# Security
# of
# Personal Financial Information


**Report**

**on the**

**Study Conducted Pursuant to Section 508**

**of the Gramm-Leach-Bliley Act of 1999**

**June 2004**

# Security
of
# Personal Financial Information


Report
on the
Study Conducted Pursuant to Section 508
of the Gramm-Leach-Bliley Act of 1999

June 2004

# SECURITY OF PERSONAL FINANCIAL INFORMATION

## Report on the Study Conducted Pursuant to Section 508 of the Gramm-Leach-Bliley Act of 1999


**TABLE OF CONTENTS** i

**TABLE OF NAMES AND ACRONYMS** iii

**CHAPTER I:** ***INTRODUCTION*** 1

**CHAPTER II:** ***THE PURPOSES FOR INFORMATION SHARING AMONG FINANCIAL INSTITUTIONS, THEIR AFFILIATES, AND NONAFFILIATES***

- Introduction 5
- Purposes for Sharing Information 7
- Types of Information Shared with Affiliates Compared with Types of Information Shared with Nonaffiliates 14

**CHAPTER III:** ***THE POTENTIAL BENEFITS OF INFORMATION SHARING AMONG FINANCIAL INSTITUTIONS AND THEIR AFFILIATES – FOR FINANCIAL INSTITUTIONS, THEIR AFFILIATES, AND THEIR CUSTOMERS***

- Introduction 17
- Benefits of Sharing Information with Affiliates 17
- Benefits of Sharing Information with Nonaffiliates 20

**CHAPTER IV:** ***INFORMATION SHARING BY FINANCIAL INSTITUTIONS WITH THEIR AFFILIATES AND WITH NONAFFILIATES: POTENTIAL RISKS FOR CUSTOMERS***

- Introduction 23
- Potential Risks to Customers When Financial Institutions Share Information With Affiliates 26
- Potential Risks to Customers when Financial Institutions Share Information with Nonaffiliated Third Parties 28

**CHAPTER V:** ***ASSESSING LAW AND REGULATION***

- Introduction 31
- Assessing the Existing Laws 32
- Suggested Changes to the Existing Law and Regulation 35

**CHAPTER VI:** ***THE FEASIBILITY OF DIFFERENT APPROACHES TO INFORMATION SHARING***

- Introduction 39
- Opt Out 39
- Opt In 40
- Alternatives 44

**CHAPTER VII:** ***ASSESSING FINANCIAL INSTITUTION PRIVACY POLICY AND PRIVACY RIGHTS DISCLOSURE UNDER EXISTING LAW***

- Introduction 47
- Assessment of Notices 48

**CHAPTER VIII:** ***CONCLUSIONS, FINDINGS, AND RECOMMENDATIONS***

- Introduction 53
- General Conclusions 53
- Key Findings 54
- Recommendations 55
- Action Under Way 55

**APPENDIX A: GLBA Statutory Requirements for Study**
**APPENDIX B: Federal Register**
**APPENDIX C: Public Comments in Response to Federal Register Notices**

## TABLE OF NAMES AND ACRONYMS

| | |
|---|---|
| AAI | Alliance of American Insurers |
| ABA | American Bankers Association |
| ACLI | American Council of Life Insurers |
| AIA | American Insurance Association |
| ACB | America's Community Bankers |
| BofA | Bank of America |
| Capital One | Capital One Financial Corporation |
| CIPL | Center for Information Policy Leadership |
| CFB | Commercial Federal Bank |
| CFTC | Commodity Futures Trading Commission |
| CSB | Community State Bank |
| CTBA | Connecticut Bankers Association |
| CUSO | Credit Union Service Organization |
| CUNA Mutual | CUNA Mutual Group |
| Denali FCU | Denali Alaskan Federal Credit Union |
| E*Trade | E*Trade Financial Group |
| EPIC et al. | Electronic Privacy Information Center, the Privacy Rights Clearinghouse, US PIRG, and Consumers Union |
| FACT Act | Fair and Accurate Credit Transactions Act of 2003 |
| FCRA | Fair Credit Reporting Act |
| FDIC | Federal Deposit Insurance Corporation |
| FRN | Federal Register Notice |
| FRB | Federal Reserve Board |
| FSRT | Financial Services Roundtable |
| FTC | Federal Trade Commission |
| FleetBoston | FleetBoston Corporation |
| GLBA | Gramm-Leach-Bliley Act |
| Household | Household Bank (Nevada), N.A., Household Bank (SB), N.A., Household Bank, f.s.b., Household Credit Services, Inc., Household Finance Corporation, Household Automotive Credit Corporation, and Household Retail Services, Inc. |
| ICBA | Independent Community Bankers of America |
| MBNA | MBNA America Bank |
| NAIC | National Association of Insurance Commissioners |
| NAAG | National Association of Attorneys General |
| NAFCU | National Association of Federal Credit Unions |
| NAMIC | National Association of Mutual Insurance Companies |
| NCUA | National Credit Union Administration |
| NPA | National Pawnbrokers Association |
| Navy FCU | Navy Federal Credit Union |
| Northern | Northern Trust Corporation |
| OCC | Office of the Comptroller of the Currency |
| OTS | Office of Thrift Supervision |
| Rogue FCU | Rogue Federal Credit Union |
| Secretary | Secretary of the Treasury Department |
| SEC | Securities and Exchange Commission |
| SIA | Securities Industry Association |
| USA FCU | USA Federal Credit Union |
| USAA | United Services Automobile Association |
| VISA | VISA U.S.A. Inc. (April 30, 2002 letter) |
| VISA(2) | VISA U.S.A. Inc. (May 10, 2002 letter) |

# CHAPTER I

# INTRODUCTION

Enactment of the Gramm-Leach-Bliley Act of 1999 (GLBA) represented the culmination of decades of effort by Congress and various Administrations to repeal restrictions that had inhibited affiliation of different types of financial institutions.[1] GLBA permits commercial banks (including foreign banks) to affiliate with investment banks, insurance companies, and other kinds of financial services firms. As the bill proceeded through the latter stages of the legislative process, many believed the new opportunities that would enable U.S. financial institutions to offer a wider range of financial products and services to consumers should entail new obligations to ensure that the security of an individual's personal information would be adequately protected. Accordingly, provisions regarding disclosure and safeguarding of nonpublic personal information were introduced into GLBA.

These provisions concerning the security of personal financial information include a requirement that financial institutions provide their customers with notices describing the institutions' policies and practices for disclosing and protecting customers' nonpublic personal information.[2] The statute also restricts the ability of a financial institution to disclose certain consumer information to nonaffiliated third parties unless the consumer is first notified about the information disclosure and given an opportunity to block it (opt out). In addition, GLBA requires the relevant regulatory agencies to establish appropriate administrative, technical, and physical standards for financial institutions to ensure the security and confidentiality of customer information and protect against anticipated threats or hazards and unauthorized access to or use of such customer information.[3]

## THE STUDY

Congress expressed a continuing interest in the security of personal financial information when it required that the Secretary of the Treasury Department (Secretary), in conjunction with the Federal functional regulators and the Federal Trade Commission (FTC), to conduct a study of information-sharing practices among financial institutions and their affiliates.[4] In addition, GLBA required that this study be conducted in consultation with representatives of state insurance authorities (represented by the National Association of Insurance Commissioners (NAIC)), the financial services industry, consumer organizations and privacy groups, and other representatives of the general public.[5] Congress also required the Secretary to submit a report to

---

[1] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[2] GLBA, §§ 501-510, Subtitle A, Title V, "Disclosure of Nonpublic Personal Information," 15 U.S.C. §§ 6801-09 (1999). See also GLBA §501(b) and Chapter V for more discussion of Financial Institutions' safeguards.

[3] GLBA, § 501(b).

[4] GLBA, § 508(a). See Appendix A. The Federal functional regulators consist of: the Board of Governors of the Federal Reserve System (FRB), the Office of Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC).

[5] GLBA, § 508(b).

Congress, "containing the findings and conclusions of the study…together with such recommendations for legislative or administrative actions as may be appropriate."[6] Originally due by January 1, 2002, the report was delayed to allow the current Administration to complete the study and issue the report, including ample opportunity for public input into the study.

To ensure a fair and transparent process for eliciting the views of all of the parties specified by Congress, the Treasury Department issued a Federal Register notice (FRN), in consultation with staff of the Federal functional regulators and the FTC. The FRN was published on February 15, 2002, and requested public comment on the specific topics that Congress required to be studied, as well as other relevant issues.[7] Due to strong public response, Treasury extended the original April 1, 2002 deadline for comment to May 1, 2002.[8] Treasury accepted all comments submitted including comments received after the extended comment deadline date.

## THE REPORT

Appendix C contains the 56 comments received in response to the FRN. The comments may also be obtained via the Internet.[9] Many comments were submitted by representatives of the financial services industries or businesses with relationships to them. Banks, credit unions, their related organizations, and associations representing banks, credit unions, and securities organizations accounted for twenty-six of the comments. Insurance companies and the associations representing them accounted for eight, while credit card banks and organizations accounted for four. Other interested businesses and financial organizations accounted for four of the comments. There were twelve responses from private individuals responding on their own behalf. The Electronic Privacy Information Center, Privacy Rights Clearinghouse, Consumers Union, and US Public Interest Research Group (EPIC et al.) filed a single response. The National Association of Attorneys General (NAAG) filed a single response signed by the attorneys general (or similar officials) of thirty-four states, the District of Columbia, the Commonwealth of Puerto Rico, and the Northern Mariana Islands.[10]

The Treasury Department staff worked in conjunction with staff of the Federal functional regulators and the FTC, and consulted with representatives of the NAIC, to review and organize commenters' views for Chapters II-VII. The Treasury Department intended these chapters of

---

[6] GLBA, § 508(c).

[7] Public Comment for Study on Information Sharing Practices among Financial Institutions and Their Affiliates, 67 Fed. Reg. 7213 (2002). See Appendix B.

[8] Extension of Public Comment Period for Study on Information Sharing Practices among Financial Institutions and Their Affiliates, 67 Fed. Reg. 16488 (2002). See Appendix B.

[9] See Public Comments in Reponses to Regulations at http://www.treas.gov/offices/domestic-finance/financial-institution/cip/glba-study/index.html. Alternatively, go to www.ots.treas.gov and search the site for "GLBA information sharing study" to view the comment letters. See also Appendix C of the printed version of this report. An additional letter from Guaranty Bank appears to have been mistakenly attributed to the GLBA request but clearly addresses a regulatory issue concerning mutual holding companies.

[10] Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Idaho, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Oregon, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington and West Virginia. Hawaii's comments were issued through its Office of Consumer Protection, which while not part of the state's Attorney General's Office, is authorized by statute to represent the state on consumer protection issues.

the report to inform the reader by presenting the comments in an organized fashion that reduces the redundancy found in many of the responses. The report relies upon the views of the commenters, i.e. financial institutions, their representatives, their critics, and those who use their services, as the best sources of information regarding the information-sharing practices of institutions. Those views are allowed to stand on their own, without attempt by the Treasury Department to characterize them. As provided in the statute, the findings and conclusions of the Secretary together with recommendations for action are found in Chapter VIII.[11]

Commenters' representations in this report regarding financial institution information-sharing practices in a commercial context in the United States are grounded in law and regulation prevailing at the time of the study. GLBA and its respective regulations (which were adopted on a consistent basis by the Federal functional regulators and the FTC),[12] the Fair Credit Reporting Act (FCRA), as amended through 1999,[13] and state laws and their respective regulations were the principal sources that governed a financial institution's information-sharing practices in a commercial context.[14] Thus, the responses submitted by commenters address the questions included in the FRN in the context of what GLBA and FCRA, principally, permitted and restricted at the time. Consequently, this report focuses on the information-sharing practices of financial institutions in the context of those statutes principally.

In order to provide context, this report describes provisions of GLBA and FCRA that were applicable to information-sharing practices. These descriptions are factual, not interpretive, and are intended to provide the reader, who may not be familiar with the regulation of information sharing by financial institutions under GLBA and FCRA, with a basic background for understanding the comments that follow.

---

[11] Given the limited experience gained so far with the various aspects of compliance with GLBA information-sharing and disclosure provisions, and after careful consideration by and among the relevant regulatory agencies consulted for this study, views of compliance examiners are not included in this report. During a financial institution's examination, the examiners do not review all of the same areas that Congress outlined for this study, nor would examiners normally attempt subjective evaluations of those topics.

[12] GLBA § 504 and 7 U.S.C. §7b-2 require the FRB, OCC, FDIC, OTS, NCUA, CFTC, SEC and FTC, after discussions with state insurance authorities designated by the NAIC, to prescribe regulations to carry out the purposes of GLBA. These regulations are to be similar to the extent possible. These regulations are in part located at: Privacy of Consumer Financial Information, 65 Fed. Reg. 35162 (2000), and are codified at: FRB, 12 C.F.R. Part 216; OTS, 12 C.F.R. Part 573; OCC, 12 C.F.R. Part 40; FDIC, 12 C.F.R. Part 332; NCUA, 12 C.F.R. Part 716; SEC, 17 C.F.R. Part 248; CFTC, 17 C.F.R. Part 160; FTC, 16 C.F.R. Part 313. ["Joint Regulations"] Where a cite is made in this report to these regulations, it shall be made as follows: Joint Regs. § __. (section cited). Note that while the four banking agencies jointly issued identical regulations, the regulations issued by the SEC, CFTC, FTC, and NCUA, while similar to the extent possible, deviate in a few instances to take into account the unique nature of the institutions they regulate. Section 505 of GLBA requires state insurance authorities to enforce the law's disclosure protections in the case of persons engaged in providing insurance. To assist the states in meeting this requirement, the state insurance regulators, through the NAIC, adopted the Privacy of Consumer Financial and Health Information Model Regulation (NAIC Model Privacy Regulation). To date, every state has taken action to satisfy this mandate.

[13] The Fair Credit Reporting Act, §§ 601-625 (15 U.S.C. §§1681-1681v (1999)).

[14] There were other federal statutes exerting an impact on a financial institution's information-sharing practices, such as the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191,110 Stat. 1936 (1996); the USA PATRIOT Act, Pub. L. No. 107-56 (2001); and the Right to Financial Privacy Act, 12 U.S.C. § 3401 et. seq. (1978). A discussion of these statutes and related regulations generally is beyond the scope of this report.

Terminology used in the report generally reflects, but does not always mirror, the definitions used in either GLBA or FCRA. For example, the terms "consumer" and "customer" are used interchangeably throughout the report. When discussing information and information sharing, the report reflects GLBA's information-disclosure provisions applicable to consumers' "nonpublic personal information" -- *i.e.,* generally, information of an individual who seeks or has obtained a personal, family, or a household financial product or service from a financial institution.[15] Note also that GLBA defines "financial institution" broadly.[16] Abbreviations used throughout the report to denote specific commenters, organizations, statutes, or categories of information are listed at the beginning of the report for easy reference.

Chapters are organized into subheadings. Under each subheading, comments are presented in two groupings: relevant remarks from private sector industry commenters and relevant remarks from EPIC et al., NAAG, and individuals. Chapter II examines the purposes for which commenters indicated that information was shared and the types of information disclosed by financial institutions, while Chapter III reviews the benefits of information sharing for financial institutions, their affiliates, and for customers, respectively. Chapter IV considers risks to consumers from information sharing, while Chapter V reflects commenters' views on the principal laws with which financial institutions had to comply to protect the personal financial information of their customers. Chapter VI examines the feasibility of using opt in, opt out, and other approaches to providing consumers options regarding information sharing, including alternatives adopted voluntarily. Chapter VII reviews the disclosures regarding the policies and practices of financial institutions required under GLBA. The Secretary's findings, conclusions, and recommendations appear in Chapter VIII.

[15] GLBA, § 509(4).

[16] A "financial institution" is defined under GLBA § 509(3) as any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956. 12 U.S.C. 1843(k).

## CHAPTER II

## THE PURPOSES FOR INFORMATION SHARING AMONG FINANCIAL INSTITUTIONS, THEIR AFFILIATES, AND NONAFFILIATES

### INTRODUCTION

Congress required that this study include an examination of "the purposes for the sharing of confidential customer information with affiliates and nonaffiliated third parties."[17] Commenters were asked to comment on the difference, if any, between the types of information financial institutions share with affiliates and the information shared with nonaffiliated third parties.[18] Both federal and state laws shape information disclosures by financial institutions to third parties by permitting the flow of information for some purposes and constraining the flow for other purposes. At the federal level, GLBA and FCRA have been the principal statutes governing the disclosure of nonpublic personal information by financial institutions to third parties in a commercial context.

GLBA permits financial institutions to disclose nonpublic personal information to nonaffiliated third parties only after providing to their customers a disclosure notice about the institution's policies and practices and then either: 1) sharing information for purposes specifically permitted under the statute, or 2) if the institution proposes otherwise to disclose information to nonaffiliated third parties, providing their customers with an opportunity to direct that such information not be disclosed (an opt out). Generally, the types of information sharing that are not subject to the opt-out standard permit financial institutions to: 1) conduct ordinary business operations, such as the servicing or maintenance of customer accounts; 2) support anti-fraud and risk management activities; and 3) comply with legal and regulatory requirements.[19]

---

[17] GLBA, § 508(a)(1).

[18] FRN, 67 Fed. Reg. 7214 (2002). Comments relating to the FRN questions on the existence of operational or voluntary limits that restrict information-sharing practices are reflected in Chapter VI.

[19] GLBA, § 502(e). Subsection (a) and (b) of this section shall not prohibit the disclosure of nonpublic personal information:

1. as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with –

   (A) servicing or processing a financial product or service requested or authorized by the consumer;

   (B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

   (C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

2. with the consent or at the direction of the consumer;

3. (A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

In addition, GLBA permits financial institutions to disclose nonpublic customer information to nonaffiliated third parties for certain marketing purposes. Under this exception, institutions may disclose information to other financial institutions pursuant to joint marketing agreements and/or to provide services to the financial institution, including assisting the financial institution in the institution's own marketing efforts. In these cases, the law mandates that financial institutions enter into written contracts with these third parties that require the third parties to maintain the confidentiality of the customer information.[20]

Under GLBA, a financial institution is expressly prohibited from disclosing its customers' account numbers to a nonaffiliated third party for use in marketing.[21] The restriction prohibits an institution from giving third-party marketers a means to access or charge a customer's account directly for the product or service that the third party is marketing. The regulations permit financial institutions to provide marketers with encrypted account numbers provided they do not give marketers the means to decode the numbers or otherwise access customer accounts. Thus, the third-party marketers will know that the individual is a customer of the financial institution, but will not be able to charge the individual's account directly. GLBA also imposes restrictions on a third party's reuse and redisclosure of nonpublic personal information it receives from a nonaffiliated financial institution.[22]

---

4. to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors.
5. to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;
6. (A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or (B) from a consumer report reported by a consumer reporting agency;
7. in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or
8. to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

[20] GLBA, § 502(b)(2).

