United States General Accounting Office

GAO

Report to Congressional Committees

May 2001

FINANCIAL PRIVACY

Too Soon to Assess the Privacy Provisions in the Gramm-Leach-Bliley Act of 1999

GAO-01-617

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 3, 2001

Congressional Committees:

This report responds to a mandate in the Gramm-Leach-Bliley Act of 1999 (GLBA) that we study the financial privacy provisions in Subtitle B of Title V that prohibit fraudulent access to customer information from financial institutions.[1] Congress enacted several privacy provisions in GLBA in response to concerns about the growing inability of consumers to control access to their personal financial information.[2] These privacy provisions created new requirements for federal regulators and financial institutions. Subtitle B made it a federal crime, generally punishable by up to 5 years in prison, for anyone to use fraud or deception to obtain nonpublic customer information from a financial institution.[3] This prohibition was enacted to address concerns about "pretext calling" or situations when someone uses misrepresentation or false pretenses to trick a financial institution into divulging a customer's nonpublic information. Once obtained, this information can be combined with other public and nonpublic information to compile an "asset profile" of the person for a business competitor, an adversary in litigation or other commercial or personal dispute, or an individual simply seeking to satisfy personal curiosity. Personal financial information collected by false pretenses can also be used to commit identity theft, whereby criminals assume the identities of their victims to gain control over or open credit card accounts, apply for loans, or incur other forms of debt, all with potentially devastating consequences for the credit rating and personal finances of the targeted individual.[4]

As mandated by GLBA, we are reporting on (1) the efficacy and adequacy of remedies provided by the act in addressing attempts to obtain financial information by false pretenses and (2) suggestions for additional legislation or regulatory action to address threats to the privacy of financial information from attempts to obtain information by fraudulent

[1] 15 U.S.C. §6826.

[2] P.L. 106-102, Title V, Subtitle A and B.

[3] 15 U.S.C. §6823.

[4] For more information about identity theft, see *Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited* (GAO/GGD-98-100BR, May 1, 1998). We also have other ongoing work related to identity theft and the use of Social Security numbers.

means or false pretenses. As required by GLBA, we consulted with and reviewed documentation provided by the Federal Trade Commission (FTC), federal banking agencies,[5] the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), appropriate federal law enforcement agencies, and state insurance regulators for this report. In addition, we obtained the perspectives of and reviewed information provided by selected privacy experts and consumer or other groups with strong interests in financial privacy. Lastly, we held discussions with officials from five states that had been identified as being particularly active regarding consumer financial privacy and reviewed available data on these states' experiences. A more detailed description of our scope and methodology is contained in appendix I.

Results in Brief

It is too soon to assess the efficacy and adequacy of the remedies provided for in Subtitle B.[6] As of March 31, 2001, federal regulatory and enforcement agencies had not taken any enforcement actions or prosecuted any cases under this law. FTC staff have begun to monitor firms' compliance with the statute's provisions and have several pending nonpublic investigations. However, FTC staff and Department of Justice officials told us that until they have fully prosecuted cases under the statute, they would lack the necessary experience to assess the effectiveness of Subtitle B provisions. The federal financial regulatory agencies are still in the process of taking steps to ensure that the financial institutions that they regulate have reasonable controls to protect against fraudulent access to financial information. For example, the federal banking agencies and NCUA are coordinating their efforts to develop guidance to financial institutions regarding fraudulent access to financial information. In addition, they plan to develop examination procedures to ensure compliance with the guidelines that they issued in January and February 2001 for safeguarding customer financial information. Lastly, we found that there are limited data available to indicate the impact of Subtitle B on the prevalence of fraudulent access to financial information.

Although all of the federal regulators and privacy experts whom we contacted agreed that additional time and experience are necessary to

[5] In this report, the term "federal banking agencies" refers to the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

[6] 15 U.S.C. §6821.

determine if Subtitle B remedies are sufficient to address fraudulent access to financial information, FTC staff and privacy experts suggested legislative changes to Subtitle B. For example, one suggestion was that Congress grant the states enforcement authority under Subtitle B to potentially increase enforcement activity. Another suggested change to Subtitle B was to provide for a private right of action to allow consumers whose personal information was stolen to obtain some level of restitution from perpetrators of the violation. These suggestions were originally considered when the legislation was debated, but reflect the continued interests and concerns of FTC staff and the privacy and consumer groups with whom we spoke. We did not evaluate the potential impact or practicality of these suggestions, since we found no consensus on these ideas. We are not making any recommendations in this report.

