personal data to third-party non-affiliates such as telemarketers and direct mail marketers, have no reasonable claim that the information is shared for the benefit of consumers.

Covered entities have treated privacy as a public relations issue, and have attempted to reverse public attitudes through a marketing campaign to convince the public that conceding control of personal data will bring offers of better products and services. For the majority of individuals this does not represent an "opportunity," but rather translates to more unwanted telemarketing calls, more junk mail and more opportunities for sensitive information to make its way into the databases of online data brokers available to identity thieves, fraudulent credit repair services, fraudulent charities and fraudulent investments, among many other schemes.

Intrusive telemarketing calls and unwanted junk mail are among the most frequent complaints made by consumers. The Privacy Rights Clearinghouse has received tens of thousands of such complaints over the years. Individuals express a high degree of frustrations with unwanted calls and mail, mainly because this marketing is continuous and virtually unstoppable. For the public, unwanted marketing, from any source, has taken on the negative connotation of privacy intrusions, frustration over the inability to

[26] 18 USC 6802(e).

control marketing, and annoyance of having no relief from marketing—especially while at home.

IV. Existing Privacy Law—Based on an Opt-Out Standard—is Inadequate to Protect the Privacy of Customer Information

A. Existing Privacy Laws Do Not Protect the Privacy of Customer Information

Existing privacy protection and regulation under the GLBA does not adequately protect the privacy of a customer's information. As otherwise discussed in these comments, any system to protect the privacy of personal information that relies upon silence as agreement has the built-in elements for abuse and eventually public outcry.

The most glaring inadequacies of the current law are that (1) the impetus for effective notice rests with entities whose interests are better serviced when there is *no* effective notice; (2) it assumes a company will, or even *can*, explain a complex set of legal definitions added to numerous exceptions to the law in a way that will allow for an informed choice; (3) there are no restrictions placed on a company's ability to freely share information that flows into the company about individuals who are not customers; (4) enforcement mechanisms are inadequate to assure compliance with even existing weak privacy protections.

1. *Opt-out Frameworks Create a Financial Incentive for the Creation of Confusing Privacy Notices and Obfuscated Opt-Out Mechanisms*

An opt-out system at its very heart carries the assumption that there will be little response to the notices because the notices will be overlooked, or will be too complicated to understand. Like other negative choice systems, permission though silence will invariably get a large percentage of "yes" responses because no response is necessary. This unfairly places the burden on the individual who is concerned about protecting privacy and not where the burden belongs – on the company that will profit from use of the personal information.

Companies are versant in how to best phrase and send opt-out notices to maximize customer confusion, and to minimize the chance that customers will read the notices.[27] In addition, companies know how to send out their opt-out notices in a manner least likely to be noticed, opened, or read by customers.[28] Studies have demonstrated that opt-out notices sent out pursuant to the GLBA are written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public.[29] Consumers have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words.[30]

---

[27] *See* Ting v. AT&T No. C 01-02969 BZ, ¶33 (Jan. 15, 2002)

[28] *See* id. at ¶¶25-28.

[29] *See* Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices* (July 2001) *at* http://www.privacyrights.org/ar/GLB-Reading.htm.

[30] *See* id.

control marketing, and annoyance of having no relief from marketing—especially while at home.

IV. Existing Privacy Law—Based on an Opt-Out Standard—is Inadequate to Protect the Privacy of Customer Information

A. Existing Privacy Laws Do Not Protect the Privacy of Customer Information

Existing privacy protection and regulation under the GLBA does not adequately protect the privacy of a customer's information. As otherwise discussed in these comments, any system to protect the privacy of personal information that relies upon silence as agreement has the built-in elements for abuse and eventually public outcry.

The most glaring inadequacies of the current law are that (1) the impetus for effective notice rests with entities whose interests are better serviced when there is *no* effective notice; (2) it assumes a company will, or even *can*, explain a complex set of legal definitions added to numerous exceptions to the law in a way that will allow for an informed choice; (3) there are no restrictions placed on a company's ability to freely share information that flows into the company about individuals who are not customers; (4) enforcement mechanisms are inadequate to assure compliance with even existing weak privacy protections.