[21] GLBA, § 502(d). See also Joint Regs. § ___.12. This corresponds to § 14 of the NAIC Model Privacy Regulation.

[22] These limits on reuse and redisclosure depend on the circumstances under which the information is transferred. If a third party receives information under one of the exceptions to the opt-out procedures contained in GLBA § 502(e), Joint Regs. § __.11, and NAIC Model Privacy Regulation § 13, the third party may only reuse or redisclose the information in the ordinary course of business to carry out the activity for which the information was provided. By contrast, if a third party receives the information after an institution's customer has not exercised the opt-out choice, then it may use the information for any purpose but may only redisclose the information consistent

FCRA regulates consumer reporting agencies, the furnishing of information to consumer reporting agencies, and the use of consumer reports. Those who provided comments for the study operated under an FCRA that permitted financial institutions to share customer transaction or experience information both with affiliated and nonaffiliated entities.[23] By contrast, a financial institution that disclosed other types of eligibility-related information about its customers (such as information from credit applications) might become a consumer reporting agency under the terms of FCRA, and thus be subject to FCRA's restrictions and requirements. However, an institution might share such information with its affiliates without becoming a consumer reporting agency, if the institution first afforded consumers an opportunity to opt out of such disclosure (and the consumer does not opt out).

Consumers also had the choice under FCRA to prevent unwanted credit or insurance solicitations by blocking the use of information for "pre-screening" by consumer reporting agencies. Consumer reporting agencies otherwise could provide lists of potential customers to prospective creditors or insurers, compiled on the basis of pre-qualification criteria set by the creditors or insurers. Every pre-screened solicitation had to contain a clear and conspicuous notice of the right to opt out of the pre-screened solicitation and how to opt out of future pre-screened offers.[24]

State laws may also restrict information sharing by financial institutions. Many of these laws predate GLBA. Some permit financial institutions to disclose customer information for purposes similar to the exceptions to the opt-out choice enumerated in GLBA, while others condition certain disclosures on consumer consent.[25] GLBA does not prohibit states from imposing additional restrictions on information sharing.[26] FCRA provides for a uniform national standard with respect to the exchange of information among affiliates.[27]

## PURPOSES FOR SHARING INFORMATION

### *Financial Services and Other Industry Perspectives*

Several commenters from the financial industries noted that legal and regulatory factors, as well as business considerations, might lead financial organizations to provide financial

---

with the institution's information use notice, and must honor any opt-out election that the financial institution's customer may exercise after the time the third party receives the information.

[23] FCRA, §§ 603(d)(2)(A)(i) and (ii). Note: This chapter does not describe aspects of FCRA arising from amendments made after 1999.

[24] FCRA, § 604(e). See also FCRA, § 615(d)(1).

[25] *See, e.g.* Connecticut (Conn. Gen. Stat. §§ 36a-41 to 36a-45 (2001)); Florida (Fla. Stat. Ann. §§ 817.58, 817.646 (2001)); Vermont (Vt. Stat. Ann. tit. 8, §§ 10201-10205 (2001)); North Dakota (N.D. Cent. Code, Ch. 6-08.1-01 to 6-08.1-08 (2002)); Illinois (205 Ill. Comp. Stat. Ann. 5/2, 5/48.1 (2002)).

[26] GLBA, § 507(b).

[27] FCRA, §§ 624(b)(2) and (d)(2). The uniform national standard included an exception, allowing for subsection (a) or (c)(1) of section 2480e of title 9, Vermont Statutes Annotated, as in effect on the date of enactment of the Consumer Credit Reporting Reform Act of 1996. This uniform national standard would have expired on January 1, 2004, if Congress had not taken action to preserve it in 2003.

products and services through separate entities within the organization rather than through a single financial institution.[28] The Financial Services Roundtable (FSRT) noted:

> The manner in which financial services firms operate varies tremendously; there is no typical model…the GLB Act requires integrated financial services firms to conduct banking, securities, and insurance activities through separate affiliates. However, some firms may operate separate corporate entities, such as banks, mortgage companies, or insurance companies on a state-by-state basis. In addition, some products may be offered by a bank, a subsidiary of the bank, or an affiliate of the parent firm.[29]

Affiliates of a financial institution may also be created in response to legal or regulatory factors, such as State insurance regulation, differences in charters for depository institutions, or various licensing programs for financial service professionals.[30] Tax considerations, historical factors, cost allocation methodologies, risk management, compensation, market segmentation, or managerial reasons may also influence whether affiliates are created.[31]

Thus, even though numerous considerations may lead to the formation of separate and distinct entities, financial institutions may share information with affiliates for many reasons.[32] They may disclose information to affiliates in order to reduce the overall cost of customer service by consolidating processing systems, customer service centers, and databases.[33] An institution may conduct administrative or service activities in an entity that is separate from each of the line businesses it services to enhance record keeping and cost allocation among affiliates.[34] Citigroup, for example, stated that it relies on affiliates for particular corporate functions, such as providing independent audit and legal functions; developing and testing operating systems; creating and delivering marketing materials, statements, and bulletins; and conducting other routine business activities.[35] In addition, Citigroup stated that affiliates in different lines of business may share a common customer interface by using joint employees.[36]

---

[28] *See, e.g.,* FSRT, addendum, pp. 3-4; Citigroup, pp. 4-7, 10; Commercial Federal Bank (CFB), p. 2; Household Bank (Nevada), N.A., Household Bank (SB), N.A., Household Bank, f.s.b., Household Credit Services, Inc., Household Finance Corporation, Household Automotive Credit Corporation, and Household Retail Services, Inc. (Household), pp. 1-2; VISA U.S.A. Inc. (VISA), pp. 3-4; CUNA Mutual Group (CUNA Mutual) p. 2; USA Federal Credit Union (USA FCU), p. 1; Navy Federal Credit Union (Navy FCU), pp. 1-2; Bank of America (BofA), p. 4; Wells Fargo, pp. 2-3, FleetBoston Corporation (FleetBoston), p. 3; Bank One, p. 2; Northern Trust Corporation (Northern), p. 2.

[29] FSRT, addendum p. 3.

[30] Citigroup, p. 10.

[31] *Id*., pp. 10-11.

[32] *See, e.g.,* FSRT, addendum, pp. 3-4; Citigroup, p. 10; CFB, p. 2; Household, pp. 1-2; VISA, pp. 3-4; E*Trade Financial Group (E*Trade), p. 2; Navy FCU, p. 2; MetLife, p. 3; Wells Fargo, p. 2.

[33] Citigroup, p. 10.

[34] *Id*.

[35] Citigroup, p. 11. See also CFB, p. 1; BofA, p. 4; FleetBoston, pp. 2-3; MBNA America Bank (MBNA), p. 2; Rogue Federal Credit Union (Rogue FCU), p. 2; MetLife, p. 3; American Council of Life Insurers (ACLI), p. 4; National Association of Mutual Insurance Companies (NAMIC), pp. 3-4; Wells Fargo, p. 3; Household, p. 2; Bank One, pp. 4-5; FSRT, p. 7; Securities Industry Association (SIA), p. 5; America's Community Bankers (ACB), pp. 3-4.

[36] Citigroup, p. 11.

Many industry commenters added that information sharing among affiliates is necessary to control or manage risk within an institution.[37] They stated that information shared with affiliates may be used to detect and prevent fraud, money laundering, and unauthorized use of accounts; fulfill due diligence or know-your-customer requirements, including requirements contained in other statutes or regulations; improve debt collection; and facilitate research and analysis of aggregate customer data.[38] Capital One Financial Corporation (Capital One), for example, explained that it shares information among affiliates for many purposes, including trending analysis, credit modeling, and target marketing efforts.[39] MetLife explained that "in the auto insurance business, it is common practice to submit a consumer's application to any of several affiliated companies to determine which one will offer to issue the insurance policy at a premium rate that is appropriate, given the risk insured."[40]

Some large, multi-institution financial organizations also commented on their reliance on information sharing with affiliates for cross selling of financial products and services as an essential business activity for maintaining customers, recouping costs, and generating profit.[41] One such financial institution noted that banks rarely recapture the acquisition cost of an account in the first year and must count on longer term, stable relationships with customers to make money.[42]

By contrast, some commenters explained that many smaller financial institutions rely on nonaffiliated third-party service providers to offer their customers a broad array of financial products and services that larger, complex corporate organizations may offer through affiliated firms.[43] The Connecticut Bankers Association (CTBA) noted the importance of "networking" programs used by smaller community banks to emulate the one-stop shopping capabilities of their larger competitors.[44] The Independent Community Bankers Association (ICBA) explained:

> The Gramm-Leach-Bliley Act, by allowing financial holding companies to provide a variety of financial services under one corporate umbrella, recognizes the increasing importance being placed on access to a variety of financial products and services through one trusted provider. Because they do not have an extensive array of affiliates within the corporate structure to provide different products and services, allowing community banks to share information with non-affiliated service providers and joint marketers permits community banks to offer a breadth of financial products and services to their customers at a reasonable cost, something they might not otherwise be able to offer.[45]

---

[37] *See, e.g.,* SIA, p. 5; BofA, p. 4; Household, p. 2; Wells Fargo, pp. 2-3; Citigroup, pp. 10-11; MBNA, pp. 8, 10; Bank One, pp. 4, 9; CUNA Mutual, p. 6; E*Trade, p. 4; NAMIC, pp. 7, 12; ACLI, p. 11; CFB, p. 2; National Association of Federal Credit Unions (NAFCU), p. 2; ACB, p. 5.

[38] *Id*.

[39] Capital One, p. 6.

[40] MetLife, p. 5.

[41] *See, e.g.,* Citigroup, p. 11; VISA, pp. 4, 7; Bank One, p. 2.

[42] Citigroup, p. 4.

[43] *See, e.g.,* Independent Community Bankers of America (ICBA), p. 3; CUNA Mutual, p. 6; ACB, p. 7; American Bankers Association (ABA), p. 7; FSRT, p. 5.

[44] CTBA, p. 5.

[45] ICBA, p. 3.

Citigroup stated that few companies, large or small, are able to "manufacture" their own services in certain product lines where the provision of such products would benefit from economies of scale or that may require special expertise.[46] Additionally, Citigroup remarked that few financial services companies engage in a sufficient volume of marketing to support their own internal "plant" for creating and mailing those offers.

The Securities Industry Association (SIA) reported that securities firms may share information with nonaffiliated service providers to administer and service customer accounts as well as to support the products and services institutions offer to their customers.[47] SIA stated that a financial institution may contract with an external service provider, for example, to prepare and send customers' account statements, proxy reports, mutual fund mailings, and company reports. A third party transfer agent must be contacted to facilitate a customer's stock transfer to another account or another firm, according to SIA. In addition, financial institutions transfer information to state authorities in order to comply with escheatment and abandoned property laws or in response to a subpoena, court order, or request by law enforcement. SIA stated that these disclosures generally include customers' names, addresses, social security numbers, and the number of shares owned in a particular company.[48]

A number of financial institution trade groups noted that their members disclose information to third parties largely for the purposes covered by the exceptions to the opt-out choice under GLBA.[49] The American Bankers Association (ABA) reported that a survey of 390 financial institutions in August 2001 found that 89 percent of those institutions did not share information outside of the exceptions permitted under GLBA and the implementing regulations.[50] America's Community Bankers (ACB) similarly found, "most community banks do not share customer information with non-affiliated third parties - beyond the basic exceptions provided under GLBA."[51] The National Association of Federal Credit Unions (NAFCU) contended that "almost all credit unions share information only within the exceptions," which are provided by sections 13 (joint marketing or marketing of the institution's own products or services), 14 (routine business purposes), and 15 (legal and regulatory requirements) of their Part 716 exceptions.[52]

Comments from insurers indicated that they also relied on both affiliated and nonaffiliated third parties to perform basic business functions. These include underwriting, evaluating or paying claims, administering and servicing existing contracts, and performing related product or service functions.[53] The American Council of Life Insurers (ACLI) and MetLife also noted that financial institutions may share information to meet legal and regulatory

---

[46] Citigroup, pp. 4-5.

[47] SIA, p. 4.

[48] *Id*., p. 4-5.

[49] *See, e.g.,* National Pawnbrokers Association (NPA), p. 2; ABA, p. 3; ACB, p. 6; ICBA, p. 3; FSRT, pp. 4-5; NAFCU, p. 1.

[50] ABA, p. 3.

[51] ACB, p. 6.

[52] NAFCU, p. 1. See NCUA GLBA privacy regulations, 12 C.F.R. §§ 716.13-716.15.

[53] *See, e.g.,* MetLife, pp. 3-4; ACLI, p. 3; NAMIC, pp. 2-3; United Services Automobile Association (USAA), pp. 2-3.

requirements, to detect and deter fraud, reinsure liabilities, and support mergers and acquisitions.[54] MetLife stated that information sharing may also be used to protect the public by reporting information to public health authorities.[55] In the life insurance business, one commenter noted, it would be unusual not to use nonaffiliated third parties to verify information from customers and others.[56] ACLI stated:

> Third parties such as actuaries, physicians, attorneys, auditors, investigators, translators, records administrators, third party administrators, employee benefits or other consultants, and others are often used to perform business functions necessary to effect, administer, or enforce insurance policies or the related product or service business of which these policies are a part.[57]

ACLI also stated that insurance companies regularly disclose personal information to state insurance departments, self-regulatory organizations, such as the Insurance Marketplace Standards Association, and state insurance guaranty funds, as well as to the Medical Information Bureau.[58]

### *EPIC et al., NAAG, and Individuals' Perspectives*

EPIC et al. believed that this study "can be expected to shed little, if any, new light on *actual* information-sharing practices within the financial services industry," because it is based on voluntary comments.[59] They noted that a good deal of the information collected about information-sharing practices is not available to the public, and commented, "Unless an agency commences litigation, the public will never know about privacy abuses recorded in audits, customer complaints, or informal investigations."[60]

In general, EPIC et al., NAAG, and some individual commenters raised concerns about consumers' inability to control the flow of personal financial information about themselves and expressed views on the potential harm that may arise as a result of current information-sharing practices.[61] Their views on the risks to consumers of information sharing are represented in greater detail in Chapter IV, in Chapter V, which reflects commenters' assessments of current law and regulation, and in Chapter VII, concerning the disclosures required under Title V of GLBA.

EPIC et al. commented that databases may be built too easily by financial institutions with hundreds or even thousands of affiliates engaged in wide-ranging activities permitted by GLBA. They wrote:

> When customer databases from these giant entities are combined, the result is a mega database containing a vast amount of financial, medical and other sensitive

---

[54] ACLI, p. 5; MetLife, p. 4.

[55] MetLife, p. 4.

[56] *Id*.

[57] ACLI, pp. 3-5.

[58] *Id*., p. 5.

[59] EPIC et al., pp. 3-4.

[60] *Id*., pp.16-17.

[61] EPIC et al., p6; NAAG, pp.7-11; Grammer, p.1; Olsen, p.1.

> 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.[62]

NAAG noted, "The list of activities that are identified by the Federal Reserve Board in its rulemaking as 'financial' in nature or closely related to financial activities and therefore permissible for inclusion within a financial holding company, goes well beyond traditional financial activities."[63]

EPIC et al. and NAAG noted that GLBA information-sharing provisions developed from public discontent about the sale of personal data for marketing purposes that was highlighted in a number of legal actions brought by state attorneys general.[64] NAAG noted that financial institutions may not disclose the valuable information they have about their customers to competitors, but added, "they do disclose the information to marketing partners and third parties for the purpose of jointly marketing products and services unrelated to the customers' current service selection, and even unrelated to the particular type of services performed by the financial institution itself."[65] Harm to consumers arises, they wrote, from subsequent tactics used by telemarketers to sell products to consumers who often do not realize that the marketer has his or her account number or access to it. EPIC et al. pointed to a number of cases to illustrate how personal financial information could be transferred to third parties whose preacquired account telemarketing efforts could disadvantage or harm thousands of people.[66] NAAG described the settlement in 1999 between the Minnesota Attorney General and U.S. Bank, "resolving allegations that U.S. Bank misrepresented its practice of selling highly personal and confidential financial information regarding its customers to telemarketers."[67] NAAG noted that Congress subsequently enacted the GLBA information-sharing provisions. These included, NAAG stated, the prohibition on sharing account numbers or similar forms of access numbers or access codes for marketing purposes and the joint marketing provisions, described earlier in this chapter.

---

[62] EPIC et al., p. 5.

[63] NAAG, p. 12.

[64] EPIC et al., p. 3; NAAG, pp. 8-10. See Chapter IV.

[65] NAAG, p. 7.

[66] EPIC et al., pp. 8-10. Se also, NAAG, p. 9.

[67] NAAG, p.7. NAAG continued: "One year later, thirty-nine additional states and the District of Columbia entered into a similar settlement. The multi-state investigation focused on the bank's sale of customer information, including names, addresses, telephone numbers, account numbers, and other sensitive financial data, to marketers. The marketers then made telemarketing calls and sent mail solicitations to the bank's customers in an effort to get them to buy the marketers' products and services, including dental and health coverage, travel benefits, credit card protection, and a variety of discount membership programs. Buyers were billed for these products and services by charges placed on their U.S. Bank credit card. In return for providing confidential information about its customers, U.S. Bank received a commission of 22% of net revenue on sales with a guaranteed minimum payment of $3.75 million." *Minnesota v US Bank National Association ND*, Docket No. 99-872 (D. Minn. June 30, 1999); also cited as *Hatch v US Bank et al.,* Final Judgment and Order for Injunctive and Consumer Relief (No. 99-872). See also *U.S. Bank Litigation*, Docket No. 99-891 (D. Minn. December 12, 2000).