Background

The Gramm-Leach-Bliley Act eliminated many of the legislative barriers to affiliations among banks, securities firms, and insurance companies.[7] One of the expected benefits of expanded affiliation across industries was to provide financial institutions with greater access—by sharing information across affiliates—to a tremendous amount of nonpublic personal information obtained from customers through normal business transactions. This greater access to customer information is important to financial institutions wishing to diversify and may give customers better product information than they would have otherwise received. At the same time, there are increasing concerns about how financial institutions use and protect their customers' personal information. Some financial industry observers have characterized the privacy provisions contained in GLBA as the most far-reaching set of privacy standards—pertaining to financial information and certain personal data—ever adopted by Congress.

Title V of GLBA sets forth major privacy provisions under two subtitles, which apply to a wide range of financial institutions.[8] Among other things, Subtitle A requires financial institutions to provide a notice to its customers on its privacy policies and practices and how information is disclosed to their affiliates and nonaffiliated third parties. Financial

[7] Most notably, GLBA repealed the Glass-Steagall Act, which placed restrictions on banks affiliating with securities firms and other banking activities.

[8] In general, the term "financial institution" means any institution engaged in financial activities, such as lending money or investing in securities for others, as specified in the Bank Holding Company Act, as amended by GLBA.

institutions are required to provide consumers the opportunity to "opt out" of having their nonpublic personal information shared with nonaffiliated third parties, with certain exceptions.[9] Subtitle A also limits the ability of financial institutions to reuse and redisclose nonpublic personal information about consumers that is received from nonaffiliated financial institutions.

Subtitle B of GLBA makes it a crime for persons to obtain, or attempt to obtain, or cause to be disclosed customer information from financial institutions by false or fraudulent means. Subtitle B provides for both criminal penalties and civil administrative remedies through FTC and federal banking regulatory enforcement. Subtitle B places the primary responsibility for enforcing the subtitle's provisions with FTC. In addition, federal financial regulators are given administrative enforcement authority with respect to compliance by depository institutions under their jurisdiction. Under section 525 in Subtitle B, the banking regulators, NCUA, and SEC are required to review their regulations and guidelines and to make the appropriate revisions as necessary to deter and detect the unauthorized disclosure of customer financial information by false pretenses. Subtitle B contains five categories of exceptions to the prohibition on obtaining customer information by false pretenses. Specifically, there were exceptions for law enforcement agencies; financial institutions under specified circumstances, such as testing security procedures; insurance institutions for investigating insurance fraud; public data filed pursuant to the securities laws; and state-licensed private investigators involved in collecting child support judgments.

Pretext calling is one common method used to fraudulently obtain nonpublic customer financial information from a financial institution. Pretext calling often involves an information broker—a company that obtains and sells financial information and other data about individual consumers—contacting a bank and pretending to be a customer who has forgotten an account number. Pretext callers may also pose as law enforcement agents, social workers, potential employers, and other figures of authority. The pretext caller then obtains detailed account data—often including exact balances and recent transactions—and sells that information to lawyers, collection agencies, or other interested parties.

[9] A financial institution is obligated to comply with the notice and opt-out provisions under Subtitle A only with respect to individual consumers who obtain a financial product or service to be used primarily for personal, family, or household purposes.

Perhaps more importantly, pretext calling can lead to "identity theft." Generally, identity theft involves "stealing" another person's personal identifying information—Social Security number, date of birth, mother's maiden name, etc.—to fraudulently establish credit, run up debt, or take over existing financial accounts. The American Bankers Association (ABA) reported that its 1998 industry survey found that $3 out of $4 lost by a community bank to credit fraud was due to some form of identity theft.[10] Consumers targeted by identity thieves typically do not know they have been victimized until the thieves fail to pay the bills or repay the loans. Identity thieves also buy account information from information brokers to engage in check and credit card fraud. A survey by the California Public Interest Research Group and Privacy Rights Clearinghouse found that fraudulent charges made on new and existing accounts in identity theft cases averaged $18,000.[11] The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime punishable, in most circumstances, by a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.[12]