1. *Opt-out Frameworks Create a Financial Incentive for the Creation of Confusing Privacy Notices and Obfuscated Opt-Out Mechanisms*

An opt-out system at its very heart carries the assumption that there will be little response to the notices because the notices will be overlooked, or will be too complicated to understand. Like other negative choice systems, permission though silence will invariably get a large percentage of "yes" responses because no response is necessary. This unfairly places the burden on the individual who is concerned about protecting privacy and not where the burden belongs – on the company that will profit from use of the personal information.

Companies are versant in how to best phrase and send opt-out notices to maximize customer confusion, and to minimize the chance that customers will read the notices.[27] In addition, companies know how to send out their opt-out notices in a manner least likely to be noticed, opened, or read by customers.[28] Studies have demonstrated that opt-out notices sent out pursuant to the GLBA are written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public.[29] Consumers have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words.[30]

[27] *See* Ting v. AT&T No. C 01-02969 BZ, ¶33 (Jan. 15, 2002)

[28] *See* id. at ¶¶25-28.

[29] *See* Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices* (July 2001) *at* http://www.privacyrights.org/ar/GLB-Reading.htm.

[30] *See* id.

An opt-in scheme would completely reverse this by making it in a company's best interest to explain its information-sharing practices in a way that individuals can understand and accept. This step is necessary to ensure that customers have knowledgeably consented to use of their personal information, and have not been tricked or confused into assenting to the loss of something they valued.

2. *Effective Choice Is Unattainable Where Broad Exceptions Exist Prohibiting an Individual's Ability to Control the Flow of Sensitive Information*

Broad exceptions to an individual's ability to control the flow of sensitive information under the GLBA create a multitude of situations in which business is conducted without knowledge, notice, or opportunity to express an opinion. The likelihood of abuses of personal data through information-sharing under an exception is evident from the fact that most of the cases brought by state attorneys general in recent years involved a large bank that shared, for a percentage of sales, information within a joint marketing agreement.[31]

Despite industry's assurance to the public that privacy protections can be achieved under the current opt-out system with notice, the last two years have shown that opt-out does nothing more than create a complicated and costly solution to a simple problem.

The difficulty of effecting adequate notice to the public in response to the GLBA is further complicated by the fact that the personal information in the files of most financial institutions requires an elaborate explanation of the circumstances under which individuals can opt-out of third-party non-affiliate sharing. In addition, under the GLBA regulations, companies must explain their practice of sharing information with affiliates––although there is no GLB opt-out out for this—and then attempt to explain that there is an opt-out for affiliate sharing of "creditworthiness" information under the GLBA, but not an opt-out for "experience and transaction" information.[32]

All of this causes a great deal of confusion for individuals attempting to absorb basic facts about how personal information is used and how to control the use. Most individuals wrongly assume they still have control over how personal information is used and merely have to opt-out to stop all unwanted disclosures. But the few who even see the notices are confronted with a complicated array of exceptions, legal concepts, and seemingly contradictory opt-out choices. Notices typically say even if an individual opts out, information can still be disclosed "as permitted by law," without giving a further explanation about what this means.

Many individuals express extreme frustration when they see references to various types of information-sharing on privacy notices and then see no means to opt-out. An understanding of these distinctions requires study, not just education, and it is inadequate

[31] *See, e.g.*, Hatch v. US Bank, *supra* note 3.
[32] *See* 15 USC §§6802, 6803.

notice to throw these complicated concepts out to the general public with small print and complex reading format, along with other obstructive tactics.

3. *There is No Privacy for Non-Customer Information*

Current law only places restrictions and requires written policies for information in a company's files on its own customers—individuals with a continuing relationship with a financial institution—or consumers—individuals who have isolated transactions with a financial institution. The law recognizes not even a modicum of privacy for those whose information is acquired by a company for marketing purposes or other reasons and who never establishes a relationship with the company.

For example, Charter Pacific Bank sold its database—including credit card numbers—to a convicted felon who in turn fraudulently charged credit cards for access to Internet pornography sites. This case represents a particularly blatant example of fraudulent use of personal information because many of the individuals whose credit cards were charged did not even have computers.[33]

The information contained in Charter Pacific's database was compiled from information obtained from the bank's merchant customers. The merchant customers supplied the names, addresses, and account numbers of *their* customers to Charter Pacific in connection with the merchant's account. But, many of the merchant's customers *were not* Charter Pacific customers.[34]

There is nothing in the GLBA to prevent fraud from information-sharing such as occurred in the Charter Pacific case. Even now, Charter Pacific is under no obligation to protect the information of the customers of the merchants—who were not Charter Pacific customers. The GLBA's failure to recognize that financial institutions *receive* as well as disclose information for marketing purposes is a major, but often overlooked, shortcoming in the effort to protect personal information.