EPIC et al. also described a case in which information had been shared among affiliates.[68] EPIC et al. and NAAG also noted that sharing of transaction or experience information among affiliates is unrestricted.[69] EPIC et al. commented that the collection of transaction or experience information can lead companies 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."[70] They maintained that customer profiling resulting from the collection and aggregation of transaction or experience information as well as other information can lead to the determination of the cost to the customer of financial services and products, and marketing of products or services by an affiliate "that does not fall within the broad definition of 'financial institution'…" (e.g., a travel company).[71]

NAAG noted, "The risk to consumers with sharing of information, whether to third parties or to affiliates, is that there will continue to be sales of membership clubs, insurance products, and other products and services through preacquired account telemarketing under circumstances where the consumer has either not authorized the transaction, or the authorization is not clear."[72] EPIC et al. stated:

> 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.[73]

Individual commenters noted that a financial institution distributes information primarily in order to increase revenues and that such distribution is detrimental to their personal privacy. One individual commented that he does not like his bank sharing his information and "putting my name on sucker lists."[74] Another commenter stated, "Spam e-mail is getting out of hand, and much of it is financial in nature. I believe the credit service bureaus are abusing their role and

---

[68] EPIC et al., pp. 6-7. They stated: "NationsSecurities obtained data on customers who had maturing low-risk securities from its NationsBank affiliate in order to market high-risk securities to them. The customers, a majority of whom were low-income elderly people, were misled by NationsSecurities 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." EPIC et al. stated that the SEC issued a cease-and-desist order with regard to NationsSecurities' sales practices. *In the Matter of NationsSecurities and NationsBank, NA*, Docket No. 3-9596, decided May 4, 1998. See Chapter IV for additional cases described by EPIC et al.

[69] EPIC et al., p. 5; NAAG, p. 2.

[70] EPIC et al., p. 5.

[71] *Id*., pp. 5-6.

[72] NAAG, p. 1. "Preacquired account telemarketing" occurs when a telemarketer has obtained account information about the consumer prior to the solicitation and may therefore charge the consumer's account without having to get the account number from the consumer. Under the GLBA implementing regulations, because a financial institution may not provide a telemarketer with a decoded account number, the telemarketer cannot directly access the consumer's account to charge it.

[73] *Id*., p. 4.

[74] Squire, p. 1.

selling information to telemarketers and anyone else willing to buy it."[75] Another individual stated that it is all too easy for fraudulent account information to be entered into the credit reporting system, creating problems for the victims of the fraud if they try to open new accounts or clear their credit history; therefore, it is essential to have a data information sharing system with rules and principles that facilitate the purging of bad data and prevent the reintroduction of such information.[76]

## TYPES OF INFORMATION SHARED WITH AFFILIATES COMPARED WITH TYPES OF INFORMATION SHARED WITH NONAFFILIATES

### *Financial Services and Other Industry Perspectives*

A number of large, diversified financial organizations indicated that customer information generally is shared widely with affiliates subject to any legal requirements that may be triggered by GLBA, FCRA, or internal policies.[77] A large, multi-institution organization typically might share the following types of information with affiliates:

- application information (e.g., assets, income and debt);
- transaction or experience information (e.g., account balances, types of account (cash or margin), payment history, parties to transactions and credit card usage, information about the institution's communications with its customers);
- consumer report information (e.g., creditworthiness or credit history);
- information from outside sources (e.g., employment verification, information about credit and other relationships, verification of information such as property insurance coverage); and
- other general information (e.g., demographics not used for eligibility purposes).[78]

VISA USA Inc. (April 30, 2002 letter) (VISA) wrote the following: "The sharing of customer information among affiliates is inherently different from the sharing of information with non-affiliated third parties, and tends to create greater efficiencies than sharing information with non-affiliated third parties."[79] Because customer information is inherently valuable, generally it is provided to nonaffiliated entities under limited circumstances, VISA reported. The company also stated that disclosures between affiliates are often broader and more frequent than those with nonaffiliated third parties. Thus, VISA stated that sharing with nonaffiliated third parties is limited because the "benefits of disclosing information must outweigh any competitive harm from releasing the information."[80] Citigroup stated that "there is a better opportunity to assess and ensure the practices of an affiliate in terms of information security, use of information, and other privacy matters," and noted further that "there are likely to be more

---

[75] Elder, p. 1.

[76] Geseli, pp. 1-4.

[77] *See, e.g.*, CFB, p. 2; Household, pp. 1-2; BofA, pp. 3-4; FleetBoston, p. 2; Capital One, p. 5; MBNA, pp. 2-3; Bank One, pp. 4-5; Citigroup, p. 10; MetLife, pp. 3-4; USAA, p. 2; NAMIC, p. 2; American Insurance Association (AIA), p. 2. Credit unions also expressed this view: Navy FCU, p. 1; Rogue FCU, p. 2.

[78] BofA, p. 3.

[79] VISA, p. 5.

[80] *Id.*, p. 11.

consistent practices among affiliates allowing for easier and less risky interfaces such as transporting and displaying data."[81] The SIA expressed a similar view:

> In general, more detailed and specific financial information is shared with affiliated entities in order to provide a customer with the opportunity to consider an affiliate's product. If the affiliate sharing is for anti-fraud purposes, the type of information shared may involve a wider range of information about the customer. More limited personal information…is shared with nonaffiliated service providers for the specific purpose of servicing and administering an account or providing other support for the financial products and services offered by the financial institution.[82]

FSRT maintained that, as a rule of thumb, firms provide nonaffiliates with as little information as is necessary for them to complete their support activities.[83] FSRT stated, "Financial firms are highly motivated to protect information because they bear the direct financial loss of misappropriated customer information as well as the loss in customer confidence."[84]

A number of commenters indicated that the type of information shared with third parties depends in large measure on the purposes for which it is to be used. Some credit union commenters indicated that they typically limit the information they share to fulfill transactions initiated by their members to name, address, telephone, and account information (e.g., types, balances, transaction history).[85] According to these commenters, a credit union may share transaction or experience information with its affiliate, a credit union service organization (CUSO), to enable the CUSO to market the credit union's products and services and to complete transactions that the member initiates.[86] NAFCU also noted that credit unions "may share credit information with affiliates if they either comply with the duties imposed on credit reporting agencies by the Fair Credit Reporting Act or offer the member the ability to opt out of such sharing."[87]

Because the type of information disclosed may be related to the purpose for the disclosure, the ABA noted little difference in the type of information shared with affiliates and nonaffiliated third parties, stating for example: "As a general rule, some financial institutions choose to offer customers a full range of financial services through affiliates, while others provide such services through third parties. In both cases, the information needed to offer or complete these financial transactions is essentially the same."[88] The National Association of Mutual Insurance Companies (NAMIC) agreed that they share the same types of information

---

[81] Citigroup, p. 14. See also Chapter IV regarding risks.

[82] SIA, p. 5.

[83] FSRT, p. 7.

[84] *Id*.

[85] *See, e.g.,* USA FCU, p. 1; Navy FCU, p. 1; Denali Alaskan Federal Credit Union (Denali FCU), p. 1; Rogue FCU, p. 2; NAFCU, p. 1.

[86] *See, e.g.,* NAFCU, p. 1; Navy FCU, p. 1. A CUSO that is controlled by a federal credit union is considered its affiliate under NCUA's privacy regulation, 12 C.F.R. §716.3(a).

[87] NAFCU, p. 1.

[88] ABA, p. 1.

with affiliates and nonaffiliated companies, but noted that "information is shared only on a 'need-to-know' basis, so only such information as is required to permit the affiliate or nonaffiliated third party to perform the function requiring customer data is actually shared."[89]

The American Insurance Association (AIA) stated that similar information is shared with affiliates and nonaffiliates; however, AIA noted, "insurers typically will provide less information to affiliates and nonaffiliated third parties in connection with the marketing of the products and services."[90] FSRT also stated that the amount of information shared with marketing partners is considerably less than that shared with affiliates or service providers.[91] Household Bank (Household) commented, "Marketing partners will … receive various amounts of customer information, depending upon the product offered and the nature of the relationship."[92]

### *EPIC et al., NAAG, and Individuals' Perspectives*

Transaction or experience information that financial institutions may share freely with affiliates, NAAG noted, "could include, for example, detailed information about a customer's purchases made on a credit card issued by the financial institution, as well as the customer's outstanding balance, whether the customer is delinquent in paying bills, and the length of time a customer has held a credit card."[93] Under FCRA, NAAG stated, the financial institution must notify the consumer and provide him or her with the opportunity to opt out before certain other types of information can be shared with affiliates, namely data from a consumer's credit application or credit report; information obtained by verifying representations made by a consumer; and information provided by another entity regarding employment, credit, or other relationships with a consumer.[94] This information might include income, credit score or credit history with others, open lines of credit with others, employment history with others, marital status, and medical history.[95]

EPIC et al. commented that detailed customer information has been disclosed to third-party marketers in exchange for commission income from the marketing effort. In one case, at least, they said such information included the following: credit cards, credit card numbers, dates of the last transaction, credit line information and whether a payment was delinquent or the account had exceeded the credit limit, numbers and amount of purchases each year and number and amount of purchases for year-to-date, cash advances, and the amount of finance charges the customer acquired per year.[96]

---

[89] NAMIC, p. 3.

[90] AIA, p. 3.

[91] FSRT, p. 7.

[92] Household, p. 2.

[93] NAAG, p. 3.

[94] *Id*., pp. 3-4.

[95] *Id*.

[96] EPIC et al., p. 9, citing to *In the Matter of Chase Manhattan Bank USA* (2000), stated: "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…Chase had contractual agreements with marketers to receive a percentage commission of any sales generated through the telemarketing and direct market 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 nonaffiliates only with express written consent (opt-

## CHAPTER III

## THE POTENTIAL BENEFITS OF INFORMATION SHARING AMONG FINANCIAL INSTITUTIONS AND THEIR AFFILIATES – FOR FINANCIAL INSTITUTIONS, THEIR AFFILIATES, AND THEIR CUSTOMERS

### INTRODUCTION

Congress requested that the Treasury Department study the potential benefits for financial institutions, affiliates, and customers of information sharing among financial institutions and their affiliates.[97] The FRN also requested commenters' insights as to any effects that would result from placing further limitations on this type of information sharing.[98]

### BENEFITS OF SHARING INFORMATION WITH AFFILIATES

#### *Financial Services and Other Industry Perspectives*

Generally, industry commenters viewed information-sharing practices among affiliates as integral to the financial modernization anticipated by enactment of GLBA. NAMIC, for example, noted that the benefits to its member companies of sharing customer information with affiliates "relate directly to the primary purpose of financial modernization under GLBA: to permit the integration of financial services – insurance, banking and securities – so that financial institutions may serve consumers through a central point of contact."[99] SIA echoed this view and explained that customers see affiliated financial institutions as a single organization that can provide integrated financial solutions to their needs. The association stated that customers expect the organization to use information about them "in a manner that facilitates access to all services and products that might meet their particular financial goals."[100]

Commenters mentioned that when products and services are bundled and marketed to a targeted receptive audience, customer satisfaction increases due to decreased costs and the availability of attractive, tailored products, and concomitantly, the financial institution's revenues improve.[101] "Cross-selling," Bank One stated, "is the key to increased profitability for most banks."[102] Bank One noted, "The incidental cost is small to supply a new financial product

---

in)." [Note: Chase settled with the New York Attorney General in January 2000 without admitting any wrongdoing and agreed to pay $101,500 as costs.]

[97] GLBA, § 508(a)(4) and (5).

[98] FRN, 67 Fed. Reg. 7215, 4(e) and 5(e) (2002). Comments in response to question 5(d) regarding alternatives to achieving the same or similar benefits without such sharing of information among financial institutions and their affiliates are reflected in Chapter VI.

[99] NAMIC, p. 11.

[100] SIA, p. 10.

[101] *See, e.g.,* E*Trade, p. 5; Navy FCU, p. 4; Wells Fargo, p. 6; ABA, pp. 4,5; CUNA Mutual, p. 6; SIA, pp. 8,10; VISA, p. 7; CFB, p. 6; USAA, pp. 4,5; CTBA, p. 9; FleetBoston, p. 8; NAFCU, p. 2; Intuit, pp. 5,6; Bank One, p. 2.

[102] Bank One, p. 2.

to a customer with whom the bank already does business. Economies of scale and improved customer satisfaction result from cross-selling products."[103]

Centralized data management, BofA noted, enables it to meet customer expectations regarding, for example, access to comprehensive account information, expedited processing of loan applications, linking of accounts for overdraft protection, honoring customers' stated preferences with respect to e-mail and telemarketing, and offering customer discounts or services that reflect a customer's total relationship with the financial institution.[104] NAMIC noted that this sharing of consumers' information creates a greater possibility for companies to understand and assist their customers with a diversity of products over a period of time.[105]

A number of commenters also noted that another benefit of information sharing is to reduce the likelihood that customers will receive unwanted telemarketing calls and junk mail. Since firms waste money when they advertise to an unreceptive audience, they use information to tailor services or offers to customers where there is a sufficient likelihood of interest, focusing as much as possible on individual needs.[106] For example, FSRT noted that if companies could not share information among affiliates, its members would send out over three times as many solicitations to achieve the same level of sales.[107]

As indicated earlier, commenters asserted that information sharing also may result in better pricing for consumers. As noted earlier, one insurer stated that it is routine in the auto insurance business to submit a consumer application to several affiliated companies to obtain a premium rate that is appropriate to the risk involved. This helps assure, the commenter notes, that the "risk is properly underwritten and priced and that customers with better driving records are not paying higher premiums in order to subsidize losses on policies issued to higher risk drivers."[108] Citigroup wrote, for example:

> It is generally accepted that customers can borrow at significantly lower interest rates in the U.S. as a result of the information sharing facilitated by the FCRA. These benefits have been addressed in various reports that contrast U.S. markets and other global markets in the penetration, pricing, and competitiveness of credit products. This is largely due to the fact that FCRA encourages and facilitates more accurate, standard, and timely information for making credit decisions.[109]

Intuit stated that providing tax preparation software to its customers along with current mortgage rate information from Quicken Loans, one of its affiliates, not only reduced customer acquisition costs and lowered overhead, but also allowed customers to receive better loan rates without having to spend an extensive amount of time shopping.[110]

---

[103] *Id*.

[104] BofA, pp. 4-5.

[105] NAMIC, p. 13.

[106] *See, e.g.,* E*Trade, p. 5; ACLI, p. 11; ABA, p. 5; Household, p. 7; USAA, p. 5; FSRT, p. 15.

[107] FSRT, p. 15.

[108] MetLife, p. 5.

[109] Citigroup, p. 19.

[110] Intuit, p. 6.

FSRT, citing a survey of its members published in 2000, reported that information sharing saves its members' customers $17 billion per year and 320 million hours of time, amounting to $195 per customer household.[111] The survey attributed savings of $8 billion and 115 million hours to sharing information with affiliates.[112] FSRT noted that the survey also indicated that its members save about $1 billion per year by using targeted marketing instead of mass marketing, savings which can be passed to customers.[113]

Fraud prevention and detection were often cited as benefits of information sharing, as indicated in Chapter II. BofA explained the issue:

> Managing information centrally also lets us see unusual activity and variations – a powerful tool to protect our customers from fraud and identity theft and to help victims recover. For example, we may use information about a customer's ATM, credit card and check card transactions to identify any unusual activity, and then contact that customer to determine if their card has been lost or stolen.[114]

Citigroup noted, "Fraud prevention is also very important for other types of accounts, such as insurance, banking, and brokerage."[115] ACB explained that information sharing in fraud detection programs not only helps to protect consumers, but is a key risk management tool for banks of all sizes.[116]

Citigroup indicated that affiliates benefit from information sharing in much the same way as the financial institution from which they receive information. Citigroup noted that affiliates may specialize in manufacturing products, while others may specialize in distribution or in operational efficiencies.[117] Thus, the banking organization stated, "By working together, each affiliate can focus on what it does best and also have a ready channel for products, distribution, and other elements that it does not have."[118] Additionally, Citigroup noted that financial institutions also achieve operational efficiencies resulting from the cross training, licensing, and employing of staff in order to service their various affiliates.[119]

Commenters stated that an affiliate also may benefit from the information received from another affiliate that it shares with a nonaffiliated third party.[120] These benefits are similar to benefits financial institutions receive when sharing information directly with an affiliate. The affiliate that ultimately receives the information may, for example, be able to make additional products and services available to its customers and generate revenues that enable that affiliate to

---

[111] FSRT, p. 14, citing to "Customer Benefits from Current Information Sharing by Financial Services Companies," Ernst & Young, December 2000.

[112] *Id*.

[113] *Id*., p. 15.

[114] BofA, p. 6.

[115] Citigroup, p. 22.

[116] ACB, p. 5.

[117] Citigroup, p. 21.

[118] *Id*.

[119] *Id*.

[120] *See, e.g.,* VISA, p. 20; E*Trade, p. 4; MetLife, p. 12; ACLI, p. 10; Household, p. 7; FSRT, pp. 13-14; NAMIC, p. 14; MBNA, p. 11, CFB, p. 6.

provide products and services at more competitive prices.[121] Citigroup, on the other hand, asserted that benefits in this case are slim because this type of information is considered "non-transactional and non-experiential" and thus restricted under FCRA. Consequently, such information sharing would be rare.[122]

### *EPIC et al., NAAG, and Individuals' Perspectives*

EPIC et al. commented that "mega-mergers" that pool customer information and cross sell products introduce a different kind of risk to customers, "the inability to exercise meaningful control and oversight over personal data."[123] They support the opt-in approach as a means of preserving consumer control. "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," they stated.[124] They added the following observation:

> 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 able to make the decision whether actual benefits outweigh the invasion of privacy.[125]

Mr. Olsen stated, "If financial organizations are going to share or otherwise sell information about me, I should get a piece of the action." He continued, "If not offered a chance to participate in the financial benefits derived from such transfers, all such transfers should be strictly prohibited."[126] Mr. Cochran concurred, "No member of government has the right to legislate away my privacy."[127]

## BENEFITS OF SHARING INFORMATION WITH NONAFFILIATES

### *Financial Services and Other Industry Perspectives*

Commenters generally noted that sharing information with a nonaffiliated third party created many of the same benefits as sharing the information with affiliates.[128] Outsourcing was seen, as noted in Chapter II, as helping financial institutions offer additional products and services to customers in cases where the financial institution itself does not have the infrastructure or resources to provide certain types of services, such as credit cards. MBNA America Bank (MBNA) stated, for example, "With respect to joint marketing agreements between two or more financial institutions, information sharing allows immediate service of the customer at any point of contact and a seamless interface from the customer's perspective."[129]

---

[121] *Id*.