Too Soon to Assess the Efficacy And Adequacy of Remedies

It is too soon to assess the efficacy and adequacy of the remedies provided for in Subtitle B of Title V of the Gramm-Leach-Bliley Act of 1999. As of March 31, 2001, federal regulatory and enforcement agencies had not taken any enforcement actions or prosecuted any cases under this law. Federal agencies have taken initial regulatory steps to ensure that financial institutions establish appropriate safeguards designed to protect customer information. Financial institutions are required to be in compliance with the new regulations by July 1, 2001. Lastly, we found that there are limited data available to indicate the prevalence of fraudulent access to financial information or pretext calling.

[10] Testimony of Richard H. Harvey, Jr. on behalf of the American Bankers Association, Committee on Banking and Financial Services, United States House of Representatives. Sept. 13, 2000, pp. 5-6.

[11] California Public Interest Research Group and Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak Out on Identity Theft*, May 2000.

[12] 18 U.S.C. §1028. To fulfill its legislative responsibilities under this act, FTC established an Identity Theft Clearinghouse database to collect consumer complaints and share this information among law enforcement agencies across the country and plans to share information with credit reporting agencies as appropriate. FTC also established a hotline for victims to call to report incidents of identity theft and to receive counseling and information.

FTC, the Department of Justice, and Federal Financial Regulators Have Not Yet Taken Any Enforcement Actions Under Subtitle B

As of March 31, 2001, FTC had initiated a number of nonpublic investigations targeting pretexters but had not fully prosecuted any cases for Subtitle B violations that prohibit obtaining customer financial information through fraudulent methods. Thus, FTC officials told us that it was too soon to assess the efficacy and adequacy of the remedies of this law because they had not had any experiences prosecuting under the statute. They stated that it would take at least 3 to 5 years before there would be sufficient case history to permit them to assess the usefulness of the statute. FTC officials stated that one key benefit of Subtitle B is that it clearly established pretext calling as a federal crime, making it easier for them to take enforcement actions against firms that use fraud to access financial information. Prior to the enactment of GLBA, FTC had undertaken one enforcement action against an information broker that was engaging in pretext calling. FTC pursued this case under its general statute, section 5(a) of the Federal Trade Commission Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."[13] One of the five FTC commissioners issued a dissenting statement because he felt pretext calling did not clearly violate FTC's long-standing deception or unfairness standard. In June 2000, FTC settled the case, which prohibited the broker from engaging in pretext calling, and entered into a $200,000 settlement with the broker, which was subsequently suspended on the basis of the defendants' inability to pay.

FTC reported to Congress that its staff began a nonpublic investigation in June 2000 to test compliance with Subtitle B provisions that prohibit the use of fraudulent or deceptive means to obtain personal financial information. On January 31, 2001, FTC issued a press release regarding its "Operation Detect Pretext." As part of this operation, FTC's staff had conducted a "surf" of more than 1,000 Web sites and a review of more than 500 advertisements in the print media for firms that offered to conduct financial searches. FTC reported that it had identified approximately 200 firms that offered to obtain and sell asset or bank account information about consumers. FTC stated that it had sent notices to these 200 firms on January 26, 2001, advising them that their practices must comply with GLBA's restrictions as well as other applicable federal laws, including the Fair Credit Reporting Act.[14] According to the press release, the notices also

[13] 15 U.S.C. §45(a)(1).

[14] 15 U.S.C. §§1681 et. seq. The Fair Credit Reporting Act regulates the collection and dissemination of personal information by consumer reporting agencies and persons, including corporations, who regularly procure or cause to be prepared consumer reports on any individual for use by a third party.

informed the firms that FTC would continue to monitor Web sites and print media advertisements offering financial searches to ensure that they complied with GLBA and all other applicable federal laws. As part of Operation Detect Pretext, FTC published a consumer alert entitled *Pretexting: Your Personal Information Revealed* that offers tips to consumers on protecting their personal information. On April 18, 2001, FTC filed suit to halt the operations of three information brokers who used false pretenses, fraudulent statements, or impersonation to illegally obtain consumers' confidential financial information, such as bank balances, and sell it.