4. *There is Inadequate Enforcement Under Current Law*

The GLBA lacks the enforcement mechanism necessary to assure compliance even with its own weak standards. Enforcement under the GLBA (and thus the obligation to assure privacy of personal information of each individual customer of regulated entities) rests solely with the federal agencies—already overtaxed with maintaining the country's financial stability in turbulent times. For the multitude of other, unregulated companies that fall within the broad definition of "financial institution," compliance is left to the Federal Trade Commission.

This is not to say federal agencies are neglecting to monitor compliance. However, much of the information collected about information-sharing practices is not available to the public. Unless an agency commences litigation, the public will never know about privacy

[33] *See* Hatch, *supra* note 3.
[34] *Id.*

abuses recorded in audits, customer complaints, or informal investigations. So, federal government efforts alone will add little to the public's knowledge of information-sharing practices among financial institutions.

Given that hundreds of thousands of companies fall within a broad interpretation of "financial institution," expanded enforcement authority to give states concurrent jurisdiction to enforce the provisions of the GLBA is necessary for a more effective enforcement program. For example, States have the authority to bring actions under Fair Credit Reporting Act (FCRA) but not GLBA.[35]

In addition, both federal and state enforcement programs are always at the mercy of staffing shortages, budget cuts, and enforcement priorities. Big cases involving high dollar amounts and many victims are, by necessity, given priority.

As a result, an individual whose situation does not rise above the government enforcement threshold in terms of number of victims and cumulative losses is left stranded. The right of an individual to seek redress is well established in most other areas of the law. The right to protect one's privacy should be given the same recognition as the right to protect property and or seek remedies for other individualized wrongs.

In addition, lawsuits brought by individuals play a significant role in developing case law, where often the government or other interested parties can express an opinion without assuming the burden of litigation. The process of discovery and trials in private lawsuits brought by individuals also frequently result in revelations of corporate practices that often change the law. Individuals have a right to protect their interests under the FCRA and should be given the same right under the GLBA. It should be noted that the FCRA was amended significantly in 1996 to give individuals that private right of action, which did not exist in the 1970 Act, indicating that without personal enforcement such a regulation fails to protect consumers.[36]

V. Financial Institutions' Privacy Policy and Privacy Rights Disclosure Are Inadequate Under Existing Law.

A. Financial Institution Privacy Notices Sent in Compliance with the GLBA Have Failed to Provide Consumers With Notice

The privacy notices sent by financial institutions beginning last year have failed in the fundamental purpose to give individuals meaningful notice upon which to base an informed agreement to share or otherwise disclose information within the terms of a company's stated policy.[37] Notices were usually overlooked and tossed away as "junk mail." Even in the few instances where a notice was recognized, the notices failed to give

[35] *Compare* 15 USC §621(c) *with* 18 USC 16801 *et seq.*

[36] In 1996, the Consumer Credit Reporting Reform Act amended the FCRA extensively (1996 Amendments). Pub. L. No. 104-208, 110 Stat. 3009 (Sept. 30, 1996).

[37] *See* Public Citizen, Petition for Rulemaking, (July 26, 2001), *available at* http://www.epic.org/privacy/consumer/glbpetition.pdf.

basic information necessary for an individual to act. Notices, furthermore, placed considerable burden on individuals in terms of time necessary to respond, costs of postage for as many as twenty requests and overall confusion about whether an opt-out was even available.

1. Most Notices Perceived as "Junk Mail"

Most individuals failed to recognize the notices at all because financial institutions were under no obligation to send the notices in separate mailings, print the notices in a readable format, write the notices at a reading level directed at the general public, or refrain from marketing. Although federal regulations gave financial institutions examples of what would meet the requirements of "clear and conspicuous," none of the requirements were mandatory.