[122] Citigroup, pp. 21, 22. See also Chapter II for FCRA explanation.

[123] EPIC et al., p. 7.

[124] *Id*. See Chapter VI for more discussion of opt in versus opt out.

[125] EPIC et al., p. 12. As noted earlier, EPIC et al., NAAG, and individuals identified many risks from information sharing, which are outlined in more detail in Chapter IV.

[126] Olsen, p. 1.

[127] Cochran, p. 1.

[128] *See, e.g.,* ABA, p. 1; NAMIC, p. 3; AIA, p. 3; Household, p. 2; FSRT, p. 7.

[129] MBNA, p. 10.

Insurers, as noted in Chapter II, commented that they rely on sharing information with nonaffiliated entities for basic business functions that benefit consumers directly. NAMIC, for example, stated that its member companies "could not continue to function in the business of insurance without sharing customer information with nonaffiliated third parties," because such information sharing is essential to the claim adjustment process, rating analyses, and the detection of fraud.[130] The association commented further, "Our member companies' customers benefit from the sharing of their information with nonaffiliated third parties every time a claim is presented and a loss is resolved more quickly because an auto repair shop or claim adjustment firm has access to customer information."[131] ACLI noted, in a wider context, that information sharing makes a "vibrant reinsurance market" possible by allowing risks to be shared broadly, thus opening access to life, disability income, and long-term care insurance to a wider pool of potential customers.[132]

CUNA Mutual Group (CUNA Mutual) declared, "For members of small and medium sized credit unions, increased product selection arising from their credit unions' relationships with nonaffiliated third parties provides convenience and value [to consumers] through their preferred financial institution."[133] ACB noted that community banks share information in ways that help ensure funding is available for homeownership: "By participating in the secondary mortgage market, community banks have access to an important source of capital that enables them to provide affordable home loans to consumers."[134] Without the ability to share information that is necessary for secondary mortgage transactions, the group commented, "consumers would be faced with increased lending costs that could price some families out of homeownership."[135] In addition, ICBA noted that community based banks may bring financial products and services to rural areas not served by larger institutions.[136]

Denali Alaskan Federal Credit Union (Denali FCU), by contrast, declared that, outside of transacting business originated through the financial institution and involving third parties, there are no benefits for consumers when their financial institutions share information with nonaffiliated third parties.[137]

### *EPIC et al., NAAG, and Individuals' Perspectives*

EPIC et al. stated, "Consumers have not been adequately informed or been given effective choice to evaluate the benefits of information-sharing against the potential harms caused by unrestricted information-sharing."[138] These groups generally did not discuss specific benefits; rather, they focused on potential risks to consumers from information sharing.

---

[130] NAMIC, p. 11.

[131] *Id*., p. 13.

[132] ACLI, p. 11.

[133] CUNA Mutual, p. 6.

[134] ACB, p. 3.

[135] *Id*.

[136] ICBA, p. 3.

[137] Denali FCU, p. 3.

[138] EPIC et al., p. 4.

## CHAPTER IV

## INFORMATION SHARING BY FINANCIAL INSTITUTIONS WITH THEIR AFFILIATES AND WITH NONAFFILIATES: POTENTIAL RISKS FOR CUSTOMERS

### INTRODUCTION

Congress requested that the study examine the potential risks for customer privacy when financial institutions share confidential personal information with affiliates and nonaffiliated third parties.[139] The prevailing U.S. law and regulation provided consumer protections that sought to limit risks to consumers from having their personal nonpublic information disclosed to entities other than the financial institution that collected it.

### Background

Those who responded to the FRN operated in a complicated statutory environment. The GLBA and its implementing information-sharing regulations required a financial institution to make clear and conspicuous disclosures to its customers regarding the types of information it collects and discloses, the types of affiliates to whom it discloses that information (except for affiliates to whom information is disclosed under the exceptions in the Joint Regs. §§ __.14 and __.15), and the FCRA disclosures described below.[140]

Financial institutions operated under an FCRA that required them (and others), before sharing certain personal information with affiliates regarding aspects of a consumer's credit status (such as standing, worthiness, reputation), to make a clear and conspicuous disclosure to the consumer in order to avoid being considered a consumer reporting agency. The financial institution's disclosure to the consumer would indicate that this information could be shared among its affiliates and would give the consumer an opportunity to forbid this type of information sharing.[141] No parallel provision existed within FCRA for sharing consumer reports with nonaffiliated third parties; thus, a financial institution ran the risk of becoming a consumer reporting agency, and subject to that regulatory structure, by disclosing such information to nonaffiliated third parties.

FCRA, however, did not restrict a financial institution's disclosure of information to affiliates or nonaffiliated third parties regarding a customer's transaction or experience with that institution, e.g. his or her payment history. The statute also prohibited states from enacting laws that limited information sharing among affiliates.[142]

---

[139] GLBA, § 508(a)(3). Note: This chapter describes statutory provisions in effect at the time of the Study. It does not describe or reflect subsequent amendments.

[140] GLBA, § 503; Joint Regs. § ___.6 (a). See also Joint Regs. §§ __.14 and __.15 and §§ 7, 16, and 17 of the NAIC Model Privacy Regulation.

[141] FCRA, § 603(d)(2)(A)(iii). See note to footnote 139.

[142] *Id*., §§ 624(b)(2) and (d)(2). (Note: This chapter describes statutory provisions prevailing at the time of the Study, when the prohibition on state action in this respect was scheduled to expire on January 1, 2004.)

GLBA, as noted in Chapter II, imposed a number of restrictions on financial institutions' ability to share consumer information with nonaffiliated entities. Financial institutions faced restrictions on transfers of nonpublic personal information by them to a nonaffiliated third party under GLBA and its implementing regulations, including:

- limits on a third party's reuse and redisclosure of customer information received from a financial institution;[143]
- a written contract to protect the confidentiality of the customer information a financial institution discloses to service providers, including joint marketing partners and agents that perform marketing activities for the institution (in lieu of providing consumers an opportunity to opt out of these disclosures);[144]
- a prohibition against the disclosure by a financial institution of customer account numbers to third parties for marketing, unless the numbers are encrypted;[145]
- a requirement that an information disclosure notice and the opportunity for the consumer to opt out are provided;[146] and
- a prohibition on disclosure if the consumer has opted out.[147]

A third party faced limits on reuse and redisclosure of the nonpublic personal information it received from a nonaffiliated financial institution, which could vary depending on the circumstances of the information transfers. The most stringent limits on a third party's reuse and redisclosure of the nonpublic information received from a nonaffiliated financial institution applied to nonaffiliated third parties, such as service providers, that received the information under one of the exceptions to the general notice and opt-out provisions in GLBA §502(e) and Joint Regs. §§ __.14 and __.15. Generally, under these exceptions, a financial institution could provide information to third parties to conduct routine business, such as to complete customer initiated transactions and to report to credit bureaus, without having to offer customers an opt out of these disclosures.[148]

Under Joint Regs. § __.11, when a nonaffiliated third party received information under an exception in § __.14 or § __.15, the third party might use or further disclose the information only in the ordinary course of business to carry out the activity for which the third party was provided the information. For example, a company that received a customer list from a nonaffiliated financial institution to perform account processing activities could use that information to perform the services, or to respond to a subpoena. However, the company could not use the

---

[143] GLBA, § 502(c); Joint Regs., § __.11. This corresponds with § 13 of the NAIC Model Privacy Regulation. This is not a restriction on the financial institution's ability to transfer information, but a restriction on the nonaffiliate's ability to use or redisclose the information.

[144] GLBA, § 502(b)(2); Joint Regs., § __.13. This corresponds with § 15 of the NAIC Model Privacy Regulation. This is not a restriction on the financial institution's ability to transfer information, but a restriction on the nonaffiliate's ability to use or redisclose the information.

[145] GLBA, § 502(d); Joint Regs., § __.12. This corresponds with § 14 of the NAIC Model Privacy Regulation.

[146] GLBA, § 502(b)(1); Joint Regs., § __.10.

[147] *Id*.

[148] GLBA, § 502(e); Joint Regs., §§ __.14, __.15. These correspond to §§ 16, 17 of the NAIC Model Privacy Regulations.

information for its own marketing purposes or to further disclose it to any other third party for marketing.[149]

Third parties would find the limits on reuse and redisclosure the least restrictive when the third party received the information from a nonaffiliated financial institution such as for the third party's own marketing purposes, where the institution offered the customer but the customer did not exercise the option to opt out. Under Joint Regs. § __.11, no additional limits on the third party's use of the information applied, and the third party's disclosure of the information was limited to that which was consistent with the financial institution's information use notice. It was clear that the third party would be bound by any opt-out election that a customer of the financial institution might exercise subsequent to the time that the nonaffiliated third party received the customer's information. [150]

The statute and the regulations further required financial institutions to enter into confidentiality agreements with nonaffiliated third party service providers, including joint marketing partners and agents that perform marketing activities for the institution, to protect customer information (where the institution is not required to afford its customers the opportunity to opt out of such arrangements). Under Joint Regs. § __.13, the financial institution would need to enter into a written contract with the third party generally prohibiting the third party from using or disclosing the information other than to carry out the purposes for which the information was provided. [151]

In addition, as mentioned in Chapter II, a financial institution would be prohibited from disclosing a decoded account number, access number, or access code for a customer's credit card, deposit, or transaction account to a nonaffiliated third party for use in marketing.[152] An account number could be provided in an encrypted manner so long as the third party was unable to decode the information.[153]

Section 501(b) of GLBA established further safeguards on the transfer of nonpublic personal information to third party service providers. These safeguards have been issued as regulatory guidelines by the banking agencies and NCUA and as regulations by the FTC, SEC, and CFTC. State insurance regulators promulgated rules based on the NAIC Model Regulation on such safeguards and states were acting upon them.[154]

---

[149] Joint Regs., § __.11. Joint Regs., § __.11(a)(1) of the rules provides that the third party may also disclose the information to an affiliate of the financial institution that initially provided the information, and to the third party's own affiliate, except that the third party's affiliate may only use and disclose the information to the same extent as could the third party. This corresponds to NAIC Model Privacy Regulation, § 13.

[150] Joint Regs., § __.11. This corresponds to § 13 of the NAIC Model Privacy Regulation.

[151] GLBA, § 502(b)(2); Joint Regs., § __.13. This corresponds to § 15 of the NAIC Model Privacy Regulation.

[152] GLBA, § 502(d); Joint Regs., § __.12(a). This corresponds to §14(a) of the NAIC Model Privacy Regulation.

[153] Joint Regs., § __.12(c). This corresponds to § 14(c) of the NAIC Model Privacy Regulation.

[154] OCC, 12 C.F.R. Part 30; FRB, 12 C.F.R. Parts 208, 211, 225, 263; FDIC, 12 C.F.R. Parts 308, 364; OTS, 12 C.F.R. Part 568, 570; NCUA, 12 C.F.R. Part 748; FTC, 16 C.F.R. Part 314; SEC, 17 C.F.R. Part 248; CFTC, 17 C.F.R. Part 160. See also NAIC Standards for Safeguarding Customer Information Model Regulation (NAIC Model Safeguarding Regulation), promulgated in 2002, and Chapter V for discussion on the security safeguards.

## POTENTIAL RISKS TO CUSTOMERS WHEN FINANCIAL INSTITUTIONS SHARE INFORMATION WITH AFFILIATES

### *Financial Services and Other Industry Perspectives*

Most of the industry commenters maintained that information sharing with affiliates poses minimal risks to the security of customer information. A substantial number of commenters stated that the risks involved in sharing information with affiliates were essentially no greater than when customers transact business with a single institution.[155]

Wells Fargo commented that the three types of risks usually ascribed to information sharing -- risk of financial loss due to fraud, risk of unwanted intrusions, and risk of inappropriate use of certain types of information -- do not materially differ whether the recipient of the information is an affiliate, another financial institution providing complementary financial products and services, an affinity or private label partner, or a service provider.[156] The bank stated that there is little evidence that planned information sharing with affiliates or other nonaffiliated parties is a significant contributor to identity theft. Rather, Wells Fargo contended that the free flow of information is essential to detect and prevent fraud. Wells Fargo also noted that information sharing results in more selective marketing, thus reducing the amount of unwanted solicitations. In addition, Wells Fargo suggested that to the extent there are policy concerns about specific uses of data, such as medical information, those uses should be restricted rather than restricting the underlying information sharing.[157]

This position was echoed by the Center for Information Policy Leadership (CIPL) at Hunton & Williams, which stated that "the legislative and policy focus should be on … risky and inappropriate applications rather than on the underlying information flows themselves."[158] CIPL wrote, "The consumer is simply not aware that information flows are the foundation for the conveniences they demand from the organizations with which they do business," such as immediacy of service, availability of instant credit, and Internet access to account balances.[159]

CUNA Mutual noted that there is little risk that an affiliate would not have the same level of information-sharing security practices in place as do other entities within the company, due to the substantial similarity in regulatory requirements adopted among financial services regulators.[160] Additionally, VISA commented that many holding companies have established company-wide privacy officers that work to ensure consistent treatment of consumer information across affiliated companies.[161] SIA noted that affiliates have an interest in maintaining a

---

[155] *See, e.g.,* CFB, pp. 3-4; MetLife, p. 9; Navy FCU, p. 3; ABA, p. 4; MBNA, p. 8; Denali FCU, p. 2; FleetBoston, p. 7; Rogue FCU, p. 4; Bank One, p. 8; Wells Fargo, pp. 1-2, 6; BofA, p. 5; ACLI, p. 8; NAMIC, p. 9; AIA, p. 6; FSRT, p. 11; SIA, p. 7.

[156] Wells Fargo, p. 6.

[157] *Id*., pp. 5-6.

[158] CIPL, p. 6.

[159] *Id*., p. 5.

[160] CUNA Mutual, p. 4.

[161] VISA, p. 16.

common reputation for customer satisfaction, thus assuring that personal information is protected, a point echoed by NAFCU.[162]

Additionally, many commenters stated that while there are always some risks in sharing information, these risks are offset by the benefits of sharing or by the risks incurred by not sharing information.[163] Citigroup stated that prohibiting the sharing of information with an affiliate could have a large impact on consumers since missing or inappropriate information may prevent companies from (1) providing customers with investment choices based on appropriate risk profiles, (2) updating addresses and phone numbers, (3) making other significant changes across accounts, or (4) properly identifying an applicant with prior credit problems or criminal activity.[164] Additionally, BofA focused on such risks as the failure to transfer a credit card payment made at a banking center to the credit card account in a timely manner, or the risk that affiliates will not know or honor a bank customer's direct marketing preferences, and the risk that a single call by a customer to the service center about a stolen wallet will not suffice as notice regarding the loss of credit cards.[165]

***EPIC et al., NAAG, and Individuals' Perspectives***

EPIC et al. and NAAG commented extensively that existing legal and regulatory controls on sharing of customer information were not sufficient and that consumers should have greater control over the use and disclosure of information about them.[166] EPIC et al. asserted:

> 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.[167]

As noted in Chapter II, NAAG and EPIC et al. raised concern that some of the largest financial organizations have hundreds or possibly thousands of affiliates and, as a result, may be engaged in broad-ranging activities, including many that may not be considered traditional financial activities, thus raising the potential for risks when information is shared among affiliates.[168] NAAG commented generally, "It may well be that the greater the quantity and level of detail of confidential information and the more entities that possess such information, the higher the chance that the information will be stolen or misappropriated, or used for purposes, such as the improper denial of credit, insurance, or employment."[169]

---

[162] SIA, p. 7; NAFCU, p. 2.

[163] *See, e.g.,* CTBA, p. 7; FSRT, p. 11; ABA, p. 4; MBNA, pp. 8-9; USA FCU, p. 1; Citigroup, p. 18; Wells Fargo, pp. 1-2, 5-6; Intuit, pp. 4-5; BofA, p. 5; FleetBoston, p. 7.

[164] Citigroup, p. 18.

[165] BofA, p. 5.

[166] EPIC et al., p. 6.

[167] *Id*., p. 13.

[168] NAAG, pp. 11-16; EPIC et al., p. 6

[169] NAAG, p. 11.

To reiterate, with respect to affiliates, EPIC et al. commented that the collection of transaction or experience information enables affiliates to track information unrelated to financial services or products, such as religious, political, dietary, medical and lifestyle information.[170] Within this "financial supermarket" structure, they stated, "Even with a history of spotless credit, an individual, profiled on undisclosed factors, can end up paying too much for a financial service or product."[171] Further, as indicated in Chapter II, EPIC et al. wrote that both affiliate sharing and joint marketing agreements have resulted in "aggressive, deceptive negative option sales of memberships" and increased the flow of junk mail and other unwanted solicitations.[172]

## POTENTIAL RISKS TO CUSTOMERS WHEN FINANCIAL INSTITUTIONS SHARE INFORMATION WITH NONAFFILIATED THIRD PARTIES [173]

### *Financial Services and Other Industry Perspectives*

While a number of industry commenters suggested that there is a slightly higher risk in sharing information with nonaffiliated third parties than there is with affiliates, they generally maintained that these risks could be contained or are minimal.[174] ACLI, for example, stated, "nonaffiliated third party recipients of nonpublic personal information from an insurer or an affiliate of an insurer are in effect, subject to the breadth of the broad privacy requirements under the GLBA," and thus do not pose new risk to consumers.[175] Another commenter noted that the "influence of the market place coupled with GLBA customer safeguard requirements to review a third party's customer information sharing practices minimizes potential privacy risks in the nonaffiliated third party information sharing context."[176]

Some asserted that the risks of this type of information sharing would largely derive from the third party's failure to honor or comply with the contract it entered into with the financial institution.[177] Others noted that financial institutions can overcome any differences in security standards or policies through careful attention to contractual obligations binding nonaffiliates to protect customer information.[178]

A few commenters specifically addressed the impact of a company's *redisclosure* of information (received by an affiliate) to a nonaffiliated entity. Of those who addressed this issue, some stated that either no risks are involved in this type of information sharing or that while risks do exist, they are no different from the risks associated with other information sharing with

---

[170] EPIC et al., p. 5.