The Department of Justice had not prosecuted any cases involving pretext calling as of March 31, 2001. Department officials told us that in their experience, pretext calling is typically a component of a larger fraud scheme. They stated that they would normally prosecute under the larger fraud schemes, such as mail, wire, or bank fraud. They supported the new legislation and felt it provided them with sufficient enforcement authority to address the full criminal activity for related bank fraud cases. They said it was premature to comment on the adequacy of the criminal penalties provided in the act because they had no experience in prosecuting cases under this statute. They believed it would likely take several years before they would have adequate case history under this law to make any suggestions concerning the remedies contained in Subtitle B.

Officials from the federal banking agencies, SEC, and NCUA all agreed that it was too soon to assess the efficacy and adequacy of the remedies in Subtitle B. None of these agencies had taken enforcement actions against financial institutions for violations of Subtitle B—which prohibits using fraudulent means to obtain personal financial information. Federal banking officials told us that they did not anticipate that there would be many circumstances in which they would use this law against a financial institution, unless an officer or employee of a financial institution was involved in the fraud. They stated that the financial institutions are typically one of the "victims" of pretext calling because the cost of the related crimes—credit card fraud or identity theft—is often borne by the financial institutions. They told us that they felt they had sufficient enforcement authority to take action against a bank officer or employee involved in fraudulent activities prior to the passage of Subtitle B and did not believe the statute gave them any additional enforcement authority. However, they supported the legislation because it explicitly makes fraudulent access to financial information a crime.

Federal Regulatory Agencies Have Taken Initial Steps to Ensure That Financial Institutions Implement Controls to Prevent Fraudulent Access to Financial Information

Subtitle B of GLBA requires the federal banking agencies, NCUA, SEC, or self-regulatory organizations, as appropriate, to review their regulations and guidelines and prescribe such revisions as necessary "to ensure that financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect" fraudulent access to customer information.[15] As of April 2001, the federal banking agencies and NCUA were coordinating their efforts to update the guidelines on pretext calling that they issued to financial institutions in the latter part of 1998 and early 1999. The earlier advisory was jointly prepared by the federal banking agencies, Federal Bureau of Investigation, U.S. Secret Service, Internal Revenue Service, and Postal Inspection Service. The advisory alerted institutions to the practice of pretext calling and warned institutions about the need to have strong controls in place to prevent the unauthorized disclosure of customer information. According to federal banking agency officials, they had discussed updating the guidelines to provide more information on identity theft and its relationship to pretext calling, but had not issued the updated guidelines as of April 2001.

In addition, NCUA and the federal banking agencies issued guidelines for financial institutions relating to administrative, technical, and physical safeguards for customer records and information on January 30, 2001,[16] and February 1, 2001.[17] As discussed earlier, Subtitle A of GLBA requires the federal banking regulatory agencies, FTC, NCUA, SEC, and the state insurance regulators to establish standards for safeguarding customer information for the institutions that they regulate. Among other things, these standards are to establish safeguards to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.[18] For example, the guidelines issued by the banking agencies and NCUA require institutions

[15] 15 U.S.C. §6825.

[16] Federal Register: January 30, 2001 (Volume 66, Number 20), Rules and Regulations, pp. 8152-8162. *Guidelines for Safeguarding Member Information*; Final Rule, 12 C.F.R. Part 748. NCUA's guidelines establish requirements for federally insured credit unions. Privately insured credit unions are subject to FTC regulation for Subtitles A and B.

[17] Federal Register: February 1, 2001 (Volume 66, Number 22), Rules and Regulations, pp. 8615-8641. *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness*; Final Rule, 12 C.F.R. Part 30, et al.

[18] 15 U.S.C. §6801.

to have controls designed to prevent employees from providing customer information to unauthorized individuals who may seek to obtain customer information through fraudulent means. Financial institutions under the jurisdiction of the federal banking agencies and NCUA are required to put in place by July 1, 2001, information security programs that satisfy the requirements of the guidelines. Officials at the bank regulatory agencies and NCUA told us that they plan to include the new guidelines for safeguarding customer financial information in their examination procedures.