In direct contrast to the findings of polls on public attitudes about privacy, very few people opted out. Estimates of opt-out percentages range from two to five percent. However, given the many different companies included in the definition of "financial institutions" a comprehensive account of the opt-out percentages is nearly impossible to determine. But, one thing is clear: Very few people opted out. While companies have attempted to make the case that the low opt-out reflects a public preference for information-sharing practices, the more reasonable conclusion for the low opt-out rate is that the procedure itself is flawed.

The indisputable fact is that most people did not see the notices in the first instance. The PRC undertook a consumer education program last year to inform the public about the GLBA notices. In response, the PRC was contacted by approximately 2,000 individuals seeking information about how to stop the flow of personal information. About sixty to sixty-five percent of the people who contacted the PRC had no knowledge of the provisions of the GLBA until seeing a media report.[38] Similarly, a study conducted by the American Bankers Association of 1,000 people showed that forty-one percent had failed to recognize the notices.[39]

The tendency of most companies to translate legal obligations into a marketing opportunity also contributed to the high instances of overlooked notices. Notices, more often than not, began with the company's commitment to protect consumer privacy, followed by statements about the company's desire to yield to customer needs for products and services. Such phrases left many who glanced at the notice with the impression that the company was simply trying to sell something. To gain attention, the first paragraph of the notices should have been aimed at drawing attention to the *real* reason for the notice without a marketing spin.

---

[38] *See* Tena Friery and Beth Givens, *2001: The GLB Odyssey—We're Not There Yet: How Consumers Responded to Financial Privacy Notices and Recommendations for Improving Them* (Dec 4, 2001) *available at* http://www.privacyrights.org/ar/fp-glb-ftc.htm.

[39] *See* American Bankers Association Press Release, "*ABA Survey Shows Nearly One Out of Three Consumers Reads Opt-Out Notices,*" (June 15, 2001) *available at* http://www.aba.com/Press+Room/bankfee060701.htm.

2. *Notices Were Confusing and Failed to Provide Basic Information*

Even for individuals who recognized and attempted to understand the notices, there was a lack of practical information about the deadline for answering, whether an opt-out was available, and even why the notice was being sent. Few notices told of the continuing nature of the right to opt-out or when information would be shared. Companies did not offer those who took the time to opt-out any confirmation or assurance that their request would be even be honored. Nor were companies required to offer any such assurance.

Individuals were often confused about why they were getting the notices. Companies were under no obligation to explain the relationship that prompted the notice. The PRC received a number of inquiries from people who were not sure why they received a notice from a company with which they had no apparent business relationship. Other people inquired as to why they had not received a notice from a company with which they did feel they had a business relationship. Companies who were confused about whether they would fall under the definition of "financial institution" also contacted the PRC on several occasions.

Furthermore, the notices were written to satisfy the legal obligations of companies, not to inform individuals. A study conducted by a readability expert and posted on the PRC web site concluded that, of sixty privacy notices examined, most were written at a third year college level or above.[40] The accepted standard for notices intended for the general public is an eight-grade reading level.[41]

3. *Notices Placed an Unfair Burden on Customers to Protect their Privacy*

One of the most common, and completely understandable, comments heard from individuals is, "Why should I have go to all this trouble to protect my private information? I already pay fees and commissions to this company for giving them my business."

An average household may have accounts at several banks and brokerage houses, insurance companies, a mortgage, a car loan, a student loan, several major credit cards, a number of store credit cards, a mutual fund, as well as a relationship with an accountant, and an attorney. When added together, the business of ordinary family finances can easily mean each household receives up to twenty privacy notices a year. All require a separate reading, a separate opt-out method, and separate postage, or phone calls.

This is in addition to considerable time that must necessarily be spent trying to understand the notices and responding to each. And, if the individual does not follow the

---

[40] *See* Mark Hochhauser, Lost in the Fine Print: Readability of Financial Privacy Notices, *at* http://www.privacyrights.org/ar/GLB-Reading.htm (July 2001).
[41] *See* id.

procedure given in the privacy notice, the company is under no obligation to accept the opt-out choice.