[171] *Id*., pp. 5-6.

[172] *Id*. See the *NationsSecurities Case* in Chapter II, involving sharing information among affiliates.

[173] This section also includes a discussion of the situations where a company receives information from an affiliated financial institution and then discloses the information to a nonaffiliated third party.

[174] *See, e.g.,* E*Trade, p. 3; VISA, p. 17; Citigroup, p. 19; CTBA, p. 8; NAMIC, p. 10; FleetBoston, p. 7; Bank One, p. 8; CFB, p. 4; NAFCU, p. 2; Navy FCU, p. 4; Rogue FCU, p. 4; SIA, p. 8; ABA, p. 4; FSRT, p. 11; CUNA Mutual, p. 4.

[175] ACLI, p. 9.

[176] CUNA Mutual, p. 4.

[177] *See, e.g.,* CFB, p. 5; SIA, p. 8.

[178] *See, e.g.,* Bank One, p. 8; E*Trade, p. 3; Rogue FCU, p. 4.

nonaffiliated third parties.[179] A few commenters noted that GLBA specifically limits this type of information sharing, minimizing the threat to consumers.[180] Citigroup, as noted earlier, stated that FCRA also places limitations on this type of information sharing.[181]

### *EPIC et al., NAAG, and Individuals' Perspectives*

As indicated throughout this report, EPIC et al. shared many concerns about the risks they view stemming from current law and practice.[182] Both EPIC et al. and NAAG expressed concerns, as mentioned earlier, about risks from aggressive and deceptive marketing practices.[183] Information sharing, they wrote, means 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.[184] EPIC et al. also asserted that 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."[185]

EPIC et al. regarded the GLBA exception to the opt-out requirement for joint marketing arrangements as a "loophole" that "allows for precisely the kind of behavior the GLBA is supposed to restrict" and added that "the loophole is particularly troubling given the broad definitions of 'financial institution' and 'financial service or product' adopted for the purposes of the GLBA."[186] EPIC et al. also stated, "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."[187] EPIC et al. noted that most of the cases brought by state attorneys general in recent years involved a large bank that shared its customer information in return for a percentage of sales revenue.[188]

As noted earlier, such activity may take the form of preacquired account telemarketing, which NAAG stated, "turns on its head the normal procedures for obtaining consumer consent…the telemarketer not only establishes the method by which the consumer will provide consent, but also decides whether the consumer actually consented."[189] Citing one particular

---

[179] *See, e.g.,* E*Trade, p. 4; MBNA, p. 10; Bank One, p. 9; NAMIC, p. 10; VISA, p. 17; FSRT, p. 12; Fleet Boston, p. 7; Navy FCU, p. 4; CUNA Mutual, p. 4.

[180] *See, e.g.,* VISA, p. 17; CUNA Mutual, p. 4; Fleet Boston, p. 7. See also GLBA, § 502; Joint Regs., § __.10.

[181] Citigroup, p. 19.

[182] EPIC et al., p. 4.

[183] EPIC et al., pp. 5-7; NAAG, pp. 6-7, 12.

[184] *Id*., pp. 10-12.

[185] *Id*, pp. 11-12.

[186] EPIC et al., p. 10.

[187] *Id*., pp. 8-10.

[188] *Id*. Like NAAG, EPIC et al. explained that the telemarketers' use of a script characterizing the sale as a "free trial offer" combined with the fact that the consumer did not provide an account number to make a charge "leads the consumer to believe that she has not made a purchase." EPIC et al. questioned whether such third parties that gain access to personal information under the joint marketing provision will be held accountable for any future use of the information, or whether there are adequate controls over their reuse of the information.

[189] NAAG, p. 9.

case, NAAG noted that it represented only one known example of the risks to consumers from having their information shared in this way, whether with affiliates or third parties. NAAG continued:

> There are other types of risks that are suspected but not yet proven, and undoubtedly still others that are as yet unknown to consumers or enforcement agencies. The harm suffered may not always be quantifiable; and even where clear economic loss is present, the relationship of that loss to the disclosure of a consumer's confidential information may not be obvious or capable of clear proof.[190]

NAAG also cited the sharing of encrypted account numbers and other billing information as dangerous in this context.[191] NAAG saw no practical difference between providing encrypted numbers or providing the decoded ones, which GLBA prohibits from disclosure. The telemarketer is able to notify a financial institution that a particular customer has purchased an item and the financial institution will use its decode mechanism to put the charge on the customer's account.[192] The group supported elimination of preacquired account telemarketing.[193]

Individual commenters also stated that they feel that their privacy is put at risk by information sharing. Mr. Lutz, a bank examiner by trade, asserted, "There is something seriously wrong with the way businesses get away with [the] free flow of customer information." He continued, "They require very personal confidential information for you to do business with them and then can share most of it in many cases and damned near all of it with affiliates. These days a bank can affiliate with nearly any type of business."[194]

---

[190] *Id*, p. 11. See e.g., *Minnesota v. Fleet Mortgage Corp*., 158 F. Supp. 2d 962 (D. Minn. 2001). Quoting a separate document prepared by state attorneys general, NAAG noted: "Fleet Mortgage Corporation, for instance, entered into contracts in which it agreed to charge its customer-homeowners for membership programs and insurance policies sold using preacquired account information. If the telemarketer told Fleet that the homeowner had consented to the deal, Fleet added the payment to the homeowner's mortgage account. Angry homeowners who discovered the hidden charges on their mortgage account called Fleet in large numbers." Fleet agreed to pay restitution to the customers and to stop the disputed practices.

[191] NAAG, pp. 7-9.

[192] *Id*., p. 8.

[193] *Id*., p. 11.

[194] Lutz, p. 1.

## CHAPTER V

## ASSESSING LAW AND REGULATION

### INTRODUCTION

Congress mandated that, in undertaking this study of information-sharing practices among financial institutions and their affiliates, the Treasury Department assess the laws and protections for customer information that were in place.[195] This chapter focuses on the prevailing protections afforded under FCRA and GLBA when the commenters responded to the FRN. These included those pursuant to both GLBA § 501(b) regarding standards relating to administrative, technical and physical safeguards, and the disclosure provisions that have been outlined in some detail in Chapters II and IV. Commenters were asked to describe the kinds of measures that financial institutions had in place and to assess whether any new or revised statutory requirements might be useful.[196]

GLBA directed the Federal functional regulators, the FTC, and state insurance authorities to establish standards requiring all financial institutions to implement administrative, technical and physical safeguards to: (1) ensure the security and confidentiality of customer records and information containing nonpublic personal information; (2) protect against any anticipated threats or hazards to the security or integrity of such records and information; and (3) protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to customers.[197]

As discussed, the Federal banking agencies and the NCUA issued guidelines and the FTC, SEC, and CFTC issued regulations requiring, in general, that each financial institution implement a comprehensive information security program appropriate to each institution. As part of developing its information security program, most of the federal agencies explicitly required that each financial institution conduct an assessment of the reasonably foreseeable risks to its customers' information and customer information systems, and correspondingly, design and implement appropriate measures to protect against those identified risks.

A financial institution's information security program generally had to ensure that its service providers also implemented reasonable safeguards designed to meet the objectives set forth in the guidelines and regulations. Financial institutions generally were required to monitor, evaluate, and adjust their safeguards in light of relevant changes in technology, the sensitivity of customers' information, their operations or business arrangements, and other factors that affect the quality of their information security programs.

---

[195] GLBA, §§ 508(a)(2) and (a)(6).

[196] FRN, 67 Fed Reg. 7214-15 (2002).

[197] GLBA, § 501(b); OCC, 12 C.F.R. Part 30; FRB, 12 C.F.R. Parts 208, 211, 225, 263; FDIC, 12 C.F.R. Parts 308, 364; OTS, 12 C.F.R. Part 568, 570; NCUA, 12 C.F.R. Part 748; FTC, 16 C.F.R. Part 314; SEC, 17 C.F.R. Part 248; CFTC, 17 C.F.R. Part 160. See also NAIC Model Safeguarding Regulation.

GLBA and FCRA provisions regarding the appropriate disclosure of personal financial information to other entities have been described in Chapters II and IV.[198] GLBA established rules for financial institutions' disclosure of customer personal financial information to nonaffiliated third parties. FCRA established parameters for disclosing consumer report information to any third party, including affiliates, and permitted the sharing of customer transaction or experience information with affiliates without restriction.[199]

## ASSESSING THE EXISTING LAWS

### *Financial Services and Other Industry Perspectives*

Financial sector commenters generally were satisfied with the statutory and regulatory requirements for administrative, technical and physical safeguards that existed. Several praised the flexibility of the safeguards in accommodating firms' current needs while allowing firms to react to future developments.[200] MBNA explained, "GLBA and the Guidelines provide a useful framework of basic conceptual requirements without driving financial institutions toward particular solutions that may be ineffective tomorrow."[201] Many commenters noted that the mandatory rules were met or exceeded by practices and procedures that were common to the safeguarding of customer information before GLBA.[202]

SIA noted some of the electronic and procedural safeguards its members use, including controls on access to nonpublic personal information, use of firewalls and encryption, training programs, and contractual restrictions on nonaffiliated third parties.[203] Other institutions listed safeguards that include the use of electronic and physical access authentication tools, such as passwords, keycards, badges, or personal identification numbers, adherence to security and ethics policies, employee background investigations and training programs, and regular internal and external examinations.[204] ABA noted similar protections and emphasized its members' attention to risk assessment and risk management and the importance of maintaining up-to-date continuity of operations and disaster recovery plans that adhere to Federal Financial Institutions Examination Council guidelines.[205]

Insurance trade associations provided lists of commonly used protections that largely parallel those previously mentioned. They cited the necessity of identifying possible threats to information security and recognized the importance of limiting physical and Internet access to information as much as possible, and to do so by using a range of methods with varying levels of

---

[198] As noted in Chapter I, other laws and regulations, such as the USA PATRIOT Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their regulations, are beyond the scope of this report.

[199] GLBA, § 502; FCRA, § 603(d)(2)(A)(i). This chapter describes GLBA as originally enacted and FCRA as in effect in 1999.

[200] *See, e.g.,* CUNA Mutual, p. 3; NAFCU, p. 2; BofA, p. 4; FleetBoston, p. 6; FSRT, p. 10; Bank One, p. 7; MBNA, p. 7; VISA, p. 15; USAA, p. 4; MetLife, p. 8.

[201] MBNA, p. 7.

[202] *See, e.g.,* NAMIC, p. 8; ACLI, p. 7; MetLife, p. 7; VISA, pp. 14-15; FleetBoston, p. 6; Household, p. 4; Wells Fargo, p. 4; MBNA, p. 7; Bank One, p. 7; CTBA, p. 7; ABA, p. 3; ACB, p. 4.

[203] SIA, p. 7.

[204] *See, e.g.,* Household, p. 4; Bank One, pp. 6-7; FleetBoston, p. 6.

[205] ABA, p. 3. See also ICBA, p. 4.

sophistication, from encryption to key cards and voice recognition.[206] The associations noted that for the insurance industry generally, the key source of guidance was the model security regulation adopted by the NAIC. States were in the process of adopting the NAIC Model Regulation on Standards for Safeguarding Customer Information.[207]

Most industry commenters also expressed satisfaction with the current laws and implementing regulations relating to the appropriate disclosure of customer nonpublic personal information.[208] Some cautioned against prematurely revising rules that are relatively new and not fully tested by experience.[209] As discussed elsewhere in this report, GLBA requires each financial institution to provide a notice to customers describing its information-sharing practices, and to provide its customers with an opportunity to prevent, or opt out of, certain disclosures of information to third parties.[210] MetLife commented, for example, that GLBA, FCRA, and various other federal and state laws in this area provide far greater protection for consumers when they deal with financial institutions than with any other type of business.[211]

***EPIC et al., NAAG, and Individuals' Perspectives***

These groups did not comment on the GLBA provisions for technical, administrative, and physical safeguards for customer information. They commented extensively, as indicated in the preceding chapters, on what they saw as shortcomings in the existing GLBA and FCRA provisions regarding the disclosure of customer financial information and the risks they view as arising from these shortcomings.[212]

EPIC et al. and NAAG stated that the standards and regulations under GLBA do not adequately protect customers' privacy.[213] EPIC et al. commented that any system that relies on silence as agreement (i.e., an opt-out system) is inherently prone to abuse.[214] They expressed the view that public concerns over the loss of privacy have intensified since GLBA was enacted, and that state actions involving the sale of sensitive financial information reflect these concerns.

EPIC et al. expect little response to opt-out notices because they view opt-out frameworks as creating incentives for presenting consumers with confusing notices and mechanisms for exercising the opt out. EPIC et al. wrote, "The impetus for effective notice rests with entities whose interests are better serviced when there is *no* effective notice."[215] They asserted that companies know how to send out their opt-out notices so that they are unlikely to be

---

[206] *See, e.g.,* AIA, pp. 4-5; ACLI, p. 7; NAMIC, p. 8; MetLife, pp. 6-8.

[207] *See, e.g.,* ACLI, p. 6; NAMIC, p. 8; AIA, p. 5; Alliance of American Insurers (AAI), p. 1.

[208] *See, e.g.,* FleetBoston, p. 10; CUNA Mutual, pp. 6-7; Rogue FCU, p. 6; Navy FCU, p. 6; USA FCU, p. 2; CUNA & Affiliates, p. 2; MBNA, pp. 13-14; Northern, pp. 2-3; Household, p. 8; Bank One, p. 12; Wells Fargo, p. 7; Citigroup, p. 23; Community State Bank (CSB), pp. 1-2; ICBA, p. 6; FSRT, p. 17; CTBA, p. 10; SIA, p. 11; ACB, p. 7; AAI, p. 1; MetLife, p. 13; ACLI, p. 12; NAMIC, p. 14; AIA, p. 9; E*Trade, p. 6; USAA, p. 6; VISA, p. 23; NAFCU, p. 3.

[209] *See, e.g.,* AAI p. 1; Wells Fargo, p. 7; Household, p. 9; ACB, p. 7; FSRT, p. 17.

[210] GLBA, §§ 502-503; Joint Regs. § ___.7.

[211] MetLife, p. 13.

[212] See Chapters II-IV for this discussion.

[213] EPIC et al., p. 14; NAAG, p. 11. See also Chapter IV for more discussion of risks.

[214] EPIC et al., p. 14.

[215] *Id*.

noticed, opened, or read by consumers, and commented further, "Litigation has revealed that companies have been known to hire consultants to obscure notices from consumers, as well as draft language in a manner least likely to reveal the importance of the notice to the customer."[216] NAAG also expressed the view that financial institutions' GLBA notices, developed in accordance with the requirements imposed under current law, have been so confusing that consumers have not been informed sufficiently about their rights and how to exercise them.[217]

EPIC et al. stated that it is very difficult for financial institutions to provide adequate and informative notices when the laws governing information-sharing practices are complex.[218] EPIC et al. argued that the opt-out framework under the existing laws "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."[219] They expressed the view that the opt-out framework confuses customers concerning basic facts "about how their information is used and how to control the use," leading most customers to "wrongly assume that they still have control over how personal information is used and merely have to opt out to stop all unwanted disclosures."[220] NAAG also said that current law does not provide consumers with sufficient control of sharing of transaction or experience information among affiliates.[221]

EPIC et al. also stated that the rules affecting disclosure of nonpublic personal information do not apply to personal information, which may have been acquired for marketing purposes, for persons with no relationship to the financial institution.[222]

In the view of EPIC et al., enforcement under GLBA rests with several federal agencies that are "already overtaxed" with other responsibilities and, for the "multitude of other, unregulated companies that fall within the broad definition of 'financial institution,' compliance is left to the Federal Trade Commission."[223] They wrote that much information about the information-sharing practices of financial institutions is not publicly available, and consequently, there is great difficulty in knowing what financial institutions are, in fact, doing and whether they are complying with the law and their own stated policies.[224] Federal regulators' efforts to investigate complaints, short of litigation, may not provide much public insight into the industry's information-sharing practices, according to EPIC et al.[225] Moreover, EPIC et al. stated that individuals who are harmed are unable to seek redress or protest their interests directly and therefore, "the right to protect one's privacy should be given the same recognition as the right to protect property and seek remedies for other individualized wrongs."[226]

---

[216] *Id*., pp. 14, 22.

[217] NAAG, pp. 17-19. See Chapter VII for more discussion on information-use notices.

[218] EPIC et al., p. 15.

[219] *Id*., p. 14.

[220] *Id*., p. 15. See also Chapter VI for more discussion of opt out.

[221] NAAG, p. 2.

[222] EPIC et al., p. 16.

[223] *Id*.

[224] *Id*.

[225] *Id*., p. 17.

[226] *Id*.