On June 22, 2000, SEC adopted regulations that require, among other things, brokers, dealers, investment companies, and registered investment advisors to adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[19] These policies and procedures must be reasonably designed to (1) ensure the security and confidentiality of customer records and information, (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information, and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[20] SEC stated that it had conducted preliminary examinations of securities firms' efforts to comply with these requirements and planned to include firms' compliance with the regulations as a formal component of its examination program as of July 2001—the mandatory compliance date. SEC did not plan to develop additional guidance on pretext calling because it concluded that its regulation on safeguarding customer financial information would satisfy the agency guidance requirements of Subtitle B.

FTC has begun the rulemaking process to establish safeguarding standards for customer information but had not issued its proposed regulations as of March 1, 2001. FTC officials told us that they expect to issue their

[19] Federal Register: June 29, 2000 (Volume 65, Number 126), Rules and Regulations, pp. 40334-40373. *Privacy Consumer Financial Information (Regulation S-P)*; Final Rule, 17 C.F.R. Part 248, et al.

[20] 17 C.F.R. 248.30.

proposed regulations by July 1, 2001[21]—the date when financial institutions regulated by the federal banking agencies, NCUA, and SEC are required to have their safeguards in place. Subtitle B does not require state insurance regulators to review their regulations and guidance to ensure that financial institutions under their jurisdiction have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information. However, Subtitle A does require the state insurance regulators to establish standards for safeguarding customer financial information. As of March 1, 2001, the National Association of Insurance Commissioners (NAIC)[22] was discussing how to approach these standards, either through issuing regulations, similar to SEC, or through general guidelines, similar to the federal banking regulators. In addition, the states were still in the process of drafting laws and regulations to be in compliance with the disclosure, information-sharing, and opt-out requirements contained in Subtitle A.

Limited Data to Indicate the Impact of Subtitle B

Officials from the federal and state agencies whom we contacted were not aware of any available data sources that would indicate the prevalence of fraudulent access to financial information. Law enforcement officials told us that they do not collect such information. Justice officials stated that they track the number of offenses filed under the statute, but no matters had been brought forward as of March 1, 2001. Representatives from privacy or consumer groups also told us they were unaware of any statistics or databases that track the prevalence of pretexting.

To obtain an indicator of the prevalence of pretext calling, we requested Suspicious Activity Report (SAR) data from the Financial Crimes Enforcement Network (FinCEN).[23] Although banks are not obligated to

[21] FTC had issued its advance notice of proposed rulemaking and request for comment on September 7, 2000. The comment period originally ended October 10, 2000, and was extended through October 24, 2000. FTC staff were still drafting the proposed regulations when we met with them in March 2001. Once the proposed regulations are released for comment, the public comment period is generally 30 to 60 days.

[22] State insurance regulators created the NAIC in 1871 to address the need to coordinate regulation of multistate insurers and to provide a forum for uniform policy development. Its membership includes insurance regulators from the 50 states, the District of Columbia, and the 4 U.S. territories.

[23] Within the Department of the Treasury, FinCEN establishes, oversees, and implements policies to prevent and detect money laundering. FinCEN provides analytical support for law enforcement investigative efforts and maintains a database that contains information reported by banks and other types of financial institutions on potential money laundering, such as the SARs.

report pretext-calling attempts, banks are generally required to file a SAR when it detects a known or suspected criminal violation of federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act.[24] Banks are not required to file SARs until a certain dollar threshold has been met or exceeded.[25] FinCEN officials told us that "false pretense"—their wording for pretext—is not part of the SAR data because it is not considered a criterion for filing a SAR, but it may be kept as secondary information contained in the narrative field as reported by the banks. At our request, in September 2000, FinCEN officials searched the narrative field of their database and found that only 3 of the 400,000 SARs in their database contained narrative regarding the use of false pretenses to obtain customer financial information. FinCEN subsequently advised us that recently completed research on SAR data for the calendar year 2000 indicated an increase in bank reporting on identity theft during the year. FinCEN noted that it is possible there may be an attendant increase in narrative reporting on attempted fraudulent access to financial information. Representatives of the Interagency Bank Fraud Working Group[26] whom we contacted also discussed potentially expanding the narrative section of the SARs to capture information on pretext calling and identity theft.