B. Regulators Must Place More Stringent Standards on Financial Institutions

As stated above, any attempts to add meaningful privacy provisions to the existing procedure through additional regulations would, in essence, be cosmetic. However, if the public is to have no alternative, regulators should place far more stringent standards on financial institutions. These should include:

- Obligation to give and accept alternative opt-out methods
- Mandatory privacy education for company staff
- Easy access to privacy policies – at branch offices and on web sites
- Obligation to confirm opt-out
- A single web site with opt out information
- Standards for readability
- Eliminate marketing in notices
- Encourage transparency in information-sharing practices

VI. Opt-In is the Only Feasible Approach to Permit Informed Customer Consent and to Permit Customers to Restrict Use of Personal Information

A. There is a Substantial, Protected Interest in Privacy of Personal Information

American jurisprudence recognizes a fundamental right to privacy, and the courts and Congress have recognized the paramount interest a citizen has in protecting her privacy.[42] The Constitutional right of privacy protects two distinct interests: "one is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[43] Financial institutions' use of customer information implicates both of these interests. Citizens have a legitimate and significant expectation of privacy with respect to sensitive non-public personal information contained within their financial information. In addition, customers have a right to personally determine how those financial institutions in possession of their personal information will use this information.

---

[42] *See, e.g.*, Edenfield v. Fane, 507 U.S. 761, 769 (1993) ("[T]he protection of potential clients' privacy is a substantial state interest."); Sheets v. Salt Lake City, 45 F.3d 1383, 1388 (10th Cir. 1995) (where an individual has an expectation that information will not be disclosed, prohibition on such disclosure is a substantial government interest). In Lanphere & Urbaniak v. Colorado, the 10th Circuit recognized that an invasion of privacy is most pernicious when "it is by those whose purpose it is to use the information for pecuniary gain." 21 F.3d 1508, 1511, 1514 (10th Cir. 1994) (applying Central Hudson analysis to uphold a Colorado statute prohibiting public access to criminal justice records "'for the purpose of soliciting business for pecuniary gain'") (quoting Colo. Rev. Stat. § 24-72-305.5 (1992)). This is exactly the purpose for which financial institutions would like to use customer information—to target consumers it believes might be interested in purchasing more of its services.

[43] Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

The fact that some of the information protected under the GLBA, such as a consumer's name and address, may be publicly available is irrelevant, because "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."[44] Additionally, the protections afforded by the regulations go well beyond concerns with the use or disclosure of publicly available information. The regulations and the underlying statute also protect even more sensitive—and very personally revealing—data contained within credit history and credit transaction data.

Privacy is a real and significant interest to most Americans: a survey performed in 1999 revealed that the loss of personal privacy was the number one concern of Americans entering the twenty-first century.[45]

It is notable that Congress recognized the importance of a citizen's privacy interest by enacting other statutes preventing disclosure of similar information to the public at large. For example, rules have been established to protect the privacy of cable subscriber records,[46] video rental records,[47] credit reports,[48] and medical records.[49]

B. Opt-In is the Only Truly Effective Means for Protecting the Privacy Interests of Consumers.

The danger of the opt-out approach lies in the fact that, because customers likely will not read their opt-out notices, there is no assurance that any implied consent would be truly informed. Under an opt-in approach, consumers must give the financial institution express approval before the company can divulge their personally identifiable information, which will minimize any unwanted or unknowing disclosure of the information. As previously discussed in these comments, under the opt-out approach, consumers may not possess the knowledge that they must affirmatively act to prevent distribution of their information. If they do not have this knowledge, then they cannot exercise discretion regarding it. Control of personal information is best achieved through consumers' prior consent to disclose information, that is, an opt-in standard. Not even an aggressive consumer education program can replace the control lost to an opt-out standard.

There is substantial independent evidence verifying that an opt-in approach is the only

[44] Department of Defense v. Federal Labor Relations Auth., 510 U.S. 487 (1994) (finding that unions could not use FOIA to obtain the home addresses of federal employees represented by unions).
[45] Wall Street Journal/NBC News poll, http://www.wsj.com, (Nov. 3, 1999). See also Testimony of Lee Rainie before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce (May 8, 2001) (86 percent of internet users surveyed stated that Internet companies should ask people for permission [opt-in] to use their personal information).
[46] See 47 U.S.C. § 551 (1994).
[47] See 18 U.S.C. § 2710 (1994).
[48] See Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994).
[49] See 42 U.S.C. § 290dd-2(a)(1994); See generally Marc Rotenberg, The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Developments 1- 173 (1999).