## SUGGESTED CHANGES TO THE EXISTING LAW AND REGULATION

### *Financial Services and Other Industry Perspectives*

With respect to the provisions of law dealing predominantly with disclosure of personal financial information, commenters expressed two main concerns. First, several trade associations and individual institutions stated a preference for establishing a uniform national standard that would prevent conflicts among federal and state laws regarding customer information-sharing practices.[227] Of these, several financial industry commenters proposed that the federal standard for sharing information among affiliates that existed under FCRA should be extended beyond the sunset date of January 1, 2004.[228] Some argued that Congress should amend GLBA to provide a similar national standard under that statute.[229]

Commenters pointed to the potential for increased state legislative efforts aimed at blocking or restricting information flows.[230] These financial institutions indicated that such state action would work to the detriment of consumers, since the likely recourse for financial institutions would be to avoid doing business in those states. These commenters argued that the absence of a national policy on protection of customers' financial information likely would confuse some customers and increase both the costs and the challenges associated with complying with varying requirements.[231] Specifically, they wrote that conflicting state laws would inhibit the ability to offer innovative products and services, and companies would not be willing to invest in costly technologies if their widespread use is apt to be threatened in a climate of curtailed information sharing.[232] Commenters representing community banks and credit unions stated that the costs of compliance with multiple federal and state laws could potentially overwhelm smaller financial institutions.[233]

As an example of the problem that confronted financial institutions, three commenters pointed to Vermont Statutes which imposed an opt-in framework on financial institutions' ability to share non-transaction or non-experience information with affiliates and were excepted under FCRA from the prohibition on state action with respect to sharing information among affiliates.[234] VISA and ICBA, for example, noted that because Vermont requires customers to give prior permission before information sharing may occur, with some exceptions, most

---

[227] *See, e.g.,* AIA, p. 9; ACLI, p. 12; MetLife, p. 14-15; VISA, p. 23; E*Trade, p. 6; CUNA and Affiliates, pp. 2-3; MBNA, p. 14; FleetBoston, p. 10; Northern, p. 3; Household, p. 8; Bank One, p. 12; Citigroup, p. 23; FSRT, p. 17; ICBA, p. 6-7; CTBA, p. 11; SIA, p. 11.

[228] *See, e.g.,* CTBA, p. 11; Household, p. 8; Bank One, p. 12; Northern, p. 3; Citigroup, p. 23; VISA, pp. 23-24; FSRT, p. 17; NAMIC, p. 15; AIA, p. 9.

[229] *See, e.g.,* NAMIC, p. 15; VISA , p. 24; Northern, p. 3; Bank One, p. 12; Citigroup, p. 23; FSRT, p. 17; ICBA, pp. 6-8; SIA, p. 11; NAFCU, p. 3; CTBA, p. 11; Household, p. 8; FleetBoston, pp. 10-11; Bank One, p. 12; CUNA and Affiliates, p. 3; MBNA, p. 14; MetLife, p. 14; AIA, p. 9.

[230] *See, e.g.,* MetLife, p. 14; Northern, p. 3; CTBA, p. 11; FleetBoston, p. 11; Household, p. 8; VISA, p. 24; CUNA and Affiliates, p. 3; FSRT, p. 17; MBNA, p. 14; Citigroup, p. 23. See also Chapter V.

[231] *See, e.g.,* SIA, p. 11; FSRT, p. 17; NAFCU, p. 3; CTBA, 11; Household, p. 8; FleetBoston, p. 11; Bank One, p. 12; Northern, p. 3; Citigroup, p. 23; CUNA and Affiliates, p. 3; MBNA, p. 14; VISA, p. 24; MetLife, pp. 14-15.

[232] *See, e.g.,* MetLife, p. 14; Northern, p. 3; CTBA, p. 11; FleetBoston, p. 11; Household, p. 8; VISA, p. 24; CUNA and Affiliates, p. 3; FSRT, p. 17; MBNA, p. 14; Citigroup, p. 23. See also Chapter V.

[233] *See, e.g.,* ICBA, pp. 6-8; CUNA Mutual, pp. 2-3.

[234] *See, e.g.,*VISA, pp. 23-24; Bank One, p. 12; ICBA, p. 7. See also Chapter II for more discussion on FCRA.

financial institutions facing the opt-in rule decided to opt out all Vermont customers, thereby denying them access to financial products and services.[235]

ACLI stated, "Member companies strongly believe that it is absolutely critical that under the current regulatory system, insurers are subject to privacy laws and regulations which are uniform with the laws and regulations to which other financial institutions are subject."[236] One financial institution commenter suggested that, to provide for greater uniformity, the national policy regarding customers' personal information should encompass all industries rather than only the financial services industries.[237]

VISA U.S.A. Inc. (May 10, 2002 letter) (VISA(2)) emphasized how different state standards also require financial institutions to apply different standards of treatment of information based on where the transaction occurs or where the consumer resides.[238] As an example, VISA(2) stated:

> In an online transaction where a customer resides in one state, but initiates a transaction to make an investment from the customer's workplace in a second state, and where the financial institution with which the transaction is conducted is located in a third state (as often occurs in the New York City and Washington, D.C. metropolitan areas), as many as three separate state laws could apply to information relating to the transaction. The resulting need to provide multiple disclosures and to apply different standards to the handling of the information would discourage companies from offering the convenience of these services and would only confuse and frustrate consumers...Moreover, the potential consequences of the resulting Balkanization would go beyond individual consumers and businesses to include law enforcement efforts, national security, and the economy as a whole. Consumers will suffer from general confusion and a reduction in the understanding of their rights, greater incidence of identity theft, and higher costs for products and services. Similarly, businesses will suffer through lost efficiencies and increased incidents of fraud.[239]

Other commenters noted the rising numbers of states implementing "do not call" telemarketing lists.[240] A large insurer wrote, "As a practical matter, this may limit the inter-

---

[235] VISA, p. 23-24; ICBA , p. 7. See also NAAG, pp. 5-6, which refers to Vermont as the only state where consumer consent is required before consumer report information can be shared among affiliates.

[236] ACLI, p. 12.

[237] Citigroup, p. 23.

[238] VISA(2), p. 11.

[239] *Id*.

[240] *See, e.g.,* MetLife, p. 6; FleetBoston, p. 4; BofA, pp. 8-9. Note that since receiving the comments for the study, the FTC announced that it amended its Telemarketing Sales Rule, 16 C.F.R. Part 310, to create a national "do not call" registry. Beginning in July, 2003, consumers may place their telephone numbers on this registry to put telemarketers subject to the FTC's Rule on notice that they do not wish to receive telemarketing calls. The effective date for compliance with the "do not call" registry was October 1, 2003. The Federal Communications Commission was also in the process of reviewing its "do not call" regulations, 47 C.F.R. 64.1200, under Congressional directive to "maximize consistency with the rule promulgated by the [FTC]. . ." P.L. 108-10 (2003).

affiliate sharing for marketing purposes of information about those customers who have placed themselves on such a list."[241]

The second general concern that financial services industry commenters raised about rules affecting information sharing involved the complexity of the statutory requirements related to the notices and the costs associated with providing them.[242] Comments on these disclosures are reflected in more detail in Chapter VII.

In addition to these two main concerns, some financial institution commenters stated that identity theft is a growing concern.[243] VISA(2) noted that identity theft is as much of a problem for financial institutions as it is for consumers since "financial institutions, particularly in the area of credit and debit card transactions, ultimately bear the financial loss from identity theft."[244] BofA noted two reasons why identity theft is the fastest growing crime in America: 1) identity thieves have easy access to information, because they are able to induce consumers to divulge this information unwittingly; and 2) identity theft often crosses many legal jurisdictions, utilizing law enforcement from both municipal and state boundaries, making it difficult for law enforcement agencies to trace the perpetrators of the crime and even more difficult for these thieves to be prosecuted.[245]

FSRT stated that laws and regulations designed to address identity theft should be developed separately from the issue of customer privacy.[246] Several commenters wrote that programs to educate consumers about the dangers of identity theft and other personal information-related crimes would increase security.[247] CTBA opined that the government should increase its educational initiatives to "enhance the likelihood that consumers will be able to protect themselves against identity theft, fraud and other security related crimes."[248] Additionally, VISA(2) stated that financial institutions have an "inherent incentive to prevent identity theft" due to the losses they incur as a result; therefore, "with this incentive, evolving fraud control systems developed by financial institutions are far more likely to be effective in preventing identity theft than other proposed alternatives, such as mandated requirements to investigate address changes in a particular way or limitations on the disclosures of social security numbers."[249]

On another note, the National Pawnbrokers Association (NPA) commented that the scope of the law enforcement exceptions in GLBA section 502(e) is greater than under other federal statutes, such as FCRA or the Right to Financial Privacy Act,[250] and urged that consideration be

---

[241] MetLife, p. 6.

[242] *See, e.g.,* CUNA Mutual, p. 7; Wells Fargo, p. 7; CFB, p. 7; ICBA, p. 7; MBNA, p. 14; E*Trade, p. 6; ACLI, p. 13. See also First Niagra Bank, p. 1, re: Amendments to FCRA guidelines.

[243] *See, e.g.,* BofA, pp. 7, 9; ABA, p. 10; FSRT, p. 18; ICBA, p. 5; VISA(2), p. 6.

[244] VISA(2), p. 6.

[245] BofA, p. 7.

[246] FSRT, p. 18.

[247] *See, e.g.,* BofA, p. 7; ICBA, p. 5; CTBA, p. 7.

[248] CTBA, p. 7.

[249] VISA(2), p. 7.

[250] Right to Financial Privacy Act of 1978, 12 USC §§ 3401-3422 (2000).

given to narrowing these specific GLBA law enforcement exceptions.[251] USAA requested clarification of FCRA rules to authorize processing exceptions, similar to GLBA rules. USAA also called for modification of the definition of "nonpublic personal information" to exclude a customer list comprised of publicly available identifying information, "unless the list was developed using financial criteria such as income, assets, debt, or ownership of a particular financial asset."[252]

First Niagara Bank recommended that the federal banking agencies expedite the issuance of the final FCRA regulations, on which they had been working, and include detailed guidance regarding what constitutes transaction or experience information that may be shared freely with affiliates. It further recommended detailed guidance on information sharing among affiliates for the centralized provision of services such as loan underwriting, processing, quality control, closing and collection, deposit account administration, and other similar purposes.[253]

***EPIC et al., NAAG, and Individuals' Perspectives***

EPIC et al. endorsed the adoption of an opt-in approach for "all information-sharing for secondary purposes whether to affiliates or third parties," which would encourage financial institutions to "make a compelling case to the customer for why they should agree to share their sensitive data."[254] They stated, "For most of the claims that opt-in would prevent crucial forms of information-sharing, an exemption is already included under the GLBA."[255] In their view, use of the opt in would help to prevent abusive sales practices and encourage greater transparency in how personal financial information is used.[256] Several of the individual commenters also expressed support for an opt-in framework that would prohibit disclosures to third parties unless authorized by the customer.[257] NAAG supported giving each consumer "effective" control over the sharing of information among affiliates, including control over the sharing of transaction or experience information.[258]

As a general matter, EPIC et al. stated, "Financial services companies should comply with fair information practices…" that would include "clear notice and full disclosure" of a bank's information-sharing policies, "full access" for consumers to records containing information about them and a right to dispute and correct errors, and enforceable legal rights.[259] They recommended amending the enforcement provisions of GLBA and proposed that the states should be given concurrent enforcement authority, as permitted under FCRA. EPIC et al. further proposed that individuals should be permitted to bring private actions under GLBA in order to protect their interests, as FCRA recognized certain private causes of action.[260]

---

[251] NPA, p. 5.

[252] USAA, pp. 5, 7. See also Mission Federal Credit Union, p. 1, re: Encouragement of federal agencies to update associated laws to exist in concert with privacy regulations.

[253] First Niagara Bank, p. 1.

[254] EPIC et al., pp. 7-8.

[255] *Id*., p. 13.

[256] *Id*., p. 7. See also Chapter VI for discussion of opt in.

[257] *See, e.g.,* Grammer, p. 1; Lutz, p. 1; Olsen, p. 1; Squire, p. 1; Elder, p. 1; Hancock, p. 1; Cochran, p. 1.

[258] NAAG, pp. 1, 5-6.

[259] EPIC et al., p. 8.

[260] *Id*., pp. 16-17.

## CHAPTER VI

## THE FEASIBILITY OF DIFFERENT APPROACHES TO INFORMATION SHARING

### INTRODUCTION

Congress mandated an examination of the feasibility of "different approaches, including opt out and opt in, to permit customers to direct that confidential information not be shared with affiliates and nonaffiliated third parties," and of "restricting sharing of information for specific uses or permitting customers to direct the uses" for which the nonpublic personal information could be shared. [261]

### OPT OUT

#### *Financial Services and Other Industry Perspectives*

A large number of financial industry commenters stated that permitting customers to opt out of information sharing across the board either would not be feasible or would not be practical because of the expense involved.[262] SIA wrote that it would not be feasible to implement an opt-out system for sharing information among affiliates without disrupting business and adversely affecting products and services offered by financial institutions.[263] Moreover, a number of commenters noted that permitting an opt-out approach to information sharing among affiliates would block the very types of activities enabled by GLBA.[264] As noted elsewhere, BofA indicated that consumers who do not wish to be solicited would receive more solicitations if affiliates could no longer share information among themselves, resulting in independent solicitations from each affiliate.[265]

Bank One cautioned that prices would rise to offset the costs of less efficient transactions and the inability to "bundle" products. In cautioning that an opt-out right for sharing information with both affiliates and nonaffiliates could have the unintended consequence of impeding fraud prevention activities and law enforcement, Bank One noted that many entities might simply stop sharing information among affiliates rather than build and maintain a complex computer system or other controls necessary to track and honor various opt-out requests.[266] As a consequence, according to Bank One, the lack of electronic or systemic infrastructure would preclude the

---

[261] GLBA, § 508(a)(8) and (9).

[262] *See, e.g.,* VISA, pp. 26-27; E*Trade, p. 8; Intuit, p. 6; AAI, p. 2; AIA, p. 11; MetLife, p. 17; ACLI, p. 14; BofA, p. 10; Bank One, pp. 14-15; FleetBoston, p. 11; CFB, p. 10; Wells Fargo, p. 8; CUNA Mutual, p. 8; NAFCU, p. 4; USA FCU, p. 2; Navy FCU, p. 8; SIA, p. 13; ABA, p. 11; FSRT, p. 21; CTBA, p. 13.

[263] SIA, pp. 12-13. See also VISA, p. 26; MetLife, p. 17; Navy FCU, p. 8; USA FCU, p. 2; E*Trade, p. 8; CFB, p. 10.

[264] *See, e.g.,* SIA, pp. 12-13; VISA, p. 26; MetLife, p. 17; Navy FCU, p. 8; USA FCU, p. 2; E*Trade, p. 8; CFB, p. 10.

[265] BofA, p. 11.

[266] Bank One, p. 14.

ability to identify quickly related relationships when there are fraud issues or other criminal activities.[267]

### *EPIC et al., NAAG, and Individuals' Perspectives*

As noted earlier, these groups asserted that individuals should have greater control over the information their financial institutions can disclose about them. EPIC et al. advocated the opt-in approach as the only feasible approach to permit informed customer consent.[268] NAAG commented that consumers should be given "effective" means of control over whether their information is shared with affiliates or nonaffiliates, and noted the Vermont opt-in requirement for sharing certain information with affiliates, such as credit reports, while exempting transaction or experience information from the restrictions.[269]

## OPT IN

### *Financial Services and Other Industry Perspectives*

Most industry commenters opposed requiring prior consumer consent, or opt in, for any information sharing.[270] These commenters generally did not differentiate between affiliates and nonaffiliated third parties. Various reasons were cited for the general objection, including statements that an opt-in system would abridge a financial institution's First Amendment right to free speech, undercut the spirit of GLBA by effectively eliminating the positive aspects of the expanded powers that the statute permits, and raise the cost of providing financial services and products. Most industry commenters agreed that requiring consumers to opt in to any information-sharing system would raise the cost of offering products to consumers to the point that many services might no longer be provided.

A number of commenters indicated that limiting information flows would decrease or eliminate the ability of financial institutions to offer linked products and services or to target certain customers for special incentives or advantageous offers.[271] SIA noted, for example, a case where a customer of a broker-dealer might seek a mortgage with an affiliate, who then might seek information about the client's account from the broker-dealer. The broker-dealer would not be permitted to share such information without explicit customer consent if an opt-in rule were in place.[272]

---

[267] *Id*., pp. 14-15.

[268] EPIC et al., pp. 20-23.

[269] NAAG, pp. 2, 5-6, 16.

[270] *See, e.g.,* Denali FCU, p. 4; USA FCU, p. 2; CUNA Mutual, pp. 7-8; CUNA and Affiliates, p. 5; Navy FCU, pp. 7-8; Capital One, pp. 2-3; Wells Fargo, p. 7; Citigroup, pp. 25-26; Household, p. 10; BofA, pp.10, 13-14; MBNA, pp. 15-16; FleetBoston, pp. 10-11; ABA, p. 9; FSRT, pp. 20-21; CTBA, p. 13; ICBA, p. 8; ACB, p. 6; AAI, p. 2; MetLife, p. 17; NAMIC, p. 16; CSB, p. 1; CFB, p. 8; Bank One, p. 14; NAFCU, pp. 2-3; Rogue FCU, p. 7; SIA, pp. 12-13; ACLI, p. 13; AIA, pp. 2, 10-11; VISA, p. 25; USAA, p. 9; Intuit, pp. 6-7; E*Trade, pp. 6-7.

[271] *See, e.g.,* AIA, pp. 10-11; Capital One, p. 2; Bank One, p. 14; Household, p. 7; BofA, p. 10; Navy FCU, p. 7; CUNA Mutual, pp. 8-9; E*Trade, p. 7; ACLI, p. 14; Citigroup, p.25; MetLife, p.17; USAA, p. 9; ABA, p. 10; MBNA, p. 15; CTBA, p.13; ICBA, p. 8.

[272] SIA, p. 10.