In our effort to identify indicators of the impact of Subtitle B, we reviewed information from FTC's Identity Theft Clearinghouse Database[27] and the federal financial regulators' consumer complaint databases. According to

[24] Treasury's SAR rule requires reporting suspicious activities related to the Bank Secrecy Act and other anti-money laundering statutes, but the federal banking agencies' SAR rules require reporting suspicious activities that go beyond anti-money laundering statutes, such as insider criminal misconduct.

[25] Banks are generally required to file a SAR relevant to a possible violation of law or regulation when a transaction is conducted at or through a bank and aggregates at least $5,000.

[26] The Interagency Bank Fraud Working Group includes representatives from the federal financial institution regulatory agencies and federal law enforcement agencies that meet to promote coordination between the regulatory and law enforcement communities in the investigation and prosecution of financial institution fraud cases.

[27] FTC established the Identity Theft Data Clearinghouse database to help meet its data gathering and coordination responsibilities under the Identity Theft and Assumption Deterrence Act of 1998. The Identity Theft Data Clearinghouse was launched in November 1999 and contains entries from consumers and victims of identity theft. The database is a subset of FTC's Consumer Sentinel database, which contains general consumer fraud complaints and is accessible to law enforcement agencies throughout the United States, Canada, and Australia.

FTC staff, victims of identity theft often typically did not know how their personal financial information was obtained, unless they had lost their wallets or family members or friends were involved. Therefore, it is unlikely these victims would be aware of whether someone had used pretexting to obtain their information. FTC reported that they had processed over 40,000 entries from consumers and victims of identity theft as of December 31, 2000. Of those entries, about 88 percent had no relationship with the identity theft suspect (about 12 percent had a personal relationship with the identity theft suspect).

According to officials from the federal banking agencies, NCUA, and SEC, they received few consumer complaints related to financial privacy. They explained that they believed that consumers may be more likely to report potential cases of fraud to their banks or to law enforcement agencies first, rather than contacting the financial regulators. Thus, consumer complaints submitted to the federal regulators may not accurately reflect the prevalence of financial privacy violations. In addition, consumer complaint databases maintained by the regulators typically did not have a specific category to capture pretext-calling allegations, which is distinct from related incidents of fraud, such as credit card fraud. In October 2000, FDIC expanded its coding system to capture additional information related to financial privacy complaints.

Pretexting is difficult to detect and is likely to be underreported. Many officials told us that pretexting was a common practice, especially among private investigators. According to many law enforcement officials we spoke with, crimes involving pretexting are particularly difficult to prove, and it was unlikely that pretexting would be reported or prosecuted as a single crime. If a pretexter is clever in his or her fraud scheme and successful in obtaining financial information, the financial institution is unaware that it was fooled into providing information. Often there is a time lag before victims of pretext calling suffer financial loss, and they may not be aware of how their financial information was obtained. According to law enforcement officials we spoke with, offenders using fraud to access financial information are generally detected as part of a larger crime, such as credit card, identity theft, or other bank fraud. An increase in related crimes, although not directly correlated to pretext calling, may be a possible indication of the prevalence of fraudulent access to financial information. For example, the number of SAR filings by the banks related to check fraud, debit and credit card fraud, false statement,

and wire transfer fraud continued to increase from 1998 to 1999, according to the October 2000 report by the Bank Secrecy Act Advisory Group.[28]

Others Suggested Few Legislative or Administrative Changes for Consideration

As stated previously, more time and experience are needed to assess the efficacy and adequacy of the remedies contained in Subtitle B regarding fraudulent access to financial information. Therefore, we are not making any recommendations for additional legislation or regulatory actions. During our consultations with representatives from FTC, the federal banking agencies, NCUA, SEC, and federal and state enforcement agencies and insurance regulators, we obtained their views about the efficacy and adequacy of the subtitle's other provisions. Some federal and state officials and representatives from consumer and privacy groups we contacted had some suggestions regarding possible changes to Subtitle B provisions, which are presented below. As discussed earlier, we did not evaluate how practical these suggestions were since we found no consensus on these issues. These suggestions reflect the continued concerns and issues raised by FTC staff and the privacy and consumer groups with whom we spoke.