effective method to protect sensitive private information. An opt-out approach is inadequate because it is not calculated to reasonably inform consumers about their privacy options. Not only is the burden on the customer to pay for and return their opt-out notice, such notices are vague, incoherent, and often concealed in a pile of less important notices mailed in the same envelope from the same source.[50] Litigation has revealed that companies have been known to hire consultants to obscure notices from customers, as well as to draft language in a manner least likely to reveal the importance of the notice to the customer.[51] If the GLBA required the strong privacy standard of "opt-in," the privacy notices would have been written in clear language, extolling the benefits of enabling the financial companies to compile, profile and sell or share customer data. Further, financial institutions would likely provide incentives for customers to allow their personal data to be shared or sold with affiliate companies and third parties – perhaps six months of fee-free service, or a round-trip airplane ticket. That way, consumers would at least get some benefit from the free flow of their personal information.

C. Implementing an Opt-In Approach Serves the Governmental Interest in Customer Privacy

There is a longstanding historical, legal, and legislative record providing that privacy protection is a real, substantial, and significant concern. In addition, there is a specific legislative record detailing that this concern was a primary impetus behind the congressional enactment of the GLBA. A customer has a reasonable expectation that her personal information will be kept private. Customers provide information to their financial institutions with the expectation that the information will be kept confidential, and have no viable alternative regarding their financial institution's collection of information. Although customers are aware that this information is captured by financial institutions in providing a necessary service, this initial capture does not provide the right of further dissemination of private information. An opt-in approach to use of such information not only protects the privacy interests of customers, but also preserves important values recognized in the First Amendment context, which is the right of customers to decide, freely and without unnecessary burden, when they wish to disclose personal information to others.[52]

VII. Conclusion

The GLBA has failed to provide adequate privacy protections for consumers engaging in modern financial services. Protection of privacy is a substantial governmental interest, and the GLBA privacy protections place an affirmative burden upon covered agencies to protect privacy (§501 (a)). The GLBA privacy provisions, because they are based on an opt-out standard, do not protect the privacy of personal information because such an

[50] *See* Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law: A Study of United States Data Protection 329-30 (1996) ("The industry itself recommends the use of only vague notices that do not offer meaningful disclosure of practices.")

[51] Ting v. AT&T, No. C 01-02969 BZ, (Jan. 15, 2002) (AT&T conducted market research to determine the method of sending opt-out notices that would be the least likely to be noticed by the consumer).

[52] See generally Buckley v. American Constitutional Law Found., Inc., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n,514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).

approach is not calculated to reasonably give individuals the opportunity to control their personal information. Additionally, opt-out frameworks create incentives for obfuscating notice and opt-out processes.

Serious harms have resulted from information-sharing as permitted by limitations and loopholes under the GLBA. Individuals face a multitude of potential risks, including the potential for confusion and abuse, through unrestricted and undisclosed information-sharing of personal financial data information among affiliates and joint marketers under the GLBA. Sharing personal information with non-affiliates raises significant risks for customers, ranging from identity theft, profiling, and financial fraud, to intrusive and harassing telemarketing. Finally, under the GLBA there are no restrictions placed on a company's ability to freely share information that flows into the company about individuals who are not customers.

There is substantial independent evidence verifying that an opt-in approach is the only effective method to protect sensitive private information. If there are benefits to information-sharing, the financial services companies can be encouraged to make a compelling case to the customer for why they should agree to share their sensitive data. An opt-in standard for sharing information among affiliates will encourage greater transparency in how personal financial information is used.

The impetus for effective notice under an opt-out regime rests with entities whose interests are best served when there is no effective notice. The GLBA assumes a company will, or even can, explain a complex set of legal definitions added to numerous exceptions to the law in a way that will allow for an informed choice. The privacy notices sent by financial institutions beginning last year have failed in the fundamental purpose to give individuals notice upon which to base an informed agreement to share or otherwise disclose information within the terms of the company's stated policy. Notices were usually overlooked and tossed away as "junk mail." Even in the few instances where consumers recognized the notices, the notices failed to give basic information necessary for the individual to act. Regulators must place more stringent standards on financial institutions.

Finally, the GLBA enforcement mechanism is inadequate to assure compliance with even existing weak privacy protections. The right to protect one's privacy should be given the same standing as the right to protect property and or seek remedies for other individualized wrongs.