Commenters suggested that underlying costs relating to such functions as system development, training, marketing, and staff and consumer education could increase, as could the time it would take one affiliate to collect information that another affiliate may already possess.[273] FSRT stated, "Requiring multiple processing capabilities for firms will simply be cost prohibitive for many firms, inhibit the ability of firms to respond to customer complaints, and force choices on firms that will harm consumers."[274] In addition, commenters noted that an opt-in system would effectively prohibit institutions from offering a central point of contact for the consumer.[275] CTBA explained that without information sharing, it would no longer be possible for a consumer with relationships at multiple affiliates to process with one phone call, a basic transaction, such as an address change, or to resolve a complaint.[276]

Capital One stated that a change to an opt-in regime could necessitate changing its holding company system or the legal structure of some affiliates within its holding company system.[277] VISA suggested that limitations on sharing information with affiliates would "encourage banks to restructure in ways that are contrary to the intent of the GLB Act."[278] VISA explained, "Restrictions on the sharing of information between affiliates will cause financial services holding companies - which are in many cases required or encouraged by legal, tax, economic and geographical considerations to operate through separate legal entities - to consolidate and transfer as many activities as possible inside a single institution, generally the bank."[279]

E*Trade mentioned that a mandatory opt-in system would create a competitive disadvantage for smaller financial institutions because they rely to a greater extent than larger institutions on information sharing with nonaffiliated third parties to undertake or provide services they cannot provide on their own.[280] These smaller institutions were able to take advantage of similar economies of scale under the exceptions of GLBA and FCRA to those enjoyed by larger institutions.[281]

Both Bank One and VISA wrote that consumers who do not opt in under such a system would not necessarily understand the true ramifications of their choices.[282] SIA commented that as a practical matter an opt-in policy would rarely benefit consumers, because many would fail to

---

[273] *See, e.g.,* Navy FCU, p. 7; E*Trade, p. 7; NAMIC, p. 16; Household, p. 10; MetLife, p. 17; USAA, p. 9; AIA, pp. 10-11; ACLI, p. 14; AAI, p. 2; MBNA, p. 15; Bank One, p. 14; Citigroup, p. 25; Fleet Boston, p. 10; NAFCU, p. 2; CUNA Mutual, pp. 8-9; ACB, pp. 6-7; ICBA, p. 8; SIA, p. 10; ABA, p. 10; CTBA, p. 13.

[274] FSRT, p. 20.

[275] *See, e.g.,* SIA, p. 10; FSRT, p. 15; BofA, pp. 10-11; Navy FCU, p. 8; ACB, p. 6; ABA, p. 6; Fleet Boston, p. 10; CSB, p. 1; Citigroup, pp. 22-23; Bank One, p. 11; CUNA Mutual, p. 6; CFB, p. 6; Wells Fargo, p. 6; MetLife, pp. 11,17; NAMIC, p. 16; ACLI, p. 11; VISA, pp. 20-21.

[276] CTBA, p. 4.

[277] Capital One, p. 2.

[278] VISA, p. 22.

[279] *Id*., pp. 22-23.

[280] E*Trade, pp. 6-7. See also Capital One, p. 2.

[281] E*Trade, pp. 6-7.

[282] Bank One, p. 14; VISA, p. 25.

exercise their opt-in choice simply due to lack of attention. These consumers would be denied the opportunity to consider products and services that they may have wished to receive.[283]

As frequently noted, for most commenters, the detection and prevention of financial fraud is a crucial reason for sharing information. Commenters stated that further limitations on information sharing could impede fraud deterrence, thus causing risk exposure to rise. Additional restrictions on information sharing also could impede the ability to identify delinquent borrowers, thus raising risk exposure and ultimately affecting the cost of credit for consumers.[284] E*Trade indicated that placing limitations on information sharing would increase costs because "the ability to target and identify fraud may be reduced" since the information "could not be shared freely in order to conduct investigations."[285]

The NPA commented that it would be "devastating to lose the ability to share information with affiliates for the purpose of enforcement of a debt or of a contract."[286] The association also stated that a change from the existing opt-out provisions of the GLBA to opt in would be "inappropriate for information transfers to law enforcement agencies and regulatory or licensing agencies, and inconsistent with the provisions of other laws such as the USA PATRIOT Act, FCRA, and the Right to Financial Privacy Act."[287]

A number of commenters stated that financial institutions should be permitted to employ an opt-in system, but such a system should never be made mandatory because of such costs and burdens as noted above.[288] E*Trade wrote that an optional opt-in system for affiliates that provides products and services that are not financial in nature could enhance customer loyalty and give customers greater control over their data. However, E*Trade commented, the costs and retooling necessary to implement a mandatory opt-in rule could undercut its effectiveness.[289]

ACLI stated that its member companies "strongly believe that it would not be feasible to require insurers to obtain customers' consent (opt in) before sharing customer medical information in connection with core insurance business functions and related product and service functions…" However, ACLI stated that the opt-in approach is feasible for sharing medical information for marketing purposes.[290]

Bank One noted that under GLBA, financial institutions could share information with nonaffiliated third parties "when the consumer has consented to such sharing, as an alternative to a required opt out."[291] Bank One found the ability to release information with customer consent to be important for day-to-day operations and the provision of service. For example, Bank One stated, "Customers want to be able to authorize the release of information under many

---

[283] SIA, p. 13.

[284] *See, e.g.,* MBNA, p. 10; Bank One, p. 10; CUNA Mutual, p. 6; ICBA, p. 6; E*Trade, p. 4; NAMIC, p. 12; Wells Fargo, pp. 1,5; BofA, p. 5.

[285] E*Trade, p. 4.

[286] NPA, p. 9.

[287] *Id*., p. 8.

[288] *See, e.g.,* AIA, p. 11; ACLI, p. 14; MetLife, p. 17; ABA, p. 11; SIA, p. 13; NAFCU, p. 4; Capital One, p. 4; FleetBoston, p. 11; Bank One, p. 14; E*Trade, p. 8; VISA, p. 26.

[289] E*Trade, p. 8.

[290] ACLI, p. 14.

[291] Bank One, p. 14.

circumstances, including credit references, authorization to present a loan application to another lender if the consumer does not qualify for the initial product, verification to a merchant of availability in a checking account to cover a check, or an introduction to a third party in connection with a product that may be appropriate for the consumer."[292] Rogue Federal Credit Union (Rogue FCU) and NAFCU suggested that an optional opt in might be acceptable for cases when a financial institution intends to disclose information to nonaffiliated third parties strictly to market nonfinancial products or services, or otherwise shares information outside of the exceptions in the GLBA rules.[293]

***EPIC et al., NAAG, and Individuals' Perspectives***

EPIC et al. stated, "Citizen have a legitimate and significant expectation of privacy with respect to sensitive non-public personal information contained within their financial information."[294] Congress, they wrote, recognized this in enacting statutes restricting disclosures relating to cable subscriber records, video rental records, credit reports, and medical records. Opt in, EPIC et al. expressed further, protects the privacy interests of consumers and the governmental interest in consumer privacy.[295]

EPIC et al. also commented that systems should be in place that do not require consumers to take affirmative steps to protect themselves. The group emphasized that the only way to achieve this goal is through an opt-in system.[296] In addition, they stated that an opt-in system will encourage greater transparency. The lack of transparency, they asserted, leads to confusion and inevitable abuse and deprives consumers of important rights. In their view, opt in would put the onus on financial institutions to explain the benefits of allowing the compilation of customer data. This might lead such companies to provide incentives to customers to allow their data to be shared or sold (such as a free air travel ticket or fee-free services for a set period of time), thereby allowing consumers to obtain benefits from the sharing of their personal information.[297] NAAG indicated that a system that requires consumers to take action in order to have information shared would better protect consumers who do not take action to opt out under the current system.[298]

Additionally, a number of individual commenters supported an opt-in method for information sharing.[299] One individual stated that the opt in should include "provisions that allow information sharing with third parties if they are necessary to provide the services of the financial institution to the customer."[300]

---

[292] *Id.*

[293] Rogue FCU, p. 9; NAFCU, p. 4.

[294] EPIC et al., p. 20.

[295] *Id*., p. 21, 22.

[296] *Id*., p. 22.

[297] *Id*., p. 21.

[298] NAAG, p. 16.

[299] *See, e.g.,* Elder, p. 1; Hancock, p. 1; Grammer, p. 1.

[300] Elder, p. 1.

## ALTERNATIVES

### *Financial Services and Other Industry Perspectives*

FleetBoston and MetLife, for example, discussed so-called "do not call, e-mail, or write" lists as examples of how alternatives have been implemented.[301] The commenters stated that these systems enable them to honor customer requests without having the compliance burden of an opt-in rule.[302]

BofA, CFB and Wells Fargo also cited "do not call" lists as an acceptable method for empowering consumers with respect to the security of their information.[303] Wells Fargo stated that this system works well as long as it remains voluntary, because competitive market conditions will dictate an entity's best actions in this regard. The bank noted that it does not provide customers with more extensive options for restricting information sharing because that would introduce too much complexity into both their own operations and their customers' decision-making processes, thus increasing consumer confusion.[304]

Capital One stated that one of its affiliates has created different levels of do-not-solicit choices, allowing customers to choose to opt out of some types of e-mail marketing without ruling out solicitations altogether. From this experience, they have gained insight into two problems: 1) the difficulty of merging this data within larger centralized data management systems, and 2) limitations on marketing flexibility outside the channel of Internet solicitations, because e-mail choices are not easily translated into telemarketing or direct mail choices.[305]

Many commenters opposed the concept of added restrictions based on use or allowing customers to provide specific directions.[306] Highly technical and costly systems would have to be developed and maintained in order to implement such programs. Capital One stated that if a financial institution were required to allow customized usage decisions by each of its customers, "we would have 50 million different sets of 'use instructions' (one for each customer), housed in a separate database that must be integrated into the other 200 databases pertaining to our customers."[307] In such view, this would require developing a process for asking the questions, tabulating and compiling the answers into an accessible database, training customer service representatives and marketing analysts how to access and use the database, and regular auditing and retraining.[308] Citigroup suggested that the market may lead institutions to create innovative solutions to consumer demands for information protection, noting, "More interesting pilots of customer relationship management programs are beginning to develop more satisfactory methods

---

[301] FleetBoston, p. 11; MetLife, p. 18.

[302] *Id*.

[303] BofA, p. 12; Wells Fargo, p. 8; CFB, p. 9.

[304] Wells Fargo, p. 8.

[305] Capital One, p. 5.

[306] *See, e.g.,* MBNA, p. 17; VISA, p. 28; BofA, p. 12; Household, p. 10; Wells Fargo, p. 8; FleetBoston, p. 12; MetLife, p. 18; AIA, p. 12; ACLI, p. 15; Denali FCU, p. 5; CUNA Mutual, p. 8; NAFCU, p. 4; Rogue FCU, p. 8; SIA, p. 14; ICBA, p. 8; ABA, p. 10-11; FSRT, p. 22; Bank One, p. 15; Navy FCU, p. 9.

[307] Capital One, p. 4.

[308] *Id*.

for offering privacy choices in a more customer friendly manner."[309] These developments probably will take some time, but mandatory rules would probably "delay advances [rather] than make them move faster," Citigroup suggested. [310]

### *EPIC et al., NAAG, and Individuals' Perspectives*

EPIC et al. advocated the opt-in approach as the only feasible approach to permit customers to restrict the use of personal information.[311] They wrote: "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."[312]

[309] Citigroup, p. 27.

[310] *Id*.

[311] EPIC et al., pp. 20-23.

[312] EPIC et al., p. 22.

## CHAPTER VII

## ASSESSING FINANCIAL INSTITUTION PRIVACY POLICY AND PRIVACY RIGHTS DISCLOSURE UNDER EXISTING LAW

### INTRODUCTION

Congress mandated that the Treasury Department also investigate "the adequacy of financial institution privacy policy and privacy rights disclosure under existing law."[313] Commenters were asked whether new or revised requirements might improve them.[314] The discussion below focuses on the notice and disclosure requirements introduced by GLBA.

Section 503 of GLBA and the Joint Regulations require a financial institution to provide its consumers a clear and conspicuous notice setting forth its policy and practices regarding consumers' nonpublic personal information.[315] The institution must provide the notice at the time of establishing the customer relationship and annually during the duration of the relationship. The notice must include the following disclosures (where relevant to the institution):

- Categories of nonpublic personal information the institution collects;
- Categories of nonpublic personal information the institution discloses;
- Categories of affiliates and nonaffiliated third parties to whom the institution discloses such information;
- Categories of nonpublic personal information about former customers that the institution discloses and categories of affiliates and third parties to whom the institution discloses the information;
- If an institution discloses nonpublic personal information under section __.13 (e.g., joint marketing partners, service providers, including marketing providers), then a separate statement of the categories of information disclosed and the categories of third parties with whom the institution has contracted;[316]
- An explanation of the consumer's opportunity to direct that nonpublic personal information not be disclosed to third parties and the method of exercising this option;
- An opt-out notice for affiliate sharing as provided for by FCRA;
- The institution's policies and practices regarding the security of the disclosure of nonpublic personal information of people who cease to be customers of the institution;
- The institution's policies and practices for safeguarding nonpublic personal information; and
- If the institution makes disclosures under Joint Regs. §§ __.14 and __.15 (e.g., as necessary to complete a transaction; with the consumer's consent; to comply with

[313] GLBA, § 508(a)(7).

[314] FRN, 67 Fed. Reg. 7215 (2002).

[315] GLBA, § 503; Joint Regs. §§ __.6, __.7.

[316] See § 15 of the NAIC Model Privacy Regulation.

federal, state, or local laws), a statement that the institution discloses information to nonaffiliated third parties as required by law.[317]

The Joint Regulations provide sample clauses that are not required but may be used, where appropriate, to meet the above requirements.[318]

## ASSESSMENT OF NOTICES

### *Financial Services and Other Industry Perspectives*

Most industry commenters expressed general satisfaction with the notices they have provided to their consumers.[319] Many commenters, including some who find that their notices are adequate under the law, noted that it is difficult or even impossible to construct notices that are both easily readable and compliant with both GLBA and state law requirements, especially if the sample clauses from the Joint Regulations are used.[320] BofA indicated that the statutes require institutions to disclose to customers information that customers do not necessarily want to know.[321] VISA(2) stated that it is hard to support the view that the low opt-out rates by consumers are due to the lack of understanding by consumers of these notices since both the media and consumer advocacy groups drew attention to these notices in the spring of 2001 and yet, the opt-out rates were not "significantly higher than the few percentage points experienced by virtually all financial institutions."[322]

A number of industry commenters asserted that it was unnecessary at the time to add new requirements or make revisions to the existing requirements. These commenters cited several reasons, including: cost, limited experience with the provisions of GLBA and the Joint Regulations, and concerns of undermining the familiarity consumers have gained with existing information-sharing notices.[323] Some observed that institutions have learned much from their experiences in crafting the first round of notices and from customer feedback on those notices, and changes to their notices could be implemented under the existing framework.[324] MBNA and BofA, for example, stated that they were already implementing these changes in their annual notices.[325]

Some industry commenters were more critical of the state of current legal requirements and information-sharing notices. A number specifically cited the sample clauses in the

---

[317] Joint Regs., § __.6. See also §§ 7, 16, and 17 of the NAIC Model Privacy Regulation.

[318] Joint Regs., Appendix A. See also Appendix A of the NAIC Model Privacy Regulation.

[319] *See, e.g.,* SIA, p. 12; ABA, p. 8; CTBA, p. 12; FSRT, p. 18; BofA, pp. 8-9; MBNA, pp. 14-15; CFB, p. 7; Household, p. 9; ACB, p. 6; Bank One, p. 13; Rogue FCU, p. 6; Denali FCU, p. 4; CUNA Mutual, p. 7; Navy FCU, p. 7; USA FCU, p. 2; CUNA, p. 4; FleetBoston, p. 10; Citigroup, p. 24; Wells Fargo, p. 7; VISA, p. 24; E*Trade, p. 6; ACLI, p. 13; NAMIC, p. 15; MetLife, p. 16; AIA, p. 10.

[320] *See, e.g.,* ABA, p. 8; ACB, p. 8; ICBA, p. 7; FSRT, p. 18; MBNA, p. 14-15; BofA, p. 9; Bank One, p. 13; USA FCU, p. 2; Citigroup, p. 24; VISA, p. 24; Household, p. 9; USAA, p. 9; ACLI, p. 13; AIA, p. 10, Wells Fargo, p. 7.

[321] BofA, pp. 9-10.

[322] VISA(2), p. 5.

[323] *See, e.g.,* Household , p. 9; FleetBoston, p. 10; BofA, p. 9; CUNA & Affiliates, p. 4; ABA, p. 9; CTBA, p. 12; SIA, p. 12; AIA, p. 10; NAMIC, p. 16.

[324] *See, e.g.,* SIA, p. 12; FSRT, pp. 18-19; BofA, p. 10; ACLI, p. 13; NAMIC, p. 15; AIA, p. 10; ABA, p. 8.

[325] MBNA, p. 15, BofA, p. 10. See also CTBA, p. 12.

regulations as being confusing to customers and needing simplification.[326] Many commenters spoke of their desire to improve the readability of their notices on their own initiative or through changed regulations or best practices guidelines.[327] ACLI mentioned that it participated in a working group to develop simplified common terminology and simplified clauses that could be used to make notices more readable.[328] AIA and NAMIC also were participating in a task force trying to make notices more understandable and readable as well as contemplating additional sample clauses and a preamble for the information-sharing notices. [329]

Some commenters suggested simplifying the notices by decreasing the amount of information required in them.[330] For example, if an institution does not share information that triggers a consumer's option to prohibit information sharing, USA FCU suggested that the initial notice simply state that the institution does not share personal information with any third party that would require the institution to provide the consumer such an option.[331] Similarly, if a consumer does not have a GLBA option to prohibit disclosures to some entities, such as certain information-sharing with affiliates, USAA believed that mentioning these entities in the information-sharing notice is unnecessary and confusing for customers.[332] If the institution does share information triggering the GLBA option, VISA and Bank One suggested that the notice simply state that the institution shares information with nonaffiliated third parties for marketing purposes and provide the consumer a reasonable opportunity to object.[333] Navy FCU, on the other hand, commented that "additional information explaining that certain information sharing practices are not eligible for 'opt out' might be useful."[334]

Commenters suggested looking to efforts by industry to encourage the development of a "short-form" notice. This short notice would contain information useful to consumers, but would not contain all the information required under the present regulations.[335] A number of commenters suggested working with regulators to develop acceptable simplified language.[336] Citigroup stated, "Such a short form notice would have to be accompanied by the full GLBA notice unless GLBA is revised to allow financial institutions to refer customers to a more detailed notice."[337] A number of commenters noted benefits from simplifying the notices and making a longer notice available only upon request.[338] MBNA discussed standardizing notices, pointing to nutrition labels as a model, stating that uniform, user-friendly privacy notices would

---

[326] *See, e.g.,* ABA, pp. 8-9; Wells Fargo, p. 7; CFB, p. 8; Bank One, p. 13; Citigroup, p. 24; CUNA Mutual, p. 7.