FTC staff and some state officials suggested that states be allowed to take enforcement actions for violations of Subtitle B provisions. According to these FTC staff and state officials, this would allow the states to augment the federal resources used to enforce compliance with the Subtitle B prohibition against pretext calling. Earlier versions of the House and Senate bills that were the basis for Subtitle B contained provisions that provided for state actions for injunctive relief or for recovering damages of not more than $1,000 per violation. These provisions were subsequently eliminated in the House and Conference versions of the legislation. FTC staff stated that the additional resources of the state attorneys general would be particularly helpful in enforcing compliance by some of the smaller information brokers that may otherwise escape detection or monitoring. According to some of the state officials we contacted, allowing state actions under the federal statute would increase the deterrent effects of the legislation. However, other state officials stated that they did not expect that providing states with enforcement authority under this statute would result in significantly greater enforcement activity due to resource limitations at the state enforcement level.

[28] Members of the Bank Secrecy Act Advisory Group include the federal financial regulatory agencies, law enforcement agencies, as well as representatives from the financial services industry.

Some of the consumer and privacy groups suggested that a private right of action provision be added to allow the consumers who were the victims of pretext calling to obtain financial compensation from the perpetrators of the violations. Like the state enforcement action provision, earlier House and Senate versions of Subtitle B contained provisions, which were subsequently eliminated, that would have allowed for civil lawsuits by individuals and financial institutions. These provisions recognized that pretext-calling victims will, in some instances, have a stronger incentive to proceed against an information broker or the broker's client than a law enforcement agency or prosecutor operating with limited resources and forced to juggle competing priorities, particularly in those cases in which the amount of monetary damages is minimal. According to some of the state officials we contacted, the possibility of civil lawsuits would potentially increase the penalties for violating the statute's provisions and, thus, help to deter such criminal activities. However, some officials did not agree with this suggestion and stated that a private right of action could also result in unintended consequences, such as frivolous lawsuits and overcrowded court dockets.

There were differing suggestions made regarding the provision in the statute that allows private investigators to use pretext calling under certain conditions. The statute allows state-licensed private investigators to use pretext calling to collect child support from persons adjudged to have been delinquent by a federal or state court and if authorized by an order or judgment of a court of competent jurisdiction. The exception for state-licensed private investigators is nullified if prohibited by another federal or state law or regulation. Some consumer and privacy representatives stated that the exception was too broad and could result in potential abuse. On the other hand, one of the trade groups for private investigators wanted Congress to amend Subtitle B to allow the use of pretexting as an investigative tool to locate hidden assets when investigators contact judgment debtors or persons who have committed fraud. According to this trade group, one of the unintended consequences of Subtitle B is that it makes it easier for criminals and judgment debtors to hide their assets from lawful collection.

Agency Comments and Our Evaluation

We provided a draft of this report to the Chairman of the Federal Trade Commission, the Attorney General, the Secretary of the Treasury, the Chairman of the Federal Deposit Insurance Corporation, the Chairman of the Federal Reserve Board, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Acting Chairman of the National Credit Union Administration, the Chair of the National Association of

Insurance Commissioners, and the Acting Chairman of the Securities and Exchange Commission for their review and consultation. The Federal Trade Commission, Treasury, Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency, NCUA, and SEC agreed with our overall report's message and provided technical comments, which we incorporated into the appropriate sections of this report. The Office of Thrift Supervision, Justice, and NAIC agreed with our overall message and did not provide any comments on our report.

In commenting on our draft report, the Financial Crimes Division of the U.S. Secret Service expressed concern over an increase in attacks directed at on-line service databases that ultimately contain personal financial information, such as credit card numbers, Social Security numbers, etc. The Secret Service also emphasized that they support any steps taken toward deterring individuals from attempting attacks directed at any institution's infrastructure for the purposes of obtaining financial information. Although we acknowledge these concerns and their support on securing the privacy of financial information on-line, our study did not focus on on-line information security.

We are sending copies of this report to the requesting congressional committees. We are also sending copies to the Honorable Robert Pitofsky, Chairman, Federal Trade Commission; the Honorable John Ashcroft, the Attorney General; the Honorable Paul H. O'Neill, Secretary of the Treasury; the Honorable Donna Tanoue, Chairman, the Federal Deposit Insurance Corporation; the Honorable Alan Greenspan, Chairman, the Federal Reserve Board of Governors; the Honorable John D. Hawke, Jr., Comptroller of the Currency; the Honorable Ellen Seidman, Director, the Office of Thrift Supervision; the Honorable Dennis Dollar, Acting Chairman, the National Credit Union Administration; the Honorable Kathleen Sebelius, Chair, the National Association of Insurance Commissioners; and the Honorable Laura S. Unger, Acting Chairman, the Securities and Exchange Commission.

