

This is the accessible text file for GAO report number GAO-06-674 entitled 'Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data' which was released on July 26, 2006.

This text file was formatted by the U.S. Government Accountability Office (GAO) to be accessible to users with visual impairments, as part of a longer term project to improve GAO products' accessibility. Every attempt has been made to maintain the structural and data integrity of the original printed product. Accessibility features, such as text descriptions of tables, consecutively numbered footnotes placed at the end of the file, and the text of agency comment letters, are provided but may not exactly duplicate the presentation or format of the printed version. The portable document format (PDF) file is an exact electronic replica of the printed version. We welcome your feedback. Please E-mail your comments regarding the contents or accessibility features of this document to Webmaster@gao.gov.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. Because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

Report to the Committee on Banking, Housing and Urban Affairs, U.S. Senate:

United States Government Accountability Office:

GAO:

June 2006:

Personal Information:

Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data:

Personal Information:

GAO-06-674:

GAO Highlights:

Highlights of GAO-06-674, a report to the Committee on Banking, Housing and Urban Affairs, U.S. Senate

Why GAO Did This Study:

The growth of information resellers—companies that collect and resell publicly available and private information on individuals—has raised privacy and security concerns about this industry. These companies collectively maintain large amounts of detailed personal information on nearly all American consumers, and some have experienced security breaches in recent years.

GAO was asked to examine (1) financial institutions' use of resellers; (2) federal privacy and security laws applicable to resellers; (3)

federal regulators' oversight of resellers; and (4) regulators' oversight of financial institution compliance with privacy and data security laws. To address these objectives, GAO analyzed documents and interviewed representatives from 10 information resellers, 14 financial institutions, 11 regulators, industry and consumer groups, and others.

What GAO Found:

Financial institutions such as banks, credit card companies, securities firms, and insurance companies use personal data obtained from information resellers to help make eligibility determinations, comply with legal requirements, prevent fraud, and market their products. For example, lenders rely on credit reports sold by the three nationwide credit bureaus to help decide whether to offer credit and on what terms. Some companies also use reseller products to comply with PATRIOT Act rules, to investigate fraud, and to identify customers with specific characteristics for marketing purposes.

GAO found that the applicability of the primary federal privacy and data security laws—the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLBA)—to information resellers is limited. FCRA applies to information collected or used to help determine eligibility for such things as credit or insurance, while GLBA only applies to information obtained by or from a GLBA-defined financial institution. Although these laws include data security provisions, consumers could benefit from the expansion of such requirements to all sensitive personal information held by resellers.

The Federal Trade Commission (FTC) is the primary federal agency responsible for enforcing information resellers' compliance with FCRA's and GLBA's privacy and security provisions. Since 1972, the agency has initiated formal enforcement actions against more than 20 resellers, including the three nationwide credit bureaus, for violating FCRA. However, FTC does not have civil penalty authority under the privacy and safeguarding provisions of GLBA, which may reduce its ability to enforce that law most effectively against certain violations, such as breaches of mass consumer data.

In overseeing compliance with privacy and data security laws, federal banking and securities regulators have issued guidance, conducted examinations, and taken formal and informal enforcement actions. A recent national survey sponsored by the National Association of Insurance Commissioners (NAIC) identified some noncompliance with GLBA by insurance companies, but state regulators have not laid out clear plans with NAIC for following up to ensure these issues are adequately addressed.

Figure: Typical Information Flow through Resellers to Financial Institutions:

[See PDF for Image]

Source: GAO(analysis); Art Explosion (image).

[End of Figure]

What GAO Recommends:

Congress should consider (1) requiring information resellers to safeguard all sensitive personal information they hold, and (2) giving

FTC civil penalty authority for enforcement of GLBA's privacy and safeguarding provisions. GAO also recommends that state insurance regulators ensure compliance with GLBA.

[Hyperlink, <http://www.gao.gov/cgi-bin/getrpt?GAO-06-674>].

To view the full product, including the scope and methodology, click on the link above. For more information, contact Yvonne D. Jones at (202) 512-8678 or jonesy@gao.gov.

[End of Section]

Contents:

Letter:

Results in Brief:

Background:

Financial Institutions Use Information Resellers for Eligibility Determinations, Fraud Prevention, PATRIOT Act Compliance, and Marketing:

Federal Privacy and Information Security Laws Apply to Many Information Reseller Products, Depending on Their Use and Source:

FTC Has Primary Responsibility for Enforcing Information Resellers' Compliance with Privacy and Information Security Laws:

Agencies Differ in Their Oversight of the Privacy and Security of Personal Information at Financial Institutions:

Conclusions:

Matters for Congressional Consideration:

Recommendation for Executive Action:

Agency Comments:

Appendix I: Scope and Methodology:

Appendix II: Sample Information Reseller Reports:

Sample Insurance Claims History Report:

Sample Deposit Account History Report:

Sample Identity Verification and OFAC Screening Report:

Sample Fraud Investigation Report:

Appendix III: Comments from the Federal Trade Commission:

Appendix IV: GAO Contact and Staff Acknowledgments:

Figures:

Figure 1: Typical Information Flow through Resellers to Financial Institutions:

Figure 2: GLBA Privacy Provisions:

Figure 3: Enforcement Responsibilities for Selected Financial Institutions under FCRA and GLBA:

Figure 4: Sample Insurance Claims History Report:

Figure 5: Sample Deposit Account History Report:

Figure 6: Sample Identity Verification and OFAC Screening Report:

Figure 7: Sample Fraud Investigation Report:

Abbreviations:

CRA: consumer reporting agency:
DISB: District of Columbia's Department of Insurance, Securities and Banking:
FACT Act: Fair and Accurate Credit Transactions Act:
FCRA: Fair Credit Reporting Act:
FDIC: Federal Deposit Insurance Corporation:
FFIEC: Federal Financial Institutions Examination Council:
FRB: Board of Governors of the Federal Reserve System:
FTC: Federal Trade Commission:
FTC Act: Federal Trade Commission Act:
GLBA: Gramm-Leach-Bliley Act:
NAIC: National Association of Insurance Commissioners:
NCUA: National Credit Union Administration:
NYSE Regulation: New York Stock Exchange Regulation:
OCC: Office of the Comptroller of the Currency:
OFAC: Office of Foreign Assets Control:
OTS: Office of Thrift Supervision:
SEC: Securities and Exchange Commission:
USA PATRIOT ACT: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act:

United States Government Accountability Office:
Washington, DC 20548:

June 26, 2006:

The Honorable Richard C. Shelby:
Chairman:
The Honorable Paul S. Sarbanes:
Ranking Minority Member:
Committee on Banking, Housing and Urban Affairs:
United States Senate:

The growth in recent years of information resellers--companies that collect, aggregate, and resell publicly available and private information on individuals--has raised privacy and security concerns related to this industry.[Footnote 1] Information resellers maintain and sell vast amounts of detailed personal information on nearly all American consumers--including such things as Social Security numbers, home and automobile values, occupations and hobbies. In addition, security breaches at some of these companies have raised concerns in light of the increasing problem of identity theft. Some policymakers and consumer advocates believe that not enough is known about these resellers and the information about consumers that they maintain and share.

Information resellers include consumer reporting agencies (CRA), which assemble and share credit histories and other personal information used to help make important decisions about individuals, such as their eligibility for financial services. Other companies, sometimes called "data brokers," collect personal information from a variety of sources for such things as marketing and fraud prevention. Advances in technology and the computerization of public records in recent years have fostered significant growth in the size of the reseller industry and the amount of personal consumer data that these companies assemble and distribute.

The primary federal laws governing the sharing and use of personal information by private sector companies are the Fair Credit Reporting Act (FCRA) and subtitle A of title V of the Gramm-Leach-Bliley Act (GLBA).^[Footnote 2] Several federal and state agencies and self-regulatory organizations enforce these laws, including the Federal Trade Commission (FTC); the banking regulators--Board of Governors of the Federal Reserve System (FRB), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), Federal Deposit Insurance Corporation (FDIC), and National Credit Union Administration (NCUA); the securities regulators--Securities and Exchange Commission (SEC), NASD (formerly known as the National Association of Securities Dealers), and New York Stock Exchange Regulation (NYSE Regulation); and state insurance regulators.

Concerned about financial institutions' use of information resellers, you asked us to examine (1) how financial institutions use data products supplied by information resellers, the types of information contained in these products, and the sources of the information; (2) how federal laws governing the privacy and security of personal data apply to information resellers, and what rights and opportunities exist for individuals to view and correct data held by resellers; (3) how federal financial institution regulators and the FTC oversee information resellers' compliance with federal privacy and information security laws; and (4) how federal financial institution regulators, state insurance regulators, and the FTC oversee financial institutions' compliance with federal privacy and information security laws governing consumer information, including information supplied by information resellers.

To address these objectives, we gathered and analyzed documents, and interviewed representatives from, 10 major information resellers; 14 financial institutions in the banking, securities, credit card, property/casualty insurance, and consumer lending industry sectors; and trade associations representing these firms. We also met with experts in the area of privacy law and with consumer advocacy organizations active in the field. Our audit work allows us to represent how financial institutions that offer a sizable and diverse portion of financial services in the United States use information resellers, and to describe the types of information products offered by the information resellers most commonly identified by these financial institutions. Our findings, however, are not representative of all financial institutions and information resellers. We also analyzed relevant laws, guidance, and regulations. Finally, to describe federal and state enforcement and supervisory activities, we interviewed and analyzed documents from FTC; the five federal banking and three securities regulators; the National Association of Insurance Commissioners (NAIC), which represents state insurance regulators; and the District of Columbia's Department of Insurance, Securities and Banking (DISB).

We conducted our review from June 2005 through May 2006 in accordance with generally accepted government auditing standards. A more extensive discussion of our scope and methodology appears in appendix I.

Results in Brief:

Financial institutions use data from information resellers to help determine individuals' eligibility for credit and insurance, comply with legal requirements, prevent fraud, and market products. Banks and other lenders use reseller data to help make eligibility and interest rate decisions for new applicants and existing customers, while insurance companies use these data to help make underwriting decisions regarding individual insurance applications. To meet PATRIOT Act requirements designed to prevent money laundering and transactions with known criminals, some financial institutions we spoke with use resellers to confirm the identity of applicants. In addition, reseller data are used to identify and investigate fraud, locate holders of delinquent accounts, and conduct due diligence on individuals associated with new business ventures. Many companies also use certain information reseller products for marketing purposes--such as to target potential customers who have certain characteristics or to gather additional information about existing customers to offer additional products. The specific information maintained by resellers varies depending on the nature of the reseller and the types and purposes of its products. Their products often include credit header data--identifying information at the top of a credit report that includes such things as name, current and prior addresses, telephone number, and Social Security number. Products used by lenders for eligibility determinations typically also contain detailed credit histories and scores, while products used by insurers may also contain past insurance claims filed by applicants. Many reseller products, particularly those used for fraud detection, include court and property records and bankruptcy filings, motor vehicle records, names of family members and associates, and professional licenses. Products used for marketing often include demographic information as well as information on individual consumers' interests and hobbies. Resellers' sources vary depending on the product, but may include public records from government agencies, publicly available information, such as telephone or business directories, and nonpublic or proprietary information from credit bureaus or provided to businesses directly by consumers.

The primary federal privacy and data security laws that apply to information resellers are the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA), but the applicability of these laws with regard to information resellers is limited. FCRA requires companies to safeguard and restrict their use and distribution of consumer information collected or used to determine eligibility for such things as credit, insurance, or employment, and provides rights to consumers to view and rectify errors in databases containing such information. The applicability of FCRA depends largely on the purpose for which the information is collected, and its intended and actual use, rather than the origins or nature of the information itself. Resellers offer many products from databases they consider not subject to FCRA, such as those used for many marketing and anti-fraud products. Information resellers vary in the extent to which they voluntarily provide consumers additional opportunities to view, correct, and opt out of the sharing of information that is not subject to FCRA. GLBA's privacy provisions restrict the sharing of nonpublic personal information collected by or acquired from financial institutions, except in certain

circumstances. However, these provisions only apply to information resellers covered by GLBA's definition of a "financial institution" or that maintain nonpublic personal information originating from such a financial institution. GLBA's safeguarding provisions require that steps be taken to ensure the security and confidentiality of customers' nonpublic personal information, but similarly this applies only to resellers that are GLBA financial institutions. Because of the limited applicability of FCRA and GLBA to information resellers, sensitive personal information these companies maintain is often not covered by explicit statutory safeguarding requirements. For example, some information resellers maintain data such as Social Security numbers in anti-fraud databases or household incomes in marketing databases that they do not consider subject to FCRA's or GLBA's safeguarding provisions. Requiring information resellers to take steps to prevent unauthorized access to all of the sensitive personal information they hold would help ensure that explicit data security requirements apply more comprehensively to a class of companies that maintains large amounts of such data. In addition, no federal statute requires companies to disclose breaches of sensitive personal information, although such a requirement could provide incentives to companies to improve data safeguarding and provide consumers at risk of identity theft or other related harm with useful information.

FTC is the primary federal agency responsible for enforcing information resellers' compliance with the privacy and information security requirements of FCRA and GLBA. Because it is a law enforcement agency, as opposed to a regulatory or supervisory agency, FTC does not routinely monitor or examine resellers, but can initiate investigations based on complaints and other sources. Since 1972, the agency has initiated formal enforcement actions against more than 20 consumer reporting agencies, including the three nationwide credit bureaus, for violating FCRA and the Federal Trade Commission Act (FTC Act). For example, in January 2006, ChoicePoint agreed to pay \$10 million in civil penalties and \$5 million for consumer redress (damages to compensate consumers for losses) to settle FTC charges that the company's security and record-handling procedures allegedly violated FCRA and the FTC Act. Many of FTC's cases involved companies alleged to have provided consumer report information without adequately ensuring that their customers had a permissible purpose for obtaining it. FTC cannot impose civil penalties for violations of GLBA's privacy and safeguarding provisions, as it can under FCRA. FTC has used its existing enforcement authority under GLBA to seek injunctions against financial institutions that have violated that law, and it can also seek redress for consumers. However, FTC staff have said that civil penalties would be a more effective tool for violations involving breaches of mass consumer data.

Federal and state regulators vary in the actions they take to oversee financial institutions' compliance with federal privacy and information security laws. In general, regulators told us that their oversight activities focus on the protection of all sensitive data; they do not typically distinguish whether the data were obtained from an information reseller or some other source. The five federal banking regulators have implemented and enforced GLBA and FCRA by issuing regulations and guidance, by using their examination procedures to check compliance with these laws, and by taking enforcement actions to address violations. SEC has issued regulations to implement GLBA for broker-dealers, investment companies, and SEC-registered investment advisers. SEC, NASD, and NYSE Regulation have also issued guidance and examined securities firms for compliance with GLBA's privacy and

safeguarding provisions, and as necessary have taken enforcement actions. State insurance regulators are responsible for enforcing GLBA for their states' property-casualty insurers. NAIC told us that state insurance regulators do not typically focus in their examinations on privacy requirements, but that they did recently participate in a multistate survey of insurance company compliance with GLBA. The survey identified a number of areas of noncompliance with GLBA, but the extent to which state regulators will be addressing these problems is unclear. FTC enforces securities firms' and insurance companies' compliance with FCRA and enforces both FCRA and GLBA for all financial institutions not otherwise supervised by another regulator. FTC has issued regulations to implement GLBA and initiated enforcement actions against consumer finance companies for not ensuring the security and confidentiality of sensitive customer information. Some federal banking regulators have authority to examine third-party service providers with which the banks may do business, and regulators have examined a limited number of information resellers under this authority.

This report suggests that Congress consider requiring information resellers, and potentially a broader class of entities, to safeguard all sensitive personal information they hold. We also suggest that Congress consider providing FTC with civil penalty authority for its enforcement of GLBA's privacy and safeguarding provisions. In addition, we recommend that state insurance regulators, individually and in concert with NAIC, take additional measures to ensure appropriate enforcement of insurance companies' compliance with GLBA's privacy and safeguarding requirements. We provided a draft of this report to FDIC, FRB, FTC, NAIC, NASD, NCUA, NYSE Regulation, OCC, OTS, and SEC, which provided technical comments that were incorporated as appropriate. In addition, FTC provided written comments, in which the agency noted that it agreed with our suggestions to Congress.

Background:

"Information reseller" is an umbrella term used to describe a wide variety of businesses that collect and aggregate personal information from multiple sources and make it available to their customers. The industry has grown considerably over the past two decades, in large part due to advances in computer technology and electronic storage. Courthouses and other government offices previously stored personal information in paper-based public records that were relatively difficult to obtain, usually requiring a personal visit to inspect the records. Nonpublic information, such as personal information contained in product registrations or insurance applications was also generally inaccessible. In recent years, however, the electronic storage of public and private records along with increased computer processing speeds and decreased data storage costs have fostered information reseller businesses that collect, organize, and sell vast amounts of personal information on virtually all American consumers.

The information reseller industry is large and complex, and these businesses vary in many ways. What constitutes an information reseller is not always clearly defined and little data exist on the total number of firms that offer information products. FTC and other federal agencies do not keep comprehensive lists of companies that resell personal information, and experts say that characterizing the precise size and nature of the information reseller industry can be difficult because it is evolving and lacks a clear definition. Although no comprehensive data exist, industry representatives say there are at least hundreds of information resellers in total, including some

companies that provide services over the Internet.[Footnote 3]

We include in our definition of information resellers the three nationwide credit bureaus--Equifax, Experian, and TransUnion, which primarily collect and sell information about the creditworthiness of individuals--as well as other resellers such as ChoicePoint, Acxiom, and LexisNexis, which sell information for a variety of purposes, including marketing.[Footnote 4] Other companies that sell information products include eFunds, which provides depository institutions with information on deposit account histories; Thompson West and Regulatory DataCorp, which help companies mitigate fraud and other risks; and ISO, which provides insurers with insurance claims histories and fraud prevention products. Information resellers sell their products to a broad spectrum of customers, including private companies, individuals, law enforcement bureaus and other government agencies.[Footnote 5] Although major information resellers generally offer their products only to customers who have successfully completed a credentialing process, some resellers offer certain products, such as compilations of telephone directory information, to the public at large. All of these businesses differ in nature, and they do not all focus exclusively on aggregating and reselling personal information. For example, Acxiom primarily provides customized computer services, and its information products represent a relatively small portion of the overall activities of the company.

Information resellers obtain their information from many different sources (see fig. 1). Generally, three types of information are collected: public records, publicly available information, and nonpublic information.

* Public records are a primary source of information about consumers, available to anyone, and can be obtained from governmental entities. What constitutes public records is dependent upon state and federal laws, but generally these include birth and death records, property records, tax lien records, voter registrations, licensing records, and court records (including criminal records, bankruptcy filings, civil case files, and legal judgments).

* Publicly available information is information not found in public records but nevertheless publicly available through other sources. These sources include telephone directories, business directories, print publications such as classified ads or magazines, Internet sites, and other sources accessible by the general public.

* Nonpublic information is derived from proprietary or nonpublic sources, such as credit header data, product warranty registrations, lists of magazine or catalog subscribers, and other application information provided to private businesses directly by consumers.[Footnote 6]

Information resellers hold or have access to databases containing a large variety of information about individuals. Although each reseller varies in the specific personal information it maintains, it can include names, aliases, Social Security numbers, addresses, telephone numbers, motor vehicle records, family members, neighbors, insurance claims, deposit account histories, criminal records, employment histories, credit histories, bankruptcy records, professional licenses, household incomes, home values, automobile values, occupations, ethnicities, and hobbies.

Figure 1: Typical Information Flow through Resellers to Financial Institutions:

[See PDF for image]

Source: GAO(analysis), Art Explosion(image).

[End of figure]

The various products offered by different types of information resellers are used for a wide range of purposes, including credit and background checks, fraud prevention, and marketing. Resellers often sell their data to each other--for example, the credit bureaus sell credit header data to other resellers for use in identity verification and fraud prevention products. Resellers might also purchase publicly available information from one another, rather than gathering the information themselves. The nature of the databases maintained and products offered by information resellers vary. Credit bureaus maintain an individual file on most Americans containing financial information related to that person's creditworthiness. Most other resellers do not typically maintain complete files on individuals, but rather collect and maintain information in a variety of databases, and then provide their customers with a single consolidated source for a broad array of personal information.

Financial Institutions Use Information Resellers for Eligibility Determinations, Fraud Prevention, PATRIOT Act Compliance, and Marketing:

Financial institutions in the banking, credit card, securities, and insurance industries use personal data purchased from information resellers primarily to help make eligibility determinations, comply with legal requirements, prevent fraud, and market their products.[Footnote 7] Credit reports from the three nationwide credit bureaus help lenders determine eligibility for and the cost of credit, and reports on insurance claims histories from specialty CRAs help insurance companies make premium decisions for new applicants and existing customers. To meet certain legal requirements and detect and prevent fraud, financial institutions we studied also use reseller products to locate individuals or confirm their identity. In addition, certain reseller products containing demographic data and information on individuals' lifestyle interests and hobbies are used to help market financial products to existing or potential customers with certain characteristics.

Consumer Reports Sold by Credit Bureaus and Other CRAs Are Used to Make Credit and Insurance Eligibility Decisions:

Banks, credit card companies, and other lenders rely on credit reports sold by the three nationwide credit bureaus--Equifax, Experian, and TransUnion--when deciding whether to offer credit to an individual, at what rate, and on what terms. Banks use credit reports to help assess the credit risk of new customers before opening a new deposit account or providing a mortgage or other loan. Credit card companies use credit reports to determine whether to grant a credit card to an applicant, determine the terms of that card, and to adjust the account terms of current cardholders whose creditworthiness may have changed. In addition to lenders, insurance companies often use scores generated from credit report information to help determine premiums for the policies they underwrite.

Credit bureaus receive the information in credit reports from the financial institutions themselves, among other sources. Credit reports consist of a "credit header"--identifying information such as name, current and previous addresses, Social Security number, and telephone number--and a credit history, or other payment history, designed to provide information on the individual's creditworthiness. The credit history might contain information on an individual's current and past credit accounts, including amounts borrowed and owed, credit limits, relevant dates, and payment histories, including any record of late payments. Credit reports also may include public record information on tax liens, bankruptcies, and other court judgments related to the payment of debts. Credit bureaus also sell credit scores, which are numerical representations of predicted creditworthiness based on information in credit reports, and are often used instead of full credit reports. For example, all three credit bureaus sell FICO® credit scores, which use factors such as payment history, amount owed, and length of credit history to help financial institutions predict the likelihood that a person will repay a loan.[Footnote 8]

Some financial institutions also use specialty CRAs, which maintain specific types of files on consumers, to help make eligibility decisions. Insurance companies commonly use products from ChoicePoint and ISO, which compile data from insurance companies on the claims that individuals have made against their homeowner's or automobile insurance policies.[Footnote 9] Most insurance companies provide these CRAs with claim and loss information about their customers, including names, driver's license information, type of loss, date of loss, and amount the insurance company paid to settle the claim. The CRAs aggregate this information from multiple insurance companies to create either full reports or risk scores designed to help assess the likelihood that an individual will file a claim. Insurance companies purchase reports, or in some cases scores, associated with individuals applying for insurance and the property being insured to help decide whether to provide coverage and at what rate. Insurance companies also use this information to help determine whether to extend coverage and set premiums for existing policy holders. (See app. II for a sample insurance claims history report.) Insurance industry representatives told us aggregated claims data provided by specialty CRAs are extremely useful in making coverage and rate determinations. They noted, for example, that past losses are the best indicator of future driving risk and thus are useful to firms that underwrite auto insurance.

Banks and credit unions frequently assess applicants of new checking and other deposit accounts using products offered by resellers such as ChexSystems, a specialty CRA that is a subsidiary of eFunds. ChexSystems compiles information from banks and credit unions on accounts that have been closed due to account misconduct such as overdrafts, insufficient funds activity, returned checks, bank fraud, and check forgery. The company also aggregates available driver's license information from state departments of motor vehicles, and receives information from check-printing companies on check order histories, which can help identify fraud. Banks we spoke with said that the name and identifying information of a customer seeking to open a new deposit account is typically run through the ChexSystems database. The reports provided back to the financial institution by ChexSystems typically include identifying information, as well as information useful in assessing an applicant's risk, such as the applicant's history of check orders and the source and details of any account misconduct. (See app. II for a sample deposit account history report.)

Financial Institutions Use Information Resellers to Comply with the PATRIOT Act, Prevent Fraud, Mitigate Risk, and Locate Individuals:

Financial institutions use data purchased from information resellers to comply with legal requirements; detect, prevent, and investigate fraud; identify risks associated with prospective clients; and locate debtors or shareholders.

Complying with PATRIOT Act Requirements:

Financial institutions we spoke with frequently use products provided by information resellers to comply with PATRIOT Act requirements.[Footnote 10] Congress intended these provisions to help prevent terrorists and other criminals from using the U.S. financial system to fund terrorism and launder money. The act requires financial institutions to develop procedures to assure the identity of new customers.[Footnote 11] Many resellers offer products that verify and validate a new customer's identity by comparing information the customer provided to the financial institution with information aggregated from public and private sources. Some financial institutions, particularly those that offer services by telephone, mail, or the Internet, often confirm customers' identities using these reseller products. Other companies may verify their customers' identity from a driver's license, passport, or other paper document, but use information resellers for additional verification.

Financial institutions must also screen their customers to ensure they are not on the Department of the Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons List. The list includes individuals and entities that financial institutions are generally prohibited from conducting transactions with because they have been identified as potential terrorists, money launderers, international narcotics traffickers, or other criminals. Many information resellers offer products to financial institutions that screen new customers against the OFAC list; often this screening is packaged with identity verification in a single product. (See app. II for a sample identity verification and OFAC screening report.) The OFAC list is a publicly available government document, but financial institutions told us they use resellers for their screening because it allows them to do so more quickly and helps distinguish between common names on the list that might result in false matches. Some financial institutions use resellers to screen new customers against the OFAC list, while others periodically screen all of their existing customers. Some companies told us they do most of their OFAC screening internally, but sometimes use a reseller to gather additional information confirming whether a potential match is indeed an individual that is on the OFAC list.

To verify a customer's identity or conduct an OFAC screening, a financial institution typically uses a Web-based portal to provide an information reseller with basic information about the individual being screened--such as the person's name, Social Security number, address, driver's license number, phone number, and date of birth. The reseller then checks the information against its own records, and typically provides a "pass" response if the information matches, or a "fail" response if, for example, the date of birth does not match the name. Resellers' screening products generally draw on credit header data purchased from the credit bureaus, along with publicly available data such as address and telephone records and drivers' license records from

state agencies. Customer verification databases also include information that may indicate suspicious activity, such as prison or campground addresses, disconnected telephone numbers, and Social Security numbers of deceased individuals.

Preventing and Detecting Fraud:

The financial institutions we reviewed use information reseller tools to assist their fraud prevention and detection efforts. For example, banks and credit card companies sometimes use information reseller products to authenticate the identity of existing customers who call to update or receive account information or to order a replacement credit card. Authentication products usually draw on information similar to that used for verification products, most commonly credit header data and public records. Some resellers offer products that also allow the financial institution to access the customers' credit history with their permission, which provides additional personal information that can be used to verify identity. For example, a customer might be asked the year an automobile loan was originated or the credit limit on a credit card.

Fraud departments of financial institutions in our review also use more detailed products from information resellers to investigate suspected identity theft or account fraud, such as the use of a stolen credit card number. (See app. II for a sample fraud investigation report.) In these cases, a company's fraud department often purchases from information resellers detailed background information on a suspect's current and prior residences, vehicles, relatives, aliases, criminal records (in certain states), and other information that can be useful in directing an investigation. Examples of the uses of fraud products offered by resellers include:

- * obtaining detailed personal information about people associated with potential fraud, or their relatives and associates;
- * detecting links between individuals who may be co-conspirators in fraud or misconduct;
- * identifying multiple insurance claims made by the same person;
- * identifying individuals who are associated with multiple addresses, telephone numbers, or vehicles in ways that indicate potential fraud;
- * obtaining contact information for key individuals, such as witnesses to car accidents identified in police reports; or:
- * identifying instances where insurance policy applicants have failed to disclose certain required information.

Reducing Risk and Locating Individuals:

Financial institutions also sometimes use reseller products to help identify potential reputational risk or other risks associated with new customers or business partners. For example, securities firms told us they screen individuals like prospective wealth management clients or merger partners to check for a criminal record, disciplinary action by securities regulators, negative news media coverage, and known affiliation with terrorism, drug trafficking, or organized crime.

Financial institutions we spoke with also often use information

resellers to locate individuals. For example, lenders use reseller products to find customers who have defaulted on debts, and some mutual fund companies use these products to locate lost shareholders. The information provided by products used for this purpose is derived largely from credit header data, telephone records, and public records data, and may include an individual's aliases, addresses, telephone numbers, Social Security number, motor vehicle records, as well as the names of neighbors and associates. For example, one financial institution told us its debt collectors use a ChoicePoint product called DEBTOR Discovery to get such information to help locate delinquent debtors.

Some Financial Institutions Use Information Resellers for Marketing:

Some information resellers offer certain products that help financial institutions market their financial products and services to new or existing customers with specific characteristics. Databases held by resellers offering marketing products include a variety of information on individuals and households, such as household size, number and ages of children, estimated household income, homeownership status, demographic data, and lifestyle interests and activities. These databases derive their information from public records as well as nonpublic sources such as self-reported marketing surveys, product warranty cards, and lists of magazine subscribers, which may be used to provide financial institutions and other companies with lists of consumers meeting certain criteria.[Footnote 12] For example, a bank marketing a college savings account might request the names and addresses of all households in certain ZIP codes that have children under the age of 18 and household incomes of \$100,000 or more. Financial institutions we studied also use certain reseller products to gather additional information on their existing customers to market additional products and services. For example, we spoke with an insurance company that used an information reseller to learn which of its existing customers owned boats, so those customers could be targeted for boat insurance. Similarly, one bank we spoke with used an information reseller to help market a sailing credit card to current customers who lived near bodies of water.

Many companies that solicit new credit card accounts and insurance policies use nationwide credit bureaus for "prescreening" to identify potential customers for the products they offer.[Footnote 13] A lender or insurance company establishes criteria, such as a minimum credit score, and then purchases from a credit bureau a list of people in the bureau's database who meet those criteria. In some cases, the financial institution already has a list of potential customers that it provides to the credit bureau to identify individuals on the list who meet the criteria. Financial institutions sometimes also use a second information reseller to help them obtain from a credit bureau a list that includes only consumers meeting specific demographic or lifestyle criteria. For example, in marketing a home equity line of credit, a lender may use a second information reseller to work with a credit bureau to identify creditworthy individuals that are also homeowners and live in certain geographic areas, to which the lender will then make a firm offer of credit. Financial institutions sometimes use data from information resellers for models--developed by either the institution or the reseller--that seek to predict consumers likely to be interested in a new product and unlikely to present a credit risk. For example, a firm we spoke with that was marketing credit cards to college students used reseller data to determine the characteristics of college students that indicate they will be successful credit card

borrowers.

Federal Privacy and Information Security Laws Apply to Many Information Reseller Products, Depending on Their Use and Source:

The Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) are the primary federal laws governing the privacy and security of personal data collected and shared by information resellers. FCRA limits resellers' use and distribution of personal data, and allows consumers to access the data held on them, but it only applies to information collected or used primarily to make eligibility determinations. Unless FCRA applies to a product and its database, resellers typically provide only limited opportunities for the consumer to access, correct, or restrict sharing of the personal data held on them. GLBA's privacy provisions restrict the sharing of nonpublic personal information collected by or acquired from financial institutions, including resellers covered by GLBA's definition of financial institution (GLBA financial institutions). Further, GLBA's safeguarding provision requires resellers that are GLBA financial institutions to safeguard this information.

Several Federal Privacy and Security Laws Apply to Personal Data Held by Information Resellers:

No single federal law governs the use or disclosure of all personal information by private sector companies. Similarly, there are no federal laws designed specifically to address all of the products sold and data maintained by information resellers.[Footnote 14] Instead, a variety of different laws govern the use, sharing, and protection of personal information that is maintained for specific purposes or by specific types of entities. The two primary federal laws that protect personal information maintained by private sector companies are FCRA and GLBA. FCRA protects the security and confidentiality of personal information that is collected or used to help make decisions about individuals' eligibility for, among other things, credit, insurance, or employment, while GLBA is designed to protect personal financial information that individuals provide to or that is maintained by financial institutions.

In addition to FCRA and GLBA, other federal laws that directly or indirectly address privacy and data security may also cover some information reseller products.[Footnote 15] The Driver's Privacy Protection Act of 1994 regulates the use and disclosure by state motor vehicle departments of personal information from motor vehicle records.[Footnote 16] Personal motor vehicle records may be purchased and sold only for certain purposes--such as insurance claims investigations and other anti-fraud activities--unless a state motor vehicle agency has received express consent from the individual indicating otherwise.[Footnote 17] In addition, the Federal Trade Commission Act (FTC Act), enacted in 1914 and amended on numerous occasions, gives FTC the authority to prohibit and act against unfair or deceptive acts or practices.[Footnote 18] The failure by a commercial entity, such as an information reseller, to reasonably protect personal information could be a violation of the FTC Act if the company's actions constitute an unfair or deceptive act or practice. Finally, some federal banking regulators have authority to oversee their institutions' third-party service providers to ensure the safety and soundness of financial institutions.[Footnote 19] For example, if a vendor such as an information reseller did not employ reasonable safeguards to maintain a bank's records, federal banking regulators

could examine the vendor to identify and remedy the risks.[Footnote 20]

FCRA Applies Only to Consumer Information Used to Determine Eligibility:

The Fair Credit Reporting Act (FCRA), enacted in 1970, protects the confidentiality and accuracy of personal information used to make certain types of decisions about consumers. Specifically, FCRA applies to companies that furnish, contribute to, or use "consumer reports"--reports containing information about an individual's personal and credit characteristics used to help determine eligibility for such things as credit, insurance, employment, licenses, and certain other benefits.[Footnote 21] Businesses that evaluate consumer information or assemble such reports for third parties are known as consumer reporting agencies, or CRAs. Consumer reports covered by FCRA comprise a significant portion of consumer data transactions in the United States. For example, according to an industry association that represents CRAs, the three nationwide credit bureaus sell over 2.5 billion credit reports each year on average. FCRA places certain restrictions and obligations on CRAs that issue these reports. For example, the law restricts the use of consumer reports to certain permissible purposes, such as approving credit, imposes certain disclosure requirements, and requires that CRAs take steps to ensure that information in these reports is not misused. It also provides consumers with certain rights in relation to their credit reports, such as the right to dispute the accuracy or completeness of items in the reports. Congress has amended FCRA a number of times, most recently with the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which sought to promote more-accurate credit reports and expand consumers' access to their credit information.[Footnote 22]

Information resellers are subject to FCRA's requirements only with regard to information used to compile consumer reports--that is, reports used to help determine eligibility for certain purposes, including credit, insurance, or employment. Thus, FCRA applies to databases used to compile credit reports sold by the three nationwide credit bureaus, and its provisions apply both to the credit bureaus themselves as well as to other information resellers that purchase and resell credit reports for use by others. FCRA also applies to databases used to generate specialty consumer reports--which consist of such things as tenant history, check writing history, employment history, medical information, or insurance claims--that are used to help make eligibility determinations. For example, according to ChoicePoint, FCRA applies to the data used in most of its Workplace Solutions products, which employers use to make hiring decisions. Similarly, according to LexisNexis, FCRA applies to its Electronic Bankruptcy Notifier product data, which financial institutions use to determine whether to offer customers credit or other financial services. Overall, 8 of the 10 information resellers we spoke with said that at least some of their products are consumer reports as defined by FCRA. They said their contracts prohibit their customers from using their non-FCRA products for purposes related to making eligibility determinations.

According to the information resellers included in our review, FCRA does not cover many databases used to create other products they offer because, as defined by the law, the information was not collected for making eligibility determinations and the products are not intended to be used for making eligibility determinations.[Footnote 23] For example, some of the information resellers we spoke with did not treat data in some products used to identify and prevent fraud as subject to

FCRA. Similarly, resellers do not typically consider databases used solely for marketing purposes to be covered by FCRA. Because the definition of a consumer report under FCRA depends on the purpose for which the information is collected and on the reports' intended and actual use, an information reseller apparently may have two essentially identical databases with only one of them subject to FCRA.

FCRA also restricts financial institutions and other companies that use consumer reports from using them for purposes other than those permitted in the law. Financial institutions must also notify consumers if they take an adverse action--such as denying an applicant a credit card--based on information in a consumer report. Under FCRA, companies that furnish information to CRAs also must take steps to ensure the accuracy of information they report. Further, users of consumer reports must properly dispose of consumer reports they maintain. The law also limits financial institutions and other entities from sharing certain credit information with their affiliates for marketing purposes. Final regulations to implement this statutory limitation have not yet been promulgated.

FCRA Provides Access, Correction, and Opt-Out Rights for Consumer Reports:

FCRA is the primary federal law that provides rights to consumers to view, correct, or opt out of the sharing of their personal information, including data held by information resellers. Under FCRA, as recently amended by the FACT Act, consumers have the right to:

- * obtain all of the information about themselves contained in the files of a CRA upon request, including their credit history;
- * receive one free copy of their credit file from nationwide CRAs and nationwide specialty CRAs once a year or under certain other circumstances;[Footnote 24]
- * dispute information that is incomplete or inaccurate, and have their claims investigated and any errors deleted or corrected, as provided by the law; and:
- * opt out of allowing CRAs to provide their personal information to third parties for prescreened marketing offers.[Footnote 25]

Most of FCRA's access, correction, and opt-out rights apply not just to the three nationwide credit bureaus--Experian, TransUnion, and Equifax--but also to other CRAs, including nationwide specialty CRAs that provide reports on such things as insurance claims and tenant histories. The law imposes slightly different requirements on these entities with respect to free annual reports. For example, FCRA's implementing regulation requires Experian, TransUnion, and Equifax to create a centralized source for accepting consumer requests for free credit reports, which must include a single dedicated Web site, a toll-free telephone number, and mail directed to a single postal address where consumers can order credit reports from all three nationwide CRAs.[Footnote 26] Nationwide specialty CRAs are individually required to maintain a toll-free number and a streamlined process for accepting and processing consumer requests for file disclosures.[Footnote 27] Other CRAs must provide consumers with a copy of their report upon request (although in most cases they may charge a reasonable fee for it), and they must allow consumers to dispute information they believe to be inaccurate. In practice, consumers may find it difficult in some

cases to effectively access and correct information held by nationwide specialty CRAs because there may be hundreds of such CRAs and no master list exists. For example, job seekers who want to confirm the accuracy of information about themselves in background-screening products would need to request their consumer reports from the dozens of such companies that offer such products.

Consumers generally do not have the legal right to access or correct information about them contained in non-FCRA databases, such as those used for marketing purposes or, in some cases, fraud detection. The information resellers we studied varied in the extent to which they voluntarily provide consumers with additional opportunities to view, correct, and opt out of the sharing of information beyond what the law requires. The three nationwide credit bureaus allowed consumers to view only information that is subject to FCRA. However, three other information resellers we spoke with allowed consumers to order summary reports of some data maintained about them that was not subject to FCRA. These reports varied in length and detail but typically contained consumer data obtained from public records, publicly available information, and credit header information. Consumers did not typically have the right to see data maintained about them related to marketing, such as information on their household income, interests, or hobbies, which was often obtained from warranty cards or self-reported survey questionnaires.

Information resellers told us that consumers who request correction of inaccurate data not covered by FCRA are typically referred to the government or private entity that was the source of the data. Many resellers told us that because their databases are so frequently updated, simply correcting their own databases would not be effective because it would soon be refreshed by new erroneous data from the original source. However, one reseller told us it has procedures that prevent such corrections from being overwritten. Some resellers offered limited opportunities for consumers to opt out of their databases even for data not covered by FCRA, but they typically allow this only for data used for marketing purposes. The five resellers we spoke with that maintain personal data used for marketing allowed consumers to request that their information not be shared with third parties. None of the resellers we spoke with offered all consumers the ability to opt out of identity verification or fraud products. They noted that it would undermine the effectiveness of the databases if, for example, criminals could remove themselves from lists of fraudsters. Some resellers do allow opt-out opportunities to certain individuals, such as judges or identity-theft victims, who may face potential harm from having their information included in reseller databases.

Industry representatives, consumer advocates, and others offer differing views on whether the access, correction, and opt-out rights provided under FCRA should be expanded. Many consumer advocates and others have argued that these rights should not be limited to consumer information used for eligibility purposes, but should explicitly extend as well to databases not currently considered by resellers to be subject to FCRA, such as those used for some anti-fraud products. Proponents of this view argue that basic privacy principles dictate that consumers should have the right to know what information is being collected and maintained about them. In addition, they argue that errors in these databases have the potential to harm consumers. For example, an individual could be denied a volunteer opportunity or falsely pursued as a crime suspect due to erroneous information in a reseller database not covered under FCRA.

In contrast, some information resellers, financial services firms, and law enforcement representatives have argued that providing individuals expanded access, correction, and opt-out rights is unnecessary and could harm fraud prevention and criminal investigations by providing individuals with the opportunity to see and manipulate the information that exists about them. They also note that expanding these rights could create new regulatory burdens. For example, firms maintaining databases for marketing purposes could face substantial costs and complications developing and implementing processes for consumers to see, challenge, and correct the data held on them. Information resellers noted that providing access and correction rights for personal information in marketing databases makes little sense because the accuracy of this information is much less important than for information used to make crucial eligibility decisions.

GLBA Applies to Information Resellers That Are Financial Institutions or Receive Information from Financial Institutions:

The Gramm-Leach-Bliley Act (GLBA), enacted in 1999, limits with certain exceptions the sharing of consumer information by financial institutions and requires them to protect the security and confidentiality of customer information. Further, GLBA limits the reuse and redisclosure of the information for those receiving it. GLBA's key provisions with regard to information resellers, therefore, cover the privacy, reuse, redisclosure, and safeguarding of information.

GLBA Privacy Provisions:

GLBA's privacy provisions generally limit financial institutions from sharing nonpublic personal information with nonaffiliated companies without first providing certain notice and, where appropriate, opt-out rights to their own customers and other consumers with whom they interact.[Footnote 28] GLBA distinguishes between a financial institution's "customers" and other individuals the financial institution may interact less with, which the law refers to as "consumers." Specifically, a consumer is an individual who obtains a financial product or service from a financial institution.[Footnote 29] On the other hand, a customer is a consumer who has an ongoing relationship with a financial institution. For example, someone who engages in an isolated transaction with a financial institution, such as obtaining an ATM withdrawal, is a consumer, whereas someone who has a deposit account with a bank would be a customer. While some GLBA requirements, such as the privacy requirements, apply broadly to cover consumer information in many cases, other provisions of GLBA apply only to customer information. For example, GLBA's safeguarding requirements oblige financial institutions to protect only customer information.

GLBA requires financial institutions to provide their customers with a notice at the start of the customer relationship and annually thereafter for the duration of that relationship. The notice must describe the company's sharing practices and give customers, and in some cases consumers, the right to opt out of some sharing. GLBA exempts companies from notice and opt-out requirements under certain circumstances. For example, financial institutions and CRAs may share personal information for credit-reporting purposes without providing opt-out opportunities, and financial institutions and others may also share this information to protect against or prevent actual or potential fraud and unauthorized transactions.[Footnote 30] Thus, financial institutions are not required to provide their customers with

opt-out rights before reporting their information to credit bureaus or sharing their information with information resellers for identity verification and fraud purposes. Under another GLBA exception, financial institutions are also not required to provide consumers with an opportunity to opt out of the sharing of information with companies that perform services for the financial institution.[Footnote 31]

GLBA's privacy provisions apply to information resellers only if (1) the reseller is a GLBA "financial institution" or (2) the reseller receives nonpublic personal information from such a financial institution (see fig. 2). The determination of whether a company is a financial institution under GLBA is complex and, for an information reseller, depends on whether the company's activities are included in implementing regulations issued by FTC. GLBA defines "financial institutions" as entities that are in the business of engaging in certain financial activities.[Footnote 32] Such activities include, among other things, traditional banking services, activities that are financial in nature on the FRB list of permissible activities for financial holding companies in effect as of the date of GLBA's enactment, and new permissible activities.[Footnote 33] While new financial activities may be identified, those activities are not automatically included in FTC's definition.[Footnote 34] FTC defines "financial institutions" as businesses that are "significantly engaged" in financial activities.[Footnote 35] For example, FRB's list of "financial activities" includes not only the activity of extending credit, but also related activities such as credit bureau services.[Footnote 36] Thus, the three nationwide credit bureaus are considered financial institutions subject to GLBA.[Footnote 37]

Figure 2: GLBA Privacy Provisions:

[See PDF for image]

Source: GAO(analysis), Art Explosion(image).

[End of figure]

FTC staff told us that the determination of whether a specific information reseller is a financial institution subject to GLBA depends on the specific activities of the company. They said they determine whether GLBA applies to an entity on a case-by-case basis and that it is difficult to generalize what types of information resellers are GLBA financial institutions. For example, CRAs other than the three nationwide credit bureaus may not necessarily be subject to GLBA if, for example, their activities do not fall under FRB's definition of credit bureau services or they do not otherwise engage in any financial activity included in the 1999 FRB list. Only four resellers with whom we spoke--the three nationwide credit bureaus and a specialty CRA that collects deposit account information--told us they consider themselves financial institutions subject to GLBA's privacy and safeguarding provisions. Moreover, we were told that these provisions do not apply to the entire company but rather only to those activities of the company that are deemed financial in nature. For example, one credit bureau told us that its credit reporting activities fall under GLBA, but that its marketing products, which are not deemed financial in nature, do not fall under GLBA.[Footnote 38]

GLBA not only limits how financial institutions share nonpublic personal information with other companies, but it also restricts what those companies subsequently do with the information. Under GLBA's

"reuse and redisclosure" provision and FTC's implementing rule, companies that receive information from a financial institution are restricted in how they further share or use that information.[Footnote 39] If a company receives information under a GLBA exception, then the reseller can only reuse and redisclose the information for activities that fall under the exception under which the information was received.[Footnote 40] Alternatively, if a company receives information from a financial institution in a way not covered by an exception--where an individual has been provided with a GLBA notice and has chosen not to opt out of sharing--then the information may be reused and redisclosed in any way the original financial institution would have been permitted.[Footnote 41]

As noted earlier, the nationwide credit bureaus sell credit header data--identifying information at the top of a credit report--to other information resellers for use in fraud prevention products. Representatives of two of the credit bureaus and their industry association told us that because credit header data contains information from financial institutions, it is subject to GLBA's reuse and redisclosure provisions. As a result, the credit bureaus can only sell credit header data under the same GLBA exception under which they received it. Credit bureau representatives said they receive the information from financial institutions under both the consumer reporting and fraud prevention exceptions, and then sell it under the fraud prevention exception.

Also, some old credit header data may not be subject to GLBA at all. Prior to GLBA's enactment in 1999, credit header information sold by credit bureaus--which included names, addresses, aliases, and Social Security numbers--could be used or resold by a third party for any purpose, as long as the information was not used to make eligibility determinations. GLBA placed restrictions on the sale of such nonpublic personal information maintained by GLBA financial institutions. Further, as noted earlier, reuse and redisclosure of the information is also restricted by GLBA. The law's privacy restrictions generally became fully effective on July 1, 2001.[Footnote 42] A nationwide credit bureau told us that the restrictions did not apply retroactively to credit header data that credit bureaus already held at the time of GLBA's enactment in 1999. The nationwide credit bureau said that just prior to GLBA's enactment, it created a new database containing "pre-GLBA" credit header data and transferred those data to a separate affiliated company.[Footnote 43] The company told us that because it gathered these data prior to GLBA's enactment, the data are not subject to GLBA's privacy and safeguarding provisions.

GLBA Safeguarding Provisions:

The safeguarding provisions of GLBA require financial institutions to take steps to ensure the security and confidentiality of their customers' nonpublic personal information.[Footnote 44] Specifically, the agency regulations provide that financial institutions must develop comprehensive written policies and procedures to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.[Footnote 45] Although the privacy provisions of GLBA apply broadly to financial institutions' consumers, GLBA's safeguarding requirements only establish obligations on financial institutions to protect their customer information.

Only information resellers defined as financial institutions under the law are required to implement these safeguards. Several of the information resellers we spoke with noted that although GLBA does not apply to all of their products, they have policies and procedures to protect all of their information in a way consistent with GLBA's safeguarding requirements. Unlike GLBA's notice and opt-out requirements (privacy requirements), the law's safeguarding provisions do not directly extend to third-party companies that receive personal information from financial institutions. However, federal agencies' provisions implementing GLBA safeguarding rules require financial institutions to monitor the activities of their service providers and require them by contract to implement and maintain appropriate safeguards for customer information.[Footnote 46]

Many commercial entities--including many information resellers--are not subject to GLBA and therefore are not explicitly required by a federal statute to have in place policies and procedures to safeguard individuals' personal data. This raises concerns given that identity theft has emerged as a serious problem and that breaches of sensitive personal data have occurred at a variety of companies that are not financial institutions. For example, in 2005, BJ's Wholesale Club, which is not considered a GLBA financial institution, settled FTC charges that it engaged in an unfair or deceptive act or practice in violation of the FTC Act by failing to take appropriate security measures to protect the sensitive information of thousands of its customers.[Footnote 47] FTC alleged that the company's failure to secure sensitive information was an unfair practice because it caused substantial injury not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. Some policymakers, consumer advocates, and industry representatives have advocated explicit statutory requirements that would expand more broadly the number and types of companies that must safeguard their data. Had there been a statutory requirement for BJ's Wholesale Club to safeguard sensitive information, FTC would have had authority to file a complaint based on the company's failure to safeguard information. Expanding the class of entities subject to safeguarding laws would impose explicit data security provisions on a larger group of organizations that are maintaining sensitive personal information. FTC has testified that should Congress enact new data security requirements, FTC's safeguards rule should serve as a model for an effective enforcement standard because it provides sufficient flexibility to apply to a wide range of companies rather than mandate specific technical requirements that may not be appropriate for all entities.[Footnote 48] To be most effective, new data security provisions would need to apply both to customer and noncustomer data because the nature of information reseller businesses is such that they hold large amounts of sensitive personal information on individuals who are not their customers.

No Federal Statute Requires Notification of Data Breaches:

Currently, there is no federal statute requiring information resellers or most other companies to disclose breaches of sensitive personal information, although at least 32 states have enacted some form of breach notification law.[Footnote 49] Policymakers and consumer advocates have raised concerns that federal law does not always require companies to reveal instances of the theft or loss of sensitive data. These concerns have been triggered in part by increased public awareness of the problem of identity theft and by a large number of

data breaches at a wide variety of public and private sector entities, including major financial services firms, information resellers, universities, and government agencies. In 2005, ChoicePoint acknowledged that the personal records it held on approximately 162,000 consumers had been compromised. As part of a settlement with the company in January 2006, FTC alleged that ChoicePoint did not have reasonable procedures to screen prospective subscribers to its data products, and provided consumers' sensitive personal information to subscribers whose applications should have raised obvious suspicions.[Footnote 50] A December 2005 report by the Congressional Research Service noted that personal data security breaches were occurring with increasing regularity, and listed 97 recent breaches, five of which had occurred at information resellers.[Footnote 51] Data breaches are not limited to private sector entities, as evidenced by the theft discovered in May 2006 of electronic data of the Department of Veterans Affairs containing identifying information for millions of veterans.

Congress has held several hearings related to data breaches, and a number of bills have been introduced that would require companies to notify individuals when such breaches occur.[Footnote 52] The bills vary in many ways, including differences in who must be notified, the level of risk that triggers a notice, the nature of the notification, exceptions to the requirement, and the extent to which federal law preempts state law. Breach notification requirements have two primary benefits. First, they provide companies or other entities with incentives to follow good security practices so as to avoid the legal liability or public relations risks that may result from a publicized breach of customer data. Second, consumers who are informed of a breach of their personal data can take actions to mitigate potential risk, such as reviewing the accuracy of their credit reports or credit card statements. However, FTC and others have noted that any federal requirements should ensure that customers receive notices only when they are at risk of identity theft or other related harm. To require notices when consumers are not at true risk could create an undue burden on businesses that may be required to provide notices for minor and insignificant breaches. It could also overwhelm consumers with frequent notifications about breaches that have no impact on them, reducing the chance they will pay attention when a meaningful breach occurs. At the same time, consumer and privacy groups and other parties have warned against imposing too weak of a trigger for notification, and expressed concerns that a federal breach notification law could actually weaken consumers' security if it were to preempt stronger state laws.[Footnote 53]

FTC Has Primary Responsibility for Enforcing Information Resellers' Compliance with Privacy and Information Security Laws:

The Federal Trade Commission is the federal agency with primary responsibility for enforcing applicable privacy and information security laws for information resellers. Since 1972, FTC has initiated numerous formal enforcement actions against information resellers for providing consumer report information without adequately ensuring that their customers had a permissible purpose for obtaining the data. FTC has civil penalty authority for violations of FCRA and, in limited situations, the FTC Act, but it does not have such authority for GLBA, which may inhibit its ability to most effectively enforce that law's privacy and security provisions.

FTC Has Primary Federal Enforcement Authority over Information

Resellers:

FTC enforces the privacy and security provisions of FCRA and GLBA over information resellers. FCRA provided FTC with enforcement authority for nearly all companies not supervised by a federal banking regulator.[Footnote 54] Similarly, GLBA provided FTC with rule-making and enforcement authority over all financial institutions and other entities not under the jurisdiction of the federal banking regulators, NCUA, SEC, the Commodity Futures Trading Commission, or state insurance regulators.[Footnote 55] In addition, the FTC Act provides FTC with the authority to investigate and take administrative and civil enforcement actions against most commercial entities, including information resellers, that engage in unfair or deceptive acts or practices in or affecting commerce. According to FTC officials, an information reseller could violate the FTC Act if it mishandled personal information in a way that rose to the level of an unfair or deceptive act or practice.

State regulators also play a role in enforcing data privacy and security laws. FCRA provides enforcement authority to a state's chief law enforcement officer, or any other designated officer or agency, although federal agencies have the right to intervene in any state-initiated action.[Footnote 56] In addition, GLBA allows states to enforce their own information security and privacy laws, including those that provide greater protections than GLBA, as long as the state laws are not inconsistent with requirements under the federal law. Several states, including Connecticut, North Dakota, and Vermont, have enacted restrictions on the sharing of financial information that are stricter than GLBA.[Footnote 57] States can also enforce their own laws related to unfair or deceptive acts or practices to the extent the laws do not conflict with federal law.

FTC Has Investigated and Initiated Formal Enforcement Actions against Information Resellers for FCRA and FTC Act Violations:

Since 1972, FTC has initiated numerous formal enforcement actions against at least 20 information resellers for violating FCRA and, in some cases, the FTC Act.[Footnote 58] All of these companies were CRAs, and they included the three nationwide credit bureaus as well as a variety of types of specialty CRAs.[Footnote 59] In most of these cases, FTC charged that the companies provided consumer report information without adequately ensuring that their customers had a permissible purpose for obtaining the data. In many cases, FTC alleged the companies sold consumer reports to users they had no reason to believe intended to use the information legally, or didn't require the users to identify themselves and certify in writing the purposes for which they wished to use the reports. In addition, some companies' reports allegedly included significant inaccuracies or obsolete information; some companies also failed to reinvestigate disputed information within a reasonable period of time.[Footnote 60]

Among the most significant of these FTC enforcement actions against information resellers are the following:

* In 1995, FTC settled charges with Equifax Credit Information Services, the credit bureau subsidiary of Equifax Inc., for alleged violations of FCRA. FTC alleged that the company furnished consumer reports to individuals without a permissible purpose, included derogatory information in consumer reports that should have been excluded after it was disputed by the consumer, and failed to take steps to reduce inaccuracies in reports and reinvestigate disputed

information. The consent agreement required Equifax to take steps to improve the accuracy of its consumer reports and limit the furnishing of such reports to those with a permissible purpose under FCRA.[Footnote 61]

* In 2000, FTC ordered the TransUnion Corporation, a nationwide credit bureau, to stop selling consumer reports in the form of target marketing lists to marketers who lack an authorized purpose under FCRA for receiving them. The company had been selling mailing lists of the names and addresses of consumers meeting certain credit-related criteria (such as having certain types of loans). FTC found that the lists were consumer reports and that the lists therefore could not be sold for target marketing purposes.[Footnote 62]

* In January 2006, FTC settled charges against ChoicePoint that its security and record-handling procedures violated federal laws with respect to consumers' privacy. FTC had alleged the company violated FCRA by providing sensitive personal information to customers despite obvious indications that the information would not be used for a permissible purpose. For example, ChoicePoint allegedly approved as customers individuals who subscribed to data products for multiple businesses using fax machines in public commercial locations. FTC also charged that the company violated the FTC Act by making false and misleading statements in its privacy policy, which said it provided consumer reports only to businesses that complete a rigorous credentialing process. Under the terms of the settlement, ChoicePoint agreed to pay \$10 million in civil penalties--the largest civil penalty in FTC history--and to provide \$5 million in consumer redress.[Footnote 63] ChoicePoint did not admit to a violation of law in settling the charges. A company representative told us it has taken steps since the breach to enhance its customer screening process and to assist affected consumers.

FTC Cannot Levy Civil Penalties for GLBA Information Privacy and Security Violations:

FTC is the primary federal agency monitoring information resellers' compliance with privacy and security laws, but it is a law enforcement rather than supervisory agency. Unlike federal financial institution regulators, which oversee a relatively narrow class of entities, FTC has jurisdiction over a large and diverse group of entities and enforces a wide variety of statutes related to antitrust, financial regulation, consumer protection, and other issues. FTC's mission and resource allocations focus on conducting investigations and, unlike federal financial regulators, FTC does not routinely monitor or examine the companies over which it has jurisdiction.

If FTC has reason to believe that violations of laws under its jurisdiction have taken place, it may initiate a law enforcement action. Under its statutory authority, it can ask or compel companies to produce documents, testimony, and other materials. FTC may in administrative proceedings issue cease and desist orders for unfair or deceptive acts or practices. Further, FTC generally may seek from the United States district courts a wide range of remedies, including injunctions, damages to compensate consumers for their actual losses, and disgorgement of ill-gotten funds.[Footnote 64] Depending on the law it is enforcing, FTC may also seek to obtain civil penalties--monetary fines levied for a violation of a civil statute or regulation.

Although FTC has civil penalty authority for violations of FCRA and in

limited situations the FTC Act, GLBA's privacy and safeguarding provisions do not give it such authority.[Footnote 65] Currently, FTC may seek an injunction to stop a company from violating these provisions and may seek redress--damages to compensate consumers for losses--or disgorgement. However, determining the appropriate amount of consumer compensation requires having information on who and how many consumers were affected and the harm, in monetary terms, that they suffered. This can be extremely difficult in the case of security and privacy violations, such as data breaches. Such breaches may lead to identity theft, but FTC staff told us that they may not be able to identify exactly which individuals were victimized and to what extent they were harmed--particularly in cases where the potential identity theft could occur years in the future. FTC could benefit from having the authority to impose civil penalties for violations of GLBA's privacy and safeguarding provisions because such penalties may be more practical enforcement tools for violations involving breaches of mass consumer data. FTC has testified that such authority is often the most appropriate remedy in such cases, and staff told us it could more effectively deter companies from violating provisions of GLBA. Unlike FTC, other regulators have civil penalty authority to enforce violations of GLBA. For example, OCC told us it can enforce GLBA privacy and safeguard provisions with civil money penalties against any insured depository institution or institution-affiliated party.[Footnote 66]

Agencies Differ in Their Oversight of the Privacy and Security of Personal Information at Financial Institutions:

In enforcing privacy and security requirements, federal regulators do not distinguish between the data that regulated entities obtain from information resellers and other personal information these entities maintain. Federal banking regulators have overseen compliance with the privacy and security provisions of GLBA and FCRA by issuing rules and guidance, conducting examinations, and taking formal and informal enforcement actions when needed. Securities and insurance regulators enforce GLBA information privacy and security requirements in a similar fashion, but FTC is responsible for FCRA enforcement among these firms. FTC is also responsible for GLBA and FCRA enforcement for financial services firms not supervised by another regulator and has initiated several enforcement actions, though it does not conduct routine examinations. Credit union, securities, and insurance regulators told us that unlike most of the banking regulators, they do not have full authority to examine their entities' third-party service providers, including information resellers.

Financial Institutions and Their Regulators Said They Do Not Distinguish between Data from Information Resellers and Other Sources:

The information privacy and security provisions of GLBA and FCRA provide several federal and state agencies with authority to enforce the laws' provisions for financial institutions. As shown in figure 3, GLBA assigns federal banking and securities regulators and state insurance regulators with enforcement responsibility for the financial institutions they oversee, and FTC has jurisdiction for all other financial institutions. FCRA similarly assigns the federal banking regulators authority over the institutions they oversee and FTC with jurisdiction over other entities.[Footnote 67] FCRA assigns FTC with enforcement responsibility for securities and insurance companies and provides securities and insurance regulators with no statutory responsibilities to enforce FCRA.[Footnote 68]

Figure 3: Enforcement Responsibilities for Selected Financial Institutions under FCRA and GLBA:

[See PDF for image]

Source: GAO.

Notes: The Commodity Futures Trading Commission, which was not identified as a functional regulator by GLBA, is nevertheless responsible for enforcing information privacy and security requirements among futures commission merchants, commodity trading advisers, commodity pool operators, and introducing brokers subject to its jurisdiction. See 7 U.S.C. § 7b-2.

[A] NCUA enforces GLBA at all federally insured credit unions and FCRA at all federally chartered credit unions. FTC has enforcement authority for all other credit unions not subject to NCUA's jurisdiction.

[B] SEC is responsible for enforcing GLBA compliance for investment advisers registered with SEC; FTC is responsible for enforcement at all other investment advisers.

[C] FTC is responsible for enforcing FCRA at securities firms and insurance companies, but it is not a supervisory agency and does not conduct routine examinations.

[End of figure]

Financial regulators told us that in their oversight of companies' compliance with privacy laws, they generally do not distinguish between data obtained from information resellers versus other sources. The nonpublic personal information maintained by financial institutions includes both data they collect directly from their customers as well as data purchased from information resellers, such as credit reports or marketing lists. Banking and securities regulators told us their efforts to oversee the privacy and security of nonpublic personal information do not focus in particular on data that came from information resellers but rather look holistically at a financial institution's information security and compliance with applicable laws. For example, OCC and FRB officials said their examiners enforce the privacy and safeguarding requirements of GLBA and FCRA regardless of whether the source of the data is an information reseller, a customer, or other source.

GLBA's safeguarding requirements apply only to nonpublic personal information that financial institutions maintain on their customers and not to information they maintain about other consumers (noncustomers). However, representatives of financial institutions we interviewed said that as a matter of policy, they generally apply the same information safeguards to both customer and consumer information. They said that their information safeguards focus on the sensitivity of the information rather than whether the person is a customer. For example, files containing Social Security numbers would have more stringent safeguards than those containing only names and addresses. Officials of a global investment banking and brokerage firm told us that although their firm maintains separate databases on customers and consumers targeted for marketing, both databases use the higher security standard required for customer information. Another company with similar practices noted that it treats all information with higher standards

rather than setting up many different safeguarding policies and procedures. Other companies noted that public relations and reputational risk concerns motivate them to maintain high safeguards to prevent any consumer information from being lost or stolen. Similarly, federal banking regulators told us that failing to safeguard consumer information may not be a violation of GLBA but is still taken very seriously because it represents a threat to a bank's safety and soundness, poses reputational risks, and reflects a weakness in a bank's corporate governance.

Federal Banking Agencies Provide Guidance and Examine Regulated Banking Organizations for GLBA and FCRA Compliance:

The banking regulators responsible for GLBA and FCRA enforcement have issued regulations and other guidance on information privacy and security requirements. The individual banking regulators examine the financial institutions under their jurisdiction for compliance with GLBA and FCRA information privacy and safeguarding requirements and have taken enforcement actions for violations.

Regulations and Other Guidance:

The banking agencies acting jointly and individually, and in coordination with FTC, have issued regulations and other guidance for financial institutions to follow in implementing the privacy and safeguarding requirements of GLBA.[Footnote 69] In 2000, following the law's passage, the banking agencies--OCC, FRB, OTS, FDIC, and NCUA--issued rules for compliance with the law's information privacy requirements.[Footnote 70] These rules helped financial institutions implement GLBA's notice and opt-out requirements. For example, they provided examples of types of information regulated by GLBA. In 2001, the agencies jointly issued guidelines establishing standards for GLBA's safeguarding requirements to assist financial institutions in establishing administrative, technical, and physical safeguards for customer information as required by law.[Footnote 71] In addition to the guidelines that implement GLBA safeguarding requirements, these regulators have in some cases issued guidance to provide further assistance to their institutions. For example, the banking agencies issued a guide on small entities' compliance with GLBA's privacy provision to help companies identify and comply with the requirements. The banking agencies also have issued additional written interagency guidance for financial institutions relating to notification of their customers in the event of unauthorized access to their information where misuse of the information has occurred or is reasonably possible.[Footnote 72]

The banking regulators have also issued rules and regulations for their institutions to implement certain provisions of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which amends FCRA.[Footnote 73] For example, in 2004, in coordination with FTC, these agencies issued a final rule to implement the FACT Act requirement that persons, including financial institutions, properly dispose of consumer report information and records.[Footnote 74] Some provisions--such as restrictions on how financial institutions can share data with their affiliates for marketing purposes--have yet to be finalized by the banking or other agencies.

Through the Federal Financial Institutions Examination Council (FFIEC)--a formal interagency body comprising representatives from OCC, OTS, FRB, FDIC, and NCUA that coordinates examination standards and

procedures for their institutions--the banking agencies have also issued guidance to help bank examiners oversee the integrity of information technology at their institutions. For example, FFIEC developed the FFIEC IT Examination Handbook, which is composed of 12 booklets designed to help examiners and organizations determine the level of security risks at financial institutions and evaluate the adequacy of the organizations' risk management. Representatives of banking regulators say their examiners rely on these booklets in addition to the GLBA and FCRA guidance when examining the integrity of an institution's information privacy and security procedures. Some of these booklets help examiners oversee financial institutions' use of information resellers and other third-party technology service providers by addressing topics such as banks' outsourcing of technology services, or banks' supervision of its technology service providers. Financial institution regulators told us their examiners use these booklets to oversee the soundness of their institutions' technology services and to address information security issues posed by third-party technology service providers such as information resellers.

Examinations and Enforcement Actions:

Banking regulators regularly examine regulated banks, thrifts, and credit unions for compliance with GLBA and FCRA requirements.[Footnote 75] Each regulatory agency told us that their agencies' safety and soundness, compliance, and information technology examinations include checks on whether their institutions are in compliance with GLBA's and FCRA's provisions related to the privacy and security of personal information. For example, OCC examination procedures tell examiners to review banks' monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems. However, the scope of the regulators' reviews with regard to privacy and security matters can vary depending on the degree of risk associated with the institution examined.

According to the banking agencies, their examinations of institutions' GLBA and FCRA compliance have discovered limited material deficiencies and violations requiring formal enforcement actions. Instead, they have mostly found various weaknesses that they characterized as technical in nature and required informal corrective action.[Footnote 76] FDIC officials said that between 2002 and 2005, the agency took 12 formal enforcement actions for GLBA violations and no formal enforcement actions under FCRA. They noted that FDIC has also taken informal enforcement actions to correct an institution's overall compliance management system, which covers all of the consumer protection statutes and regulations in the examination scope.

According to OCC officials, between October 1, 2000, and September 30, 2005, the agency took 18 formal enforcement actions under GLBA and no formal enforcement actions under FCRA. OCC's actions in these cases resulted in outcomes such as cease and desist orders and civil money penalties levied against violators. The agency also informally required banks to take corrective action in several instances, such as requiring a bank to notify customers whose accounts may have been compromised, or requiring a bank to correct and reissue its initial privacy notice. According to OCC staff, OCC's examinations for compliance with GLBA's privacy requirements most commonly found that banks' initial privacy notices were not clear and conspicuous, and its examinations for compliance with GLBA's safeguarding requirements most commonly found cases of inadequate customer information programs, risk assessment processes, testing, and reports to the board.

FRB officials said the agency has taken 12 formal enforcement actions in the past 5 years for violations of GLBA's information-safeguarding standards and no formal actions for FCRA violations. They said FRB has taken several informal enforcement actions, including three related to violations of Regulation P, which implements GLBA's privacy requirements, and five informal actions for violations of FCRA. According to FRB staff, FRB's examinations for compliance with the interagency information security standards have found cases of inadequate customer information security programs, board oversight, and risk assessments, as well as cases of incomplete assessment of physical access controls and safeguarding of the transmission of customer data. The most commonly found problem in FRB's examinations for compliance with Regulation P was banks' failure to provide clear and conspicuous initial notices of their privacy policies and procedures. With regard to FCRA compliance, the violations cited most frequently were the failure to provide notices of adverse actions based on information contained in consumer reports or obtained from third parties.

Securities Regulators Oversee GLBA Compliance of Securities Firms:

SEC, NASD, and NYSE Regulation oversee securities industry participants' compliance with GLBA's privacy and information safeguarding requirements. Similar to the banking agencies, they have issued rules and other guidance, conducted examinations of firms' compliance with federal securities laws and regulations, and, if appropriate, taken enforcement actions.

Regulations and Other Guidance:

In June 2000, SEC adopted Regulation S-P, which implements GLBA's Title V information privacy and safeguarding requirements among the broker-dealers, investment companies, and SEC-registered investment advisers subject to SEC's jurisdiction.[Footnote 77] Regulation S-P contains rules of general applicability that are substantively similar to the rules adopted by the banking agencies. In addition to providing general guidance, Regulation S-P contains numerous examples specific to the securities industry to provide more meaningful guidance to help firms implement its requirements. For example, the rule provides detailed guidance on the provision covering privacy and opt-out notices when a customer opens a brokerage account. It also contains a section regarding procedures to safeguard information, including the disposal of consumer report information.[Footnote 78]

Since Regulation S-P was adopted, SEC staff have issued additional written guidance in the form of Staff Responses to Questions about Regulation S-P. According to SEC staff, companies also receive feedback on Regulation S-P compliance during the examination process, as well as during telephone inquiries made to SEC offices. However, unlike the federal banking agencies, SEC has issued no additional written guidance on institutions notifying customers in the event of unauthorized access to customer information. SEC staff said they are considering possible measures that would address information security programs in more detail, including the issue of how to respond to security breaches.

Examinations and Enforcement Actions:

SEC has examined registered firms for Regulation S-P compliance. SEC staff said compliance with Regulation S-P was a focus area in SEC examinations during the first 1 to 1½ years after July 2001, when it

became effective. During this period, Regulation S-P compliance was reviewed in 858 broker-dealer examinations, of which 105 resulted in findings.[Footnote 79] Also, during this period, Regulation S-P compliance was reviewed in 1,174 investment adviser examinations, of which 128 resulted in findings, and 218 investment company examinations, of which 17 resulted in findings.

SEC staff said that more recently SEC has adopted a risk-based approach to determine the depth of a review of compliance with Regulation S-P. Under this approach, an initial review of compliance with Regulation S-P is done to determine if a closer look is warranted. During the past 2½ years, compliance with Regulation S-P was reviewed in 1,891 investment adviser examinations, of which 301 resulted in findings, and 257 investment company examinations, of which 20 resulted in findings. SEC staff said they had not broken out separate Regulation S-P examination findings of broker-dealer examinations for this period and could not provide those numbers. They said the most common deficiencies were failure to provide privacy notices, no or inadequate privacy policy, and no or inadequate policies and procedures for safeguarding customer information. SEC staff said they had not found any deficiencies during their exams that warranted formal enforcement actions. They told us they have dealt with Regulation S-P compliance more as a supervisory matter and required registrants to resolve deficiencies without taking formal actions.

SEC staff also said that SEC is now conducting a special review coordinated with NYSE Regulation looking at how broker-dealers are outsourcing certain functions that involve customer information. They said they are concerned with how registrants are managing the outsourcing process, including, among other things, due diligence in contractor selection, monitoring contractor performance, and disaster recovery/business continuity planning.

NASD and NYSE Regulation Oversee Compliance of Member Broker-Dealers:

NASD and NYSE Regulation also oversee Regulation S-P compliance among member broker-dealers. According to NASD officials, NASD took a two-pronged approach to ensure that its members understand their obligations under Regulation S-P and comply with its requirements. First, NASD issued guidance to its members regarding requirements of the regulation. For example, when Regulation S-P was adopted, NASD issued guidance to facilitate compliance by providing a notice designed to inform and educate its members about Regulation S-P.[Footnote 80] In the summer of 2001, NASD issued an article setting forth questions and answers regarding Regulation S-P and reminding members of the mandatory compliance deadline.[Footnote 81] In July 2005, NASD issued another notice reminding members of their obligations relating to the protection of customer information.[Footnote 82] Second, according to NASD officials, NASD conducts routine examinations--approximately 2,500 per year--to check compliance with NASD rules and the federal securities laws, including Regulation S-P. Examiners check compliance with Regulation S-P using a risk-based approach in which examiners review certain information such as supervisory review procedures to assess the controls that exist at a firm. Depending on its findings, NASD determines whether to inspect in more detail the firm's Regulation S-P policies and procedures to ensure they are reasonably designed to achieve compliance with Regulation S-P, including its safeguarding and privacy requirements. Regulation S-P compliance was reviewed in 4,760 NASD examinations of broker-dealers between October 1, 2000, and September 30, 2005. These examinations resulted in 502 informal actions

and two formal actions--called Letters of Acceptance, Waiver, and Consent--for Regulation S-P violations. According to NASD, in one formal action, it censured and fined the respondents a total of \$250,000 for various violations related to their failure to establish supervisory procedures and devote sufficient resources to supervision, including Regulation S-P compliance. In the other action, according to NASD, it censured and fined the firm and a principal associated person \$28,500 and suspended the person for 30 days for failing to provide privacy notices to its customers and for several other non-privacy-related violations.

Similarly, NYSE Regulation issued guidance on Regulation S-P to its member firms and sent its members an information memo reminding them of Regulation S-P requirements shortly before they became mandatory.[Footnote 83] NYSE Regulation's Sales Practice Review Unit conducts examinations of member firms' compliance with Regulation S-P and other privacy requirements on a 1-, 2-or 4-year cycle, or when the member firm is otherwise deemed to be at a certain level of risk.

State Insurance Regulators Require Insurers to Comply with Information Privacy and Security Provisions, but Enforcement May Be Limited:

GLBA designates state insurance regulators as the authorities responsible for enforcement of its information privacy and safeguarding provisions among insurance companies. The individual states are responsible for enforcing GLBA with respect to insurance companies licensed in the state, and they may issue regulations.[Footnote 84] The National Association of Insurance Commissioners (NAIC) has issued model rules to guide states in developing programs to enforce GLBA requirements and has sponsored a multistate review of insurance companies' performance in this regard.

NAIC Has Developed Model GLBA Privacy and Safeguarding Rules, but Not All States Have Adopted GLBA Regulations:

NAIC has developed two model rules for states to use in developing regulations or laws to implement the GLBA information privacy and safeguarding provisions among the insurance companies they regulate. The first model rule, the Privacy of Consumer Financial and Health Information Regulation, issued in 2000, includes notice and opt-out requirements relating to insurance entities, and can be used by states as models for state laws and regulations. An August 2005 NAIC analysis showed that all states and the District of Columbia had adopted insurance laws or regulations to implement GLBA's requirements related to the privacy of financial information.[Footnote 85]

The second model rule, the Standards for Safeguarding Customer Information Model Regulation, issued in 2002, establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. In contrast to the privacy model, an October 2005 NAIC analysis showed that 17 states had yet to adopt a law or regulation setting standards for safeguarding customer information. In April 2002, GAO reported that insurance customer information and records in states that had not established safeguards may not be subject to a consistent level of legal protection envisioned by GLBA's privacy provisions.[Footnote 86]

Individual State Insurance Regulators Have Not Consistently Examined for Privacy and Security Compliance:

Individual state insurance regulators have procedures for examining companies for compliance with information privacy and safeguarding requirements, but do not routinely do so. According to an NAIC official, NAIC's Market Conduct Examiners Handbook contains detailed examination procedures for reviewing information privacy requirements and its Financial Examiners Handbook has a segment devoted to security of computer-based systems. He said the individual state regulators can examine for compliance with privacy requirements as part of their comprehensive examinations of companies, but that states are focusing less on conducting comprehensive examinations and more on targeted examinations. As a result of a lack of complaints regarding privacy matters, however, he said the states are probably doing few targeted examinations of compliance with privacy requirements.

To forestall possible multiple, overlapping, and inconsistent examinations by numerous states, NAIC in 2005 sponsored a multistate review to gather information on insurance companies' compliance with GLBA privacy and safeguarding provisions. The review team, led by the District of Columbia's Department of Insurance, Securities and Banking (DISB), with the participation of 19 states, covered more than 100 of the largest insurance groups, representing about 800 insurance companies operating in the United States.[Footnote 87] The review team administered a survey questionnaire, reviewed each insurer's responses to the questionnaire, and subsequently held conferences with representatives of the insurer. The review resulted in:

- * 22 findings related to the risk assessment process, including failure to work toward a formalized assessment process to identify risks of internal and external threats and hazards to the safeguarding, confidentiality, and integrity of information;
- * 18 findings related to GLBA's requirements for information storage, transmission, and integrity;
- * 16 findings related to the delivery of privacy notices (although 12 of those findings related to the provision of the initial notice rather than recurring findings); and:
- * no findings related to GLBA procedures for providing opt-out notifications or procedures for collecting opt-out elections.

These findings were similar to those of other financial regulators' examinations of GLBA compliance. However, unlike the other regulators, state insurance regulators do not have comparable examination programs to follow up to ensure that such findings are corrected and do not become more numerous. The DISB qualified the scope of its survey by noting that it did not include (1) a review of the insurer's efforts with respect to remediation activities, (2) a detailed analysis of the effectiveness of the insurer's plans to correct privacy problems or to protect the business against the consequences associated with any privacy-related occurrences, or (3) a determination of steps the insurer must take to become privacy compliant or maintain privacy compliance.

Although this survey was not a substitute for regulatory examination of insurers' compliance with GLBA, it could serve as a basis for further examination of such compliance. Other financial regulators have gathered preliminary information that they then use as a basis for further examinations of regulated entities. For example, in 2003, SEC

followed up on reports of abusive practices in mutual fund trading by requesting information from various mutual fund companies on these trading practices, and this served as a basis for further examinations of individual companies. According to NAIC officials, the DISB survey results were never reviewed by state insurance regulators as part of their examinations of insurance companies. NAIC officials said the survey results were reviewed by NAIC's Market Analysis Working Group and referred back to DISB to determine what, if any, additional follow-up was necessary. DISB staff told us that most state insurance regulators, as well as DISB, do not have staff with adequate expertise to actually examine insurers' information privacy and safeguarding programs. They said the states would have to contract with vendors to obtain this expertise.

FTC Enforces GLBA and FCRA Compliance of Financial Institutions within Its Jurisdiction:

As discussed earlier, FTC enforces GLBA for financial institutions not otherwise assigned to the enforcement authority of another regulator, and enforces FCRA for the same entities and others, including securities firms and insurance companies. FTC has issued rules implementing GLBA and FCRA information privacy and safeguarding requirements and developed other materials that provide detailed guidance for companies to implement the requirements. FTC issued two rules--referred to as the Privacy Rule and the Safeguards Rule--to implement GLBA's requirements for financial institutions not covered by similar regulations issued by the financial institution regulators. These rules provide examples to clarify things such as what constitutes a customer relationship and what types of information are covered under the law's sharing restrictions. FTC has also issued rules to implement the FACT Act amendments to FCRA, although some rules have not yet been issued in final form.[Footnote 88] FTC provides additional guidance to financial institutions on how to comply with GLBA and FCRA in the form of business alerts, fact sheets, frequently asked questions, and a compliance guide for small businesses. For example, FTC has issued alerts on safeguarding customers' personal information, disposing of consumer report information, and insurers' use of consumer reports.

Between 2003 and 2005, FTC took enforcement actions against at least seven financial service providers for violations of GLBA information privacy and safeguarding requirements, resulting in settlement agreements with:

- * an Internet mortgage lender accused of false advertising and failure to protect sensitive consumer information;
- * a credit card telemarketer that allegedly failed to notify consumers of its privacy practices and obtained information from consumers under false pretenses;
- * two or more mortgage lenders charged with failing to protect consumers' personal information; and
- * three nonprofit debt management organizations accused of failing to notify consumers how their personal information would be used, and other violations.[Footnote 89]

NCUA, Securities, and Insurance Regulators Do Not Have Full Authority to Examine Third-Party Vendors, Including Information Resellers:

As part of their bank examinations, FRB, FDIC, OCC, and OTS have authority to examine third-party service providers, such as some information resellers with which banks may do business.[Footnote 90] Technology service provider examinations are done under the auspices of FFIEC and coordinated with other regulators.[Footnote 91] Some vendors may be examined routinely; for example, officials of one information reseller providing services to banks told us that it is subject to periodic examinations under the auspices of FFIEC. In other cases, a service provider may be examined only once for a particular purpose. For example, OCC and FDIC examiners visited Acxiom, which provides a number of banks with information services, such as analyzing and enhancing customer information for marketing purposes. The examiners' visit focused on a security breach in which a client was granted access to information files obtained from other clients. According to Acxiom officials, this was a one-time review of the breach that occurred in its computer services operations and did not result in the company being added to a list of technology service providers that banking regulators routinely review.

Unlike the banking regulators, NCUA does not have authority to examine the third-party service providers of credit unions, including information resellers.[Footnote 92] In 2003, we reported that credit unions increasingly rely on third-party vendors to support technology-related functions such as Internet banking, transaction processing, and fund transfers.[Footnote 93] With greater reliance on third-party vendors, credit unions subject themselves to operational and reputational risks if they do not manage these vendors appropriately. While NCUA has issued guidance regarding the due diligence credit unions should apply to third-party vendors, the agency has no enforcement powers to ensure full and accurate disclosure. As such, in 2003 we suggested that Congress consider providing NCUA with legislative authority to examine third-party vendors, and NCUA has also requested such authority from Congress. However, an NCUA official told us that few of these vendors are information resellers because credit unions typically do not use them to a great extent. He said that credit unions generally use methods other than resellers to comply with PATRIOT Act customer identification requirements, and credit unions' bylaws typically forbid sharing customers' personal financial information for marketing purposes.

Similarly, federal securities regulators and representatives of state insurance regulators told us they generally do not have authority to examine or review the third-party service providers of the firms they oversee, including information resellers. According to SEC staff, the agency can examine the third-party vendor only if the firm also is an SEC-registered entity over which the agency has examination authority. However, they said that, to date, SEC has not seen sufficient problems with third-party vendors to justify requesting the authority to examine them at this time. They noted that in their examinations, they hold entities accountable for ensuring that personal information is appropriately safeguarded whether the information is managed in-house or by a vendor. Similarly, NASD officials said that although they do not have jurisdiction to oversee third-party vendors, their examiners review member firms' procedures for monitoring contractors, including whether such contracts contain clauses ensuring the privacy and security of customer information. In July 2005, NASD issued a Notice to Members reminding them that when they outsource certain activities as part of their business structure, they must conduct a due diligence analysis to ensure that the third-party service provider can adequately perform the outsourced functions and comply with federal securities

laws and NASD rules.[Footnote 94] Similarly, NYSE Regulation examinations review third-party contracts to ensure that they contain confidentiality clauses prohibiting the contractor from using or disclosing customer information for any use other than the purposes for which the information was provided to the contractor. NYSE Regulation has proposed a rule governing its members' use of contractors, which, if adopted, will require member firms to follow certain steps in selecting and overseeing contractors, such as applying prescribed due diligence standards and the record-keeping requirements of the securities laws[Footnote95].

State insurance regulators generally do not have authority to examine information resellers and other third-party service providers. NAIC officials told us that state insurance regulators can only examine information resellers or other companies if they are registered as rating organizations--companies that collect and analyze statistical information to assist insurance companies in their rate-making process. For example, NAIC said state insurance regulators can examine ISO--one of the resellers included in our review--because it is registered with states as a rating organization.

Conclusions:

Advances in information technology and the computerization of records have spawned the growth of information reseller businesses, which regularly collect, process, and sell personal information about nearly all Americans. The information maintained by resellers commonly includes sensitive personal information, such as purchasing habits, estimated incomes, and Social Security numbers. The expansion in the past few decades in the sale of personal information has raised concerns about both personal privacy and data security. Many consumers may not be aware how much of their personal information is maintained and how frequently it is disseminated. In addition, identity theft has emerged as a serious problem, and data security breaches have occurred at some major resellers. At the same time, however, information resellers also provide some important benefits to both individuals and businesses. Financial institutions rely heavily on these resellers for a variety of vital purposes, including credit reporting (which reduces the cost of credit), PATRIOT Act compliance, and fraud detection. As Congress weighs various legislative options, it will need to consider the appropriate balance between protecting consumers' privacy and security interests and the benefits conferred by the current regime that allows a relatively free flow of information between companies.

No federal law explicitly requires all information resellers to safeguard all of the sensitive personal information they may hold. As we have discussed, FCRA applies only to consumer information used or intended to be used to help determine eligibility, and GLBA's safeguarding requirements apply only to customer data held by GLBA-defined financial institutions. Much of the personal information maintained by information resellers that does not fall under FCRA or GLBA is not necessarily required by federal law to be safeguarded, even when the information is sensitive and subject to misuse by identity thieves. Given financial institutions' widespread reliance on information resellers to comply with legal requirements, detect fraud, and market their products, the possibility for misuse of this sensitive personal information is heightened. Requiring information resellers to safeguard all of the sensitive personal information they hold would help ensure that explicit data security requirements apply more comprehensively to a class of companies that maintains large amounts of

such data. Further, although the scope of this report focused on information resellers, this work has made clear to us that a wide range of retailers and other entities also maintain sensitive personal information on consumers. As Congress considers requiring information resellers to better ensure that all of the sensitive personal information they maintain is safeguarded, it may also wish to consider the potential costs and benefits of expanding more broadly the class of entities explicitly required to safeguard sensitive personal information. Any new safeguarding requirements would likely be more effectively implemented and least burdensome if, as with FTC's Safeguards Rule, they provided sufficient flexibility to account for the widely varying size and nature of businesses that hold sensitive personal information.

The proliferation of sensitive personal information in the marketplace and increasing numbers of high-profile data breaches have motivated many states to enact data security laws with breach notification requirements. No federal statute currently requires breach notification, but such legislation could have certain benefits. Companies would have incentives to improve data safeguarding to reduce the reputational risk of a publicized breach, and consumers would know to take potential action against a risk of identity theft or other related harm. Congress has held many hearings related to data breaches, and several bills have been introduced that would require breach notification. We support congressional actions to require information resellers, and other companies, to notify individuals when breaches of sensitive information occur. In previous work, we have also identified key benefits and challenges of notifying the public about security breaches that occur at federal agencies. To be cost effective and reduce unnecessary burden on consumers, agencies, and industry, it would be important for Congress to identify a threshold for notification that would allow individuals to take steps to protect themselves where the risk of identity theft or other related harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Objective criteria for when notification is required and appropriate enforcement mechanisms are also important considerations. Congress should also consider whether and when a federal breach notification law would preempt state laws.

FTC has taken many significant enforcement actions against information resellers and other companies that have violated federal privacy laws, and it is important that the agency have the appropriate enforcement remedies. Unlike FCRA, GLBA does not provide FTC with civil penalty authority, and agency staff have expressed concerns that the remedies FTC has available under GLBA--such as disgorgement and consumer redress--are impractical enforcement tools for violations involving breaches of mass consumer data. Providing FTC with the authority to seek civil penalties for violations of GLBA could help the agency more effectively enforce that law's safeguarding provisions.

Federal financial regulators generally appear to provide suitable oversight of their regulated entities' compliance with privacy and information security laws governing consumer information. The regulators do not typically distinguish between data that entities receive from resellers and other sources, but this seems reasonable given that the sensitivity, rather than the source, of the data is the most important factor in examining data security practices. However, state insurance regulators do not have comparable examination programs to other financial regulators to ensure consistent GLBA compliance. This may be a source of concern given the recent multistate survey that

identified deficiencies in GLBA compliance at insurance companies.

Matters for Congressional Consideration:

Safeguarding provisions of FCRA and GLBA do not apply to all sensitive personal information held by information resellers. To ensure that such data are protected on a more consistent basis, Congress should consider requiring information resellers to safeguard all sensitive personal information they hold. As Congress considers how best to protect data maintained by information resellers, it should also consider whether to expand more broadly the class of entities explicitly required to safeguard sensitive personal information. If Congress were to choose to expand safeguarding requirements, it should consider providing the implementing agencies with sufficient flexibility to account for the wide range in the size and nature of entities that hold sensitive personal information.

To ensure that the Federal Trade Commission has the tools it needs to most effectively act against data privacy and security violations, Congress should consider providing the agency with civil penalty authority for its enforcement of the Gramm-Leach-Bliley Act's privacy and safeguarding provisions.

Recommendation for Executive Action:

We recommend that state insurance regulators, individually and in concert with the National Association of Insurance Commissioners, take additional measures to ensure appropriate enforcement of insurance companies' compliance with the privacy and safeguarding provisions of the Gramm-Leach-Bliley Act. As a first step, state insurance regulators and NAIC should follow up appropriately on deficiencies related to compliance with these provisions that were identified in the recent nationwide survey as part of a broader targeted examination of GLBA privacy and safeguarding requirements.

Agency Comments:

We provided a draft of this report to FDIC, FRB, FTC, NAIC, NASD, NCUA, NYSE Regulation, OCC, OTS, and SEC for comment. These agencies provided technical comments, which we incorporated, as appropriate. In addition, FTC provided a written response, which is reprinted in appendix III. In its response, FTC noted that it has previously recommended that Congress consider legislative actions to increase the protection afforded personal sensitive data, including extending GLBA safeguarding principles to other entities that maintain sensitive information. FTC also noted that it concurs with our finding that a civil penalty often is the most appropriate and effective remedy in cases under GLBA privacy and safeguarding provisions.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the report date. At that time, we will provide copies to other interested congressional committees, as well as the Chairman of the Board of Governors of the Federal Reserve System, the Acting Chairman of the Federal Deposit Insurance Corporation, the Chairman of the Federal Trade Commission, the President of the National Association of Insurance Commissioners, the Chairman and Chief Executive Officer of NASD, the Chairman of the National Credit Union Administration, the Chief Executive Officer of New York Stock Exchange Regulation, the Comptroller of the Currency, the Director of the Office of Thrift

Supervision, and the Chairman of the Securities and Exchange Commission. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at [Hyperlink, <http://www.gao.gov>].

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or jonesy@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Signed by:

Yvonne D. Jones:
Director, Financial Markets and Community Investment:

[End of section]

Appendix I: Scope and Methodology:

Our report objectives were to examine (1) how financial institutions use data products supplied by information resellers, the types of information contained in these products, and the sources of the information; (2) how federal laws governing the privacy and security of personal data apply to information resellers, and what rights and opportunities exist for individuals to view and correct data held by resellers; (3) how federal financial institution regulators and the Federal Trade Commission (FTC) oversee information resellers' compliance with federal privacy and information security laws; and (4) how federal financial institution regulators, state insurance regulators, and FTC oversee financial institutions' compliance with federal privacy and information security laws governing consumer information, including information supplied by information resellers.

For the purposes of this report, we defined "information resellers" broadly to refer to businesses that collect and aggregate personal information from multiple sources and make it available to their customers. The three nationwide credit bureaus were included in this definition. Our audit work focused primarily on larger information resellers and did not cover smaller Internet-based resellers because these companies were rarely or never used by financial institutions from which we collected information. Our scope was limited to resellers' use and sale of personal information about individuals; it did not include other information that resellers may provide, such as data on commercial enterprises. Our review of financial institutions covered the banking, securities, property and casualty insurance, and consumer lending and finance industries, but excluded life insurance and health insurance companies because they use health data that are covered by federal laws that were outside the scope of our work. In addition, we included financial institutions' use of reseller information for purposes related to customers and other consumers, but excluded their use of reseller products for screening their own employees or making business decisions such as where to locate a facility.

To address all of the objectives, we interviewed or received written responses from 10 information resellers--Acxiom, eFunds, ChoicePoint, Equifax, Experian, LexisNexis, ISO, Regulatory DataCorp, Thompson West, and TransUnion. We also reviewed marketing materials, sample contracts, sample reports, and other items from these companies that provided

detailed information on the data contained in their products. These companies were selected because, according to the financial institutions, trade associations, and industry experts we spoke with, they constitute most of the largest and most significant information resellers offering services to the financial industry sector, and collectively they represent a variety of different products. The information resellers we included and the products they offer do not necessarily represent the full scope of the industry. We also spoke with representatives of the Consumer Data Industry Association and the Direct Marketing Association, trade associations that represent portions of the information reseller industry.

To determine how financial institutions use data products supplied by information resellers and the types and sources of the data, we also interviewed or received written responses, and collected and analyzed documents, from knowledgeable representatives at financial institutions in the banking, securities, property and casualty insurance, and consumer lending and finance industries. We gathered information from Bank of America, Citigroup, and JPMorgan Chase, which are the three largest U.S. bank holding companies by asset size, as well as Goldman Sachs, Morgan Stanley, and Merrill Lynch, which are the three largest global securities firms by revenue. We also interviewed representatives at American International Group, State Farm, and Allstate, which are the three largest U.S. insurance companies and include the two largest property/casualty insurers. We also interviewed representatives at GE Consumer Finance, one of the world's 10 largest consumer finance companies, and four other financial institutions-- American Express, Wells Fargo Financial, Security Finance, and Check into Cash--which together offer a variety of consumer lending products, including automobile financing, credit cards, and payday loans. We also interviewed officials at trade associations representing these financial services industries, including the American Bankers Association, Independent Community Bankers of America, Securities Industry Association, Investment Company Institute, American Insurance Association, and American Financial Services Association.

These financial institutions from which we gathered information conduct a significant portion of the transactions in the financial services sector. For example, they collectively own 9 of the 50 largest commercial depository institutions, holding about 20 percent of total domestic deposits, as well as 8 of the 10 largest credit card issuers. The insurance companies we spoke with represent about a quarter of the U.S. property and casualty insurer market share. In most cases, we selected these financial institutions by determining the largest companies in each of the four industries, based on data from reputable sources. In two cases, we spoke with firms because they were recommended by representatives of their trade association. Our findings on how financial institutions use information resellers are not representative of the entire financial services industry. However, we believe they accurately represent institutions' use of resellers because our findings from discussions with these companies and their representatives were corroborated by discussions with information resellers, regulators, legal experts, and privacy and consumer advocacy groups.

To identify how federal privacy and data security laws and regulations apply to information resellers and individuals' rights and opportunities to view and correct reseller data, we reviewed and analyzed relevant federal laws, regulations, and guidance. We also met with staff of the Board of Governors of the Federal Reserve System,

Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision, and Securities and Exchange Commission, as well as the National Association of Insurance Commissioners (NAIC), NASD (formerly known as the National Association of Securities Dealers), New York Stock Exchange Regulation (NYSE Regulation), and the District of Columbia's Department of Insurance, Securities and Banking (DISB). In addition, we interviewed three legal experts in the area of privacy law that work in academia or represent financial institutions and information resellers. We also interviewed and collected documents from information resellers, financial institutions, federal regulators, and a variety of privacy and consumer advocacy groups, to gather views on the applicability of laws to information resellers and the adequacy of existing laws.

To describe how regulators oversee information resellers' and financial institutions' compliance with federal privacy and data security laws, we met with the federal agencies, financial institutions, information resellers, and other parties listed above. We also reviewed federal agencies' guidance, examination procedures, settlement agreements, and other documents, as well as relevant reports and documents from NAIC, NASD, and NYSE Regulation. To help illustrate regulators' examination activities in this area, we also met with OCC staff who conduct examinations at three national banks and reviewed their examination workpapers. We also gathered data from regulators about the number and nature of examination findings, where applicable.

To describe the efforts of state insurance regulators to oversee insurance companies' compliance with the Gramm-Leach-Bliley Act (GLBA), we also reviewed the DISB survey report of insurance companies' implementation of GLBA policies and procedures. DISB used the survey responses to determine findings for each company on the level of compliance with GLBA and related NAIC model rule provisions. The DISB review defined a "finding" as an occurrence of a perceived gap between a company's privacy practices and procedures and the guidelines outlined in one of the model acts or regulations of NAIC. The findings were derived from responses to the survey questions. The companies DISB surveyed comprised major companies, including property and casualty insurance groups with 2002 gross written premiums of approximately \$250 million or more; life insurance groups with 2002 gross written premiums of approximately \$200 million or more; and health insurance groups with 2002 gross written premiums of approximately \$500 million or more. This initial list contained 129 insurance groups. After the initial list was compiled, 26 groups were exempted from the survey examination for one of three reasons: (1) there was a prior, ongoing, or upcoming examination of the group that included (or would include) a comprehensive review of the group's privacy policy (23 groups); (2) the group engaged primarily or solely in reinsurance (2 groups); or (3) the state insurance regulator for the company's state of domicile requested that the group be exempted (1 group). The survey questionnaire included 93 questions asking for detailed documentary and testimonial evidence of companies' level of compliance with GLBA and related NAIC model rule provisions.

We conducted our review from June 2005 through May 2006 in accordance with generally accepted government auditing standards.

[End of section]

Appendix II: Sample Information Reseller Reports:

This appendix provides examples of reports from different types of products sold by information resellers. These sample reports, which are reprinted with permission, contain fictitious data and have also been redacted to reduce possible coincidental references to actual people or places.

Sample Insurance Claims History Report:

This sample insurance claims history report from ChoicePoint provides insurers with insurance claims histories on individuals applying for coverage.

Figure 4: Sample Insurance Claims History Report:

[See PDF for image]

Source: ChoicePoint.

[End of figure]

Sample Deposit Account History Report:

ChexSystems, a subsidiary of eFunds, offers a product that assesses risks associated with individuals applying to open new deposit accounts. The report includes information on an applicant's account history, including accounts closed for reasons such as overdrafts, returned checks, and check forgery. The report may include a numeric score representing the individual's estimated risk.

Figure 5: Sample Deposit Account History Report:

[See PDF for image]

Source: eFunds.

[End of figure]

Sample Identity Verification and OFAC Screening Report:

ISO, a company that provides information services to insurance companies, offers this product for screening new customers and verifying their identities. It provides a "pass" or "fail" response to indicate whether information provided by the applicant matches information maintained by the company.

Figure 6: Sample Identity Verification and OFAC Screening Report:

[See PDF for image]

Source: ISO.

[End of figure]

Sample Fraud Investigation Report:

Below are selected excerpts from a sample report of ChoicePoint's AutoTrack XP product, which helps users such as corporate fraud investigators and law enforcement agencies conduct investigations, locate individuals and assets, and verify physical addresses.

Figure 7: Sample Fraud Investigation Report:

[See PDF for image]

Source: ChoicePoint.

[End of figure]

[End of section]

Appendix III: Comments from the Federal Trade Commission:

Federal Trade Commission:
Washington, D .C. 20580:
The Chairman:

June 2, 2006:

Ms.Yvonne Jones:
Director, Financial Markets and Community Investment:
Government Accountability Office:
Washington, D.C. 20548:

Dear Ms. Jones:

The Commission is pleased to have the opportunity to comment on the Government Accountability Office's draft report entitled: Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard all Sensitive Data (GAO-06-674). ("Report") The Report describes the sources of consumer personal data, how different entities use or reuse the data, and the statutory provisions that govern the collection, use, and reuse of sensitive personal information. The Report also explains how banking regulators, the Securities and Exchange Commission, and the Federal Trade Commission ("FTC") oversee compliance with the privacy and safeguarding provisions of the Gramm-Leach-Bliley Act ("GLBA"), and describes the FTC's enforcement of the Fair Credit Reporting Act ("FCRA") with respect to information resellers. The Report concludes that "[n]o federal law explicitly requires all information resellers to safeguard all the sensitive personal information they may hold." It also finds that entities other than information resellers hold sensitive personal information.

We understand that the agencies' staffs worked cooperatively throughout the preparation of this report and that FTC staff has provided infonnal technical comments on the draft of the Report to the GAO staff, the vast majority of which have been incorporated.

The Report makes several legislative recommendations, two of which the Commission supports, and one on which the Commission has no opinion. First, the Report recommends that Congress consider requiring information resellers to safeguard all sensitive personal information they hold, and suggests that Congress consider the benefits and costs of expanding the class of entities explicitly required to safeguard sensitive personal information. (Report at 42) The FTC similarly has recommended that Congress consider legislative actions to increase the protection afforded sensitive personal data. In its June 2005 testimony before the Senate Committee on Commerce, Science, and Transportation on data breaches and identity theft, the Commission recommended that

Congress consider extending the GLBA safeguards principles, which require financial institutions to implement procedures to protect consumer financial information, to other entities that maintain sensitive information.[Footnote 96]

Second, the Report recommends that Congress consider authorizing the FTC to seek civil penalties for violations of the GLBA privacy and safeguarding provisions. In its testimony to the Senate Committee cited above, the Commission noted that a civil penalty often is the most appropriate and effective remedy in cases under those provisions[Footnote 97]. The Commission thus agrees with the Report's recommendation.

Finally, the Report recommends that state regulators ensure compliance with GLBA in its oversight of insurance companies. Although the Commission does not have an opinion regarding state oversight of insurance companies, the Commission agrees with GAO's conclusion that insurance companies often hold sensitive personal data.

Protecting the privacy and security of personal information collected or sold by data brokers and others is one of the Commission's highest priorities. The Commission will continue to monitor this area and will take law enforcement action when appropriate against entities that fail to protect properly sensitive consumer data[Footnote 98].

Further, the Commission encourages consumers to understand their rights under the FCRA and GLBA, and to take appropriate measures to protect their data. We have developed an array of consumer education materials for these purposes, which are available online at [Hyperlink, <http://www.ftc.gov>].

The Commission appreciates this opportunity to review and comment on GAO's Report.

By direction of the Commission.

Signed by:

Deborah Platt Majoras:
Chairman:

[End of section]

Appendix IV: GAO Contact and Staff Acknowledgments:

GAO Contact:

Yvonne D. Jones, (202) 512-8678 or jonesy@gao.gov:

Staff Acknowledgments:

In addition to the contact named above, Jason Bromberg, Assistant Director; Katherine Bittinger; David Bobruff; Randy Fasnacht; Evan Gilman; Marc Molino; David Pittman; Linda Rego; and David Tarosky made key contributions to this report.

FOOTNOTES

[1] This report uses "information resellers" to describe businesses that collect and resell personal information, but there is no one

commonly agreed-upon term for such companies. FTC has sometimes used the term "data brokers" but the companies themselves typically use other terms, such as "information solutions providers."

[2] The Fair Credit Reporting Act, Pub. L. No. 90-321, title VI (May 29, 1968) as added by Pub. L. No. 91-508, title VI, § 601, 84 Stat. 1128 (Oct. 26, 1970) (codified at 15 U.S.C. § 1681-1681x); and Title V of the Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No. 106-102, title V, subtitle A, 113 Stat. 1338 (Nov. 12, 1999) (codified at 15 U.S.C. § 6801-6809). As discussed later in this report, other federal laws--such as the Driver's Privacy Protection Act of 1994 and the Health Insurance Portability and Accountability Act of 1996--also govern the use and sharing of certain types of personal information.

[3] For more information about Internet resellers, see GAO, Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs, GAO-06-495 (Washington, D.C.: May 17, 2006).

[4] We use "nationwide credit bureau" and "nationwide consumer reporting agency" interchangeably in this report, and they have the same meaning as the FCRA phrase "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis." FCRA defines this phrase as a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining public record information and credit account information for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity. 15 U.S.C. § 1681a(p).

[5] For information about federal agencies' use of information resellers, see GAO, Personal Information: Agency and Reseller Adherence to Key Privacy Principles, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

[6] Credit header data are the nonfinancial identifying information located at the top of a credit report, such as name, current and prior addresses, telephone number, and Social Security number.

[7] This report focuses on how financial institutions use data from information resellers in conducting transactions with consumers. We did not review other ways that financial institutions use information resellers, such as to screen their potential employees or to gather information about other businesses.

[8] The three nationwide credit bureaus use software models developed by the Fair Isaac Corporation to produce FICO® credit scores, which are credit scores used by many financial services firms. In March 2006, the bureaus announced they will begin selling a new credit score that they developed jointly. The score will be calculated the same way for each credit bureau to enhance consistency among all three bureaus.

[9] A nationwide specialty CRA is defined in FCRA to mean a CRA that compiles and maintains files on consumers on a nationwide basis relating to medical records or payments; residential or tenant history; check-writing history; employment history; or insurance claims. 15 U.S.C. § 1681a(w).

[10] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of

2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). We will refer to the act as the PATRIOT Act.

[11] Title III of the PATRIOT Act (cited as the "International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001") amended the U.S. government's anti-money laundering regulatory structure. For instance, section 326 added new requirements for the Secretary of the Treasury and the federal financial regulators to issue regulations setting forth minimum standards for financial institutions to (1) verify the identity of persons seeking to open an account; (2) maintain records of the information used to verify a person's identity, including name, address, and other identifying information; and (3) consult lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on the list. See 31 U.S.C. § 5318(1). Section 326 requirements for customer verification apply to financial institutions broadly, including, among others, financial institutions that are subject to regulation by one of the federal banking regulators, as well as nonfederally insured credit unions, private banks and trust companies; securities broker-dealers; futures commission merchants and introducing brokers; and mutual funds. 31 U.S.C. § 5312 and 31 C.F.R. § Part 103.

[12] A manufacturer may request that consumers submit their contact information on a warranty card in the event of a product malfunction or insurance claim. For marketing purposes, many warranty cards request additional information on such things as the gender and age of household occupants, occupation and income information, spending habits, and lifestyle interests; this information is sometimes sold to information resellers.

[13] The Fair Credit Reporting Act, described in more detail below, generally permits prescreening only if the financial institution makes a firm offer of credit or insurance for all consumers who meet the criteria for the credit or insurance being offered. 15 U.S.C. § 1681b(c)(1)(B).

[14] This report focuses on the use and sharing of personal information among private sector entities, and therefore we only describe laws governing these entities. Other laws, primarily the Privacy Act of 1974, govern the collection and use of personal information by government agencies. See Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974), codified at 5 U.S.C. § 552a.

[15] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 262, 110 Stat. 1936 (Aug. 21, 1996), codified at 42 U.S.C. §§ 1320d - 1320d-8, protects the privacy of individually identifiable health information. The scope of this work did not include the collection and use of health information.

[16] Pub. L. No. 103-322, title XXX, 108 Stat. 2099 (Sept. 13, 1994) (codified at 18 U.S.C. §§ 2721 - 2725).

[17] 18 U.S.C. § 2721(b)(11).

[18] Pub. L. No. 63-203, ch. 311, 38 Stat. 717 (Sept. 26, 1914) (codified at 15 U.S.C. §§ 41 - 58).

[19] See 12 U.S.C. § 1867 (FRB, FDIC, and OCC); and 12 U.S.C. § 1464(d)(7) (OTS).

[20] Although the scope of this report is limited to federal privacy and data security laws, many states have laws of their own that apply to the activities of information resellers. Many of these laws require companies to notify consumers when their personal data may have been lost or stolen. For example, in 2002, California enacted a database breach notification act (Cal. Civ. Code § 1798.82), which requires disclosure of any security breach of data to any state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

[21] FCRA defines a "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [15 U.S.C. § 1681b]." 15 U.S.C. § 1681a(d)(1).

[22] Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003) (codified at 15 U.S.C. §§ 1681c-1, 1681c-2, 1681x, 1681s-3, 1681w).

[23] We did not determine which information reseller databases are subject to FCRA. The information we include is based on what information resellers told us about how FCRA applies to their activities.

[24] Consumers also have the right to receive a free copy of their credit file from CRAs when they have been victims of identity theft or are subject to an adverse action as a result of information in their file, or in certain other circumstances where they are unemployed, recipients of public welfare, or have reason to believe that their file contains inaccurate information due to fraud.

[25] FCRA also provides certain other opt-out rights concerning affiliate sharing. See 15 U.S.C. §§ 1681a(d)(2)(iii); and 1681s-3. In addition to FCRA, GLBA requires that financial institutions allow their customers to opt out of the sharing of their nonpublic personal information with nonaffiliated companies, unless the sharing falls under an exception under GLBA. See 15 U.S.C. § 6802.

[26] 16 C.F.R. § 610.2.

[27] 16 C.F.R. § 610.3.

[28] 15 U.S.C. § 6802.

[29] See 15 U.S.C. § 6809(9). GLBA defines a consumer as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes." Thus, GLBA does not apply to a business customer, such as a sole proprietor. 16 C.F.R. § 313.3(e). A "customer" means a consumer who has a "customer relationship"--that is, a continuing relationship with the financial institution.

[30] 15 U.S.C. § 6802(e)(3)(B) and (6).

[31] 15 U.S.C. § 6802(e)(1)(A).

[32] 15 U.S.C. § 6809(3)(A).

[33] 12 U.S.C. § 1843(k). This is a list of nonbanking activities determined by FRB as of the date of GLBA's enactment to be "so closely related to banking or managing or controlling banks as to be a proper incident thereto." See 12 C.F.R. § 225.28 (1999). FDIC, FRB, NCUA, OCC, OTS and SEC in their implementing GLBA regulations define the term "financial institution" as those institutions in the business of engaging in activities that are financial in nature or incidental to such financial activities. See 12 C.F.R. §§ 40.3(k)(1) (OCC), 216.3(k)(1) (FRB), 332.3(k)(1) (FDIC), 573.3(k)(1) (OTS), and 716.3(l)(1) (NCUA); and 17 C.F.R. § 248.3(n)(1) (SEC). See 16 C.F.R. § 313.3(k)(1) (FTC).

[34] 16 C.F.R. § 313.18(a)(2); and 65 Fed. Reg. 33646, 33654 (May 24, 2000).

[35] 16 C.F.R. §§ 313.3(k)(1) and (3)(iv).

[36] 12 C.F.R. § 225.28(b)(2)(v) (1999). FRB described credit bureau services as those services "maintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower."

[37] See *Trans Union LLC v. FTC*, 295 F.3d 42, 48 (D.C. Cir. 2002); and 16 C.F.R. § 313.3(k).

[38] A representative of the company noted that, as required by law, the data used for these two products are kept in separate databases that are not commingled.

[39] 16 C.F.R. § 313.11 (FTC); see also 12 C.F.R. §§ 40.11 (OCC), 216.11 (FRB), 332.11 (FDIC), 573.11 (OTS), and 716.11 (NCUA); and 17 C.F.R. § 248.11 (SEC). The regulations were upheld in *Individual Reference Services Group, Inc. v. FTC*, 145 F. Supp.2d 6, 34 - 35 (D. DC 2002) ("the use restrictions affirmatively imposed by the Regulations are consistent with the purpose of the GLB Act").

[40] The FTC regulation states: "[y]ou may disclose and use the information pursuant to [a GLBA exception] in the ordinary course of business to carry out the activity covered by the exception under which you received the information." 16 C.F.R. § 313.11(a)(1)(iii).

[41] See 15 U.S.C. § 6802(c), which states: "[A] nonaffiliated third party that receives from a financial institution nonpublic personal information . . . shall not . . . disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution." This provision is commonly referred to as GLBA's reuse and redisclosure provision. See 16 C.F.R. § 313.11(b)(1)(iii).

[42] See 15 U.S.C. § 6801 note.

[43] The company said that it does not allow information collected for its FCRA-regulated database to be used to update the "pre-GLBA" database.

[44] 15 U.S.C. § 6801.

[45] See, for example, 16 C.F.R. § 314.3 (FTC).

[46] See, for example, 16 C.F.R. § 314.4(d).

[47] The settlement will require BJ's Wholesale Club to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years. In the Matter of BJ's Wholesale Club, Inc., F.T.C. No. 0423160 (2005). A consent agreement does not constitute an admission of a violation of law.

[48] Prepared Statement of the Federal Trade Commission on "Data Breaches and Identity Theft" Before the Senate Comm. on Commerce, Science, and Transportation, 109th Cong., 1st Sess. (2005).

[49] Although there is no applicable federal statute governing notification of data breaches, the banking agencies have issued guidance to financial institutions under their jurisdiction requiring them in some cases to notify customers affected by a data breach. States that have enacted breach notification requirements include Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin. Many other states have introduced legislation.

[50] United States v. ChoicePoint, Inc., No. 1:06-cv-00198-JTC (N.D. Ga., Feb. 15, 2006). As part of the settlement, ChoicePoint admitted no violations of law. According to ChoicePoint, the company has taken steps since the breach to enhance its customer screening process and to assist affected consumers.

[51] Congressional Research Service, Personal Data Security Breaches: Context and Incident Summaries, Order Code RL33199 (Washington, D.C., Dec. 16, 2005).

[52] For example, Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs, 109th Cong., 1st Sess. (2005); Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary, 109th Cong., 1st Sess. (2005); Assessing Data Security: Preventing Breaches and Protecting Sensitive Information: Hearing Before the House Comm. on Financial Services, 109th Cong., 1st Sess. (2005); Securing Consumers' Data: Options Following Security Breaches: Hearing Before the Subcomm. On Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce, 109th Cong., 1st Sess. (2005).

[53] For more information on the key benefits and challenges associated with notifying the public about security breaches, see GAO, Privacy: Preventing and Responding to Improper Disclosures of Personal Information, GAO-06-833T (Washington, D.C.: June 8, 2006).

[54] FCRA gives enforcement authority to FDIC, FRB, OCC, OTS, and NCUA over their banks, thrifts, and credit unions, among other entities.

FCRA assigned regulatory authority to the Departments of Transportation and Agriculture over entities under their jurisdiction. 15 U.S.C. § 1681s.

[55] 15 U.S.C. § 6805. GLBA required FTC and other regulators with responsibilities under the statute to issue consistent and comparable regulations. 15 U.S.C. § 6804.

[56] 15 U.S.C. § 1681s(c).

[57] Conn. Gen. Stat. Anno. §§ 36a-41 - 44 (disclosure to broker-dealers or investment advisers engaged in contractual networking arrangements with the financial institution permitted after the customer is given notice and an opportunity to opt out); N.D. Cent. Code §§ 6.08.1-01 - 10; Vt. Stat. Anno. Tit 8, §§ 10201 - 10205.

[58] For instance, FTC staff told us the agency filed suit in the following cases: In the Matter of Credit Bureau of Lorain, Inc., 81 F.T.C. 381 (1972); In the Matter of Credit Bureau of Columbus, Inc., 81 F.T.C. 938 (1972); In the Matter of Credit Bureau of Greater Syracuse, Inc., 84 F.T.C. 1660 (1974); In the Matter of Robert N. Barnes, 85 F.T.C. 520 (1975); In the Matter of Filmdex Chex System, Inc., 85 F.T.C. 889 (1975); In the Matter of Credit Data Northwest, 86 F.T.C. 389 (1975); In the Matter of Interstate Check Systems, Inc., 88 F.T.C. 984 (1976); In the Matter of Moore & Associates, Inc., 92 F.T.C. 440 (1978); In the Matter of Howard Enterprises, Inc., 93 F.T.C. 909 (1979); In the Matter of Trans Union