[327] *See, e.g.,* Bank One, p. 13; VISA, p. 25; ICBA, p. 7; USAA, p. 9; FSRT, p. 19; ACLI, p. 13; Citigroup, p. 24; CUNA Mutual, p. 7; Household, p. 9; Wells Fargo, p. 7; ABA, p. 8; ACB, p. 8; CTBA, p. 12; SIA, p. 12; CUNA and Affiliates, p. 4.

[328] ACLI, p. 13.

[329] AIA, p. 10. See also NAMIC, p. 15.

[330] *See, e.g.,* FSRT, pp. 18-19; BofA, p. 9; CBA, p. 12; ACB, p. 7; USAA, p. 9.

[331] USA FCU, p. 2.

[332] USAA, p. 9.

[333] VISA, p. 25; Bank One, p. 13.

[334] Navy FCU, p. 7.

[335] *See, e.g.,* ABA, p. 8; VISA, p. 25; CTBA, p. 12; Bank One, p. 13.

[336] *See, e.g.,* CTBA, p. 12; SIA, p. 12; Wells Fargo, p. 7; CUNA Mutual, p. 7; ACLI, p. 7; CUNA & Affiliates, p. 4.

[337] Citigroup, p. 24.

[338] *See, e.g.,* ABA, p. 9; Bank One, p. 13; VISA, p. 25; FSRT, p. 19; Household, p. 9.

aid consumers' understanding of their rights and increase trust in their financial institution.[339] Two insurance associations opposed such standardization, citing the difficulty in developing short, simple, "one size fits all" notices that would be applicable to all financial institutions.[340] Insurers noted the importance of flexibility, their need to comply with state regulation, and the efforts of the NAIC's Privacy Notice Contact Task Force.[341] Changes to the information-sharing notices also must reflect the differing requirements of GLBA and FCRA, according to one commenter.[342]

Some industry commenters suggested eliminating the annual notice requirement. Instead, they argued that notices should be provided initially and then provided only when an institution's information-use policy changes; thus, they asserted, customers would be more likely to pay attention to these notices.[343] Commenters noted that complying with various state laws has added to consumers' confusion. Many commenters wrote that a uniform national privacy standard would alleviate the problem of confusing notices.[344]

Some industry commenters stated that consumer education would lessen the confusion. While the ABA pointed to the consumer-friendly resources issued by the FDIC[345] and FTC,[346] others suggested that more needs to be done to educate consumers.[347] Wells Fargo wrote: "Until the level of consumer knowledge improves – and that will require more than mandated disclosures – making notices easier to read will not guarantee that they are really understood."[348]

***EPIC et al., NAAG, and Individuals' Perspectives***

NAAG called the current GLBA and FCRA notices "woefully inadequate."[349] EPIC et al. agreed, noting that GLBA information-use notices fail to give consumers meaningful notice because the notices were not clear and conspicuous.[350] Both EPIC et al. and NAAG cited Dr. Mark Hochhauser's readability study of the GLBA privacy notices. Of the 60 notices examined, the study indicated that most were written at a third- or fourth-year college level or above, while an eighth-grade reading level would have been an accepted standard for notices for the general public.[351]

---

[339] MBNA, p. 15.

[340] ACLI, p. 13; NAMIC, p. 16.

[341] *Id*.

[342] Citigroup, p. 25.

[343] *See, e.g.,* ACB, p. 8; MetLife, p. 16; USAA, p. 9; ICBA, p. 7; FSRT, p. 19; CFB, p. 9; USAA, p. 9.

[344] *See, e.g.,* SIA, p. 11; FSRT, p. 17; NAFCU, p. 3; CTBA, 11; Household, p. 8; FleetBoston, p. 11; Bank One, p. 12; Northern, p. 3; Citigroup, p. 23; CUNA and Affiliates, p. 3; MBNA, p. 14; VISA, p. 24; MetLife, pp. 14-15.

[345] FDIC: FDIC Guidance Materials to Help Financial Institutions and Customers Understand GLBA Privacy Protections at www.fdic.gov/consumers/privacy/index.html.

[346] FTC: "Sharing Your Personal Information: It's Your Choice" at www.ftc.gov/privacy/protect.htm.

[347] *See, e.g.,* ABA, p. 9; Wells Fargo, p. 7; ICBA, p. 7.

[348] Wells Fargo, p. 7.

[349] NAAG, p. 16.

[350] EPIC et al., p. 19.

[351] EPIC et al., p. 19; NAAG, pp. 17, 18.

One individual, a bank examiner by trade, explained that the privacy notices he received were "not in an easy form to read and understand."[352] This view is supported by NAAG, which cited a Harris Interactive Survey for the Privacy Leadership Initiative showing that 58% of consumers did not read the notices at all or only glanced at them.[353] Lack of time or interest and difficulty in understanding or reading the notices, according to this survey, top the list of the reasons why consumers do not spend more time reading the notices.[354] EPIC et al. maintained that the notices are confusing and difficult to understand because they are written to satisfy legal obligations of companies and not to inform individuals.[355] NAAG stated that consumers voiced numerous complaints and raised concerns that financial institutions' "unintelligible notices are an attempt to mislead" consumers.[356]

EPIC et al. asserted that another reason the notices are not clear and conspicuous is because they are mailed to consumers with other disclosures.[357] NAAG and EPIC et al. cited the ABA survey as showing that 41% of consumers did not recall receiving their opt-out notices, and 22% recalled receiving them but did not read them.[358] Customers, it was argued, often overlook the notices or regard them as "junk mail." EPIC et al. commented that many notices may have been regarded as nothing more than a marketing tool; some notices begin with statements about a company's commitment to protect consumer privacy.[359]

One individual wrote that he asked several other people about the notices they received, and they did not know what he was talking about. A majority of this individual's respondents stated that they thought "it was just another statement stuffer from their financial institution and threw it away without reading it. It looked like junk mail."[360]

Even when customers identify and read the privacy notices, EPIC et al. argued the notices lack practical information. For example, the notices do not explain why they were sent, the consumer's relationship with the financial institution, the date by which consumers must reply before their information is shared, or the fact that consumers have a continuing option to object to disclosure.[361]

EPIC et al. attributed the low opt-out rates not to a public preference for information sharing by institutions, but rather to the public's inability to identify or to understand information-use notices and consumers' overall confusion about whether opt out is even available. EPIC et al. believed that the notices place an unfair burden on consumers to protect

---

[352] Lutz, p. 1.

[353] NAAG, p. 18.

[354] *Id*.

[355] EPIC et al., p. 14.

[356] NAAG, p. 18.

[357] EPIC et al., p. 17.

[358] NAAG, p. 18; EPIC et al., p. 18. NAAG and EPIC et al. referred in their comments to the survey by the American Bankers Association (June 2001).

[359] EPIC et al., p. 18.

[360] Lutz, p. 1.

[361] EPIC et al., p. 19.

their privacy, requiring that they respond to each separate privacy notice and follow each company's particular method or requirement to opt out.[362]

Some of the individual commenters echoed that sentiment.[363] One individual commented that, of the many notices she received:

> [T]he opt-out procedure was different on each one. Either fill out the form and return separately or call this number (and of course, you could not just say 'mark me opt-out', they have to explain what you will not get or sometimes ask you survey questions about why, etc.) or go to website and answers [sic] questions, check boxes, etc., etc. Much too complicated and aggravating.[364]

Another individual stated that tearing off the opt-out check-off form to send back to the company resulted in tearing off "some of the customer information that was to be shared."[365]

EPIC et al. wrote that the only effective way to protect consumers' information is to require consent to information sharing, e.g., an opt-in system.[366] They stated that, if the public has no such alternative, then the government should impose more stringent standards on financial institutions. Such options might include: an obligation to give and accept alternative opt-out methods; mandatory privacy education for company staff; permitting easy access to privacy policies at branch offices and on websites; the obligation to confirm an opt-out request; providing a single website with opt-out information; developing standards for readability; eliminating marketing in privacy notices; and encouraging transparency in information-sharing practices.[367]

NAAG concluded that if most consumers do not read the notices, and those who do read them do not understand them, one cannot believe that consumers are "able to understand their rights and exercise their choices intelligently." Therefore, NAAG called on the "FTC and other federal regulatory agencies to create standard notices and require much simpler language so that consumers could understand them."[368]

---

[362] *Id*.

[363] Elder, p. 1; Grammer, p. 1.

[364] Grammer, p. 1.

[365] Lutz, p. 1.

[366] EPIC et al., p. 15.

[367] *Id*., p. 20.

[368] NAAG, p. 19.

## CHAPTER VIII

## CONCLUSIONS, FINDINGS, AND RECOMMENDATIONS

### INTRODUCTION

The security of personal financial information is the primary issue under scrutiny in this study. It is also of vital concern to President Bush and to the Treasury Department. Threats to that security may be the top financial services worry of consumers today. Fraud through identity theft can be a life disrupting nightmare for its victims and for their families.

Our financial services providers are world leaders at meeting the needs of their customers, and most go to great lengths to implement policies and practices for the security of customer information. But new challenges, practices, and technologies demand – and fortunately make it possible – that they be safer. As they become safer, customers will benefit, as will the financial firms that serve them. And our economy will grow faster as customers take greater advantage of the increased variety and lower cost of financial products that modern information technology in a free society make possible. That will happen as customers perceive that their personal financial information is used for their benefit, not for their harm.

The preceding chapters have presented the views of organizations, institutions, and individuals who responded to a Federal Register Notice (FRN) requesting comment on "information-sharing practices among financial institutions and their affiliates." The Treasury Department published the notice on February 15, 2002, pursuant to its obligation to conduct a study on this subject, mandated under section 508 of the Gramm-Leach-Bliley Act of 1999 (GLBA).

### GENERAL CONCLUSIONS

Five general conclusions can be drawn in relation to the information obtained from the study:

- First, financial services providers and their customers have a strong interest in promoting the security of personal financial information, that is, following prudent practices so that information is used for the benefit rather than the harm of the customer.
- Second, the sharing of information, within secure parameters reinforced by uniform national standards, has increased the access of more consumers to a wider variety of financial services, at lower costs, than ever before.
- Third, the growing problem of fraud through identity theft not only disrupts the lives of individuals and families, but it also tears at the fabric of commerce in our information age.
- Fourth, in our technology-based economy, so dependent upon accurate, timely information, current uniform national standards for information sharing have proven as essential to fighting identity theft as they are for economic growth and prosperity.
- Fifth, customers need to understand more easily and clearly the information-sharing practices of their financial institutions and how to exercise their say in how that information is shared in support of the customer relationship.

## KEY FINDINGS

The study demonstrated a number of important points that should influence policy makers in considering the effectiveness of programs and practices for the security of personal financial information. Some of the key findings are:

- The goals of GLBA for informing customers have not been adequately met. That is to say, although disclosures of policies on the use of nonpublic personal information are being provided, the format, length, and language are unfriendly. Too many customers are unaware of their options under current law with regard to the use of personal financial information, and too many who are aware of their options are daunted by the procedures for exercising them. It seems all too possible that while disclosure requirements may have been met from the point of view of the statute and regulations, customers are unable to understand or unwilling to read the disclosures and remain uninformed.

- Enterprises that use consumer reports, as well as consumers themselves, have a strong interest in accurate and up-to-date credit records. Improved accuracy will lead to greater efficiency economy-wide with benefits felt by individual companies and their customers.

- Most businesses have a powerful market interest in not annoying their customers with unwanted solicitations, particularly businesses that value customer loyalty. This interest may be less strongly perceived by businesses content with only brief, occasional contacts with their individual customers.

- Fraud through impersonation—identity theft—is a major problem, with serious costs to consumers and businesses. Fear of identity theft may well inhibit the growth of electronic commerce. Reduction of the risk of fraud could stimulate electronic commerce, with benefits to consumers from increased access, lower costs, and greater choice and variety of available products and services.

- Timely business access to ample and accurate information, particularly at point of sale or contract, can be a powerful deterrent to identity theft. Information sharing *per se* is not the cause of identity theft. Rather, inadequate identifying information facilitates identity theft. Gathering customer data for the benefit of the customer is no more responsible for identity theft than depositing money in banks is responsible for bank robberies, provided that sound security practices are followed. Financial institutions can help prevent identity theft if they know more about their customer than the thief does.

- Identity theft is a multi-jurisdictional problem, typical cases involving several communities, in various states. Thieves take advantage of the enforcement difficulties that this presents, using city limits and state borders to shield themselves from detection, investigation, and prosecution.

## RECOMMENDATIONS

These key findings point to a number of possible actions that would help to enhance the security and accuracy of personal financial information while at the same time encouraging robust financial markets that are more accessible to all Americans. These include the following:

- **Developing Easy to Read, Easy to Use GLBA Notices.** The information use notices required under the Gramm-Leach-Bliley Act should be made useful to customers by regulators, working with industry and customers, developing a tiered notice system. Under such a system, customers could be provided a standardized, single-page notice that contains the essential information that customers need, in familiar, understandable language, without fluff and without excess, similar to the nutrition labeling information notices developed under the Nutrition Labeling and Education Act. More detailed information, as required today under GLBA and implementing regulations, can be made readily available to those customers who request it. The options to prohibit information sharing should be made as easy to exercise as a change of billing address.

- **Enlisting Consumers in the Battle.** Businesses and consumers alike rely upon the accuracy of credit reports, and no one is more likely to be interested in searching a report for errors—or for fraudulent activity—and correcting them than the consumers themselves. It might seem obvious that consumers are interested in the security of their own financial information, but there are tools that can be provided to enable them to assist in their own defense against predators. Several important tools were provided in the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), signed by President George W. Bush on December 4, 2003. The effective use of these new tools should be monitored and encouraged.

- **Encouraging Innovative Technologies, Policies and Practices.** Financial institutions should be recognized for the initiatives they launch to deter, detect, pursue, and punish identity thieves and others engaged in financial fraud. Financial institutions also should be recognized for the administrative, technical, and procedural measures they implement to thwart identity theft, educate consumers, and assist customers who have been victimized.

## ACTION UNDER WAY

The Secretary of the Treasury is pleased to note that action to implement these recommendations has already begun. The federal financial regulators[369] and the Federal Trade Commission have issued an Advance Notice of Public Rulemaking (ANPR) on whether to amend relevant GLBA regulations to provide for financial institutions to issue privacy policy notices in formats that would be easier for consumers to understand and use.

As noted above, the FACT Act addresses many of the issues raised in this report. The legislation, which amends the Fair Credit Reporting Act, encompasses Administration recommendations announced by Secretary Snow on June 30, 2003, for enhancing the security and accuracy of personal financial information and promoting access by all Americans to U.S.

[369] Same as federal functional regulators.

credit and other financial services. A priority for the Administration, the legislation was signed by President George W. Bush early in December. Among the key provisions of the FACT Act relating to the issues reviewed in this study are the following:

- **Uniform National Standards.** The legislation reaffirms the uniform national standards incorporated in the FCRA in 1996. Retention of uniform national standards for information sharing can help speed the use of verification data to detect fraud (sometimes catching thieves in the very act) to spread alerts when people have been threatened by identity thieves, and to hasten the correction of consumer records of victims. The FACT Act also establishes additional uniform national standards for combating identity theft and improving the accuracy of personal financial information.

- **Free Credit Reports**. Consumers will be able to review a free copy of their credit report from each national consumer reporting agency every year for inaccurate information or unauthorized activity, including activity that might be the result of identity theft.

- **National Security Alert System.** With one phone call consumers who fear they may be victims of fraud will receive advice from the national credit bureaus, be able to place fraud alerts on their credit reports, and deter further misuse of their credit histories while hastening the clean up process.

- **Red Flag Indicators of Identity Theft.** Financial regulators will identify "red flags," the raising of which indicates the high likelihood of the presence of identity fraud, and will verify in their safety and soundness examinations that financial institutions make sensitivity to these red flags part of their relationship with their customers.

In addition, the FACT Act will help to enhance the accuracy of personal financial information by streamlining and expediting the investigation of complaints and removal of inaccurate information from credit reports and the records of creditors. The legislation also will protect consumers from unwanted solicitations and from inappropriate use of their medical information. The law will facilitate prompt investigation of employee misconduct.

The legislation requires extensive rule making. The challenge is to avoid harmful duplication, coordinate existing related measures established under other federal law, and be careful not to undermine continuation of the progress made in recent years to extend financial services to more customers in greater variety and lower cost than ever before.

## APPENDIX A

### GLBA Statutory Requirement for the Study

### Sec. 508. STUDY OF INFORMATION SHARING AMONG FINANCIAL AFFILIATES

(a) In General – The Secretary of the Treasury, in conjunction with the Federal functional regulators and the Federal Trade Commission, shall conduct a study of information sharing practices among financial institutions and their affiliates. Such study shall include –

(1) the purposes for the sharing of confidential customer information with affiliates or with nonaffiliated third parties;
(2) the extent and adequacy of security protections for such information;
(3) the potential risks for customer privacy of such sharing of information;
(4) the potential benefits for financial institutions and affiliates of such sharing of information;
(5) the potential benefits for customers of such sharing of information;
(6) the adequacy of existing laws to protect customer privacy;
(7) the adequacy of financial institutions privacy policy and privacy rights disclosure under existing law;
(8) the feasibility of different approaches, including opt-out and opt-in, to permit customers to direct that confidential information not be shared with affiliates and nonaffiliated third parties; and
(9) the feasibility of restricting sharing of information for specific uses or of permitting customers to direct the uses for which information may be shared.

(b) Consultation – The Secretary shall consult with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, and also with financial services industry, consumer organizations and privacy groups, and other representatives of the general public, in formulating and conducting the study required by subsection (a).

(c) Report – On or before January 1, 2002, the Secretary shall submit a report to the Congress containing the findings and conclusions of the study required under subsection (a), together with such recommendations for legislative or administrative action as may be appropriate.

**APPENDIX B**

**FEDERAL REGISTER NOTICES**

**AND**

**APPENDIX C**

**PUBLIC COMMENTS IN RESPONSE TO FEDERAL REGISTER NOTICES**

**May be accessed separately at:**

**http://www.treas.gov/offices/domestic-finance/financial-institution/cip/glba-study/index.html?IMAGE.X=17\&IMAGE.Y=12**