If you or your staff have any questions on this report, please contact me at (202) 512-8678 or Harry Medina at (415) 904-2000. Key contributors to this report were Debra R. Johnson, Nancy Eibeck, Shirley A. Jones, and Charles M. Johnson, Jr.

Richard J, Hillman
Director, Financial Markets and
Community Investment

List of Congressional Committees:

The Honorable Phil Gramm
Chairman
The Honorable Paul S. Sarbanes
Ranking Member
Committee on Banking, Housing,
and Urban Affairs
United States Senate

The Honorable Orrin G. Hatch
Chairman
The Honorable Patrick Leahy
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Michael G. Oxley
Chairman
The Honorable John J. LaFalce
Ranking Minority Member
Committee on Financial Services
House of Representatives

The Honorable F. James Sensenbrenner, Jr.
Chairman
The Honorable John Conyers, Jr.
Ranking Minority Member
Committee on the Judiciary
House of Representatives

The Honorable W.J. "Billy" Tauzin
Chairman
The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Appendix I: Scope and Methodology

To determine the efficacy and adequacy of the remedies provided by the Gramm-Leach-Bliley Act of 1999 (GLBA) in addressing attempts to obtain financial information by false pretenses, we interviewed officials from the Department of Justice, the Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Federal Trade Commission (FTC), the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Securities and Exchange Commission. Within Justice, we interviewed officials representing its Criminal and the Civil Divisions, the Federal Bureau of Investigation, and the Executive Office of the United States Attorneys. In addition, we talked with officials at seven U.S. attorney offices: (1) Eastern District of New York, (2) Southern District of New York, (3) Central District of California, (4) Northern District of California, (5) District of Massachusetts, (6) District of Minnesota, and (7) District of Colorado. The officials at the U.S. attorney offices we spoke with are primarily responsible for overseeing any federal prosecution of financial crimes that occur in their respective districts. We selected these offices because they were located in states that had been identified as being particularly active regarding consumer financial privacy. We also consulted with a number of state officials located in those same five states. Specifically, we interviewed staff from the state insurance regulatory agency and the attorney general's office located in California, Colorado, Massachusetts, Minnesota, and New York. In addition, we interviewed representatives of the National Association of Insurance Commissioners.

Within Treasury, we talked with officials from its Office of Financial Institutions, Office of Enforcement, Financial Crimes Enforcement Network, Internal Revenue Service, and U.S. Secret Service. We interviewed FTC staff from the Bureau of Consumer Protection who monitor compliance of financial institutions under FTC's jurisdiction and FTC officials responsible for designing and implementing "Operation Pretext," and we reviewed relevant FTC documents on FTC's enforcement activities related to information brokers. We also examined the regulations and guidelines developed by the Federal Deposit Insurance Corporation, the Federal Reserve Board, FTC, the National Credit Union Administration, the Office of Comptroller of the Currency, the Office of Thrift Supervision, and the Securities and Exchange Commission related to their implementation of the privacy provisions of GLBA. In addition, we requested and reviewed data from the various agencies regarding enforcement activity and consumer complaints related to fraudulent access to financial information.

To identify suggestions for additional legislation or regulatory actions with respect to fraudulent access to financial information, we obtained the viewpoints of the federal and state agencies' officials we met with and interviewed a number of consumer and privacy groups that have been active in the area of financial privacy. Specifically, we interviewed representatives of the Center for Democracy and Technology, the Consumer Federation of America, Consumers Union, Eagle Forum, the Electronic Privacy Information Center, the Privacy Rights Clearinghouse, Privacy Times, the U.S. Public Interest Research Group, and the California Public Interest Research Group. In addition, we also talked with the American Bankers Association; the Association of Credit Bureaus; the North American Securities Administrators Association, Inc.; and the National Council of Investigation and Security Services, which represents the investigation and guard industry.

We conducted our work in Washington, D.C.; San Francisco, CA; and New York City, NY, between August 2000 and April 2001, in accordance with generally accepted government auditing standards.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- E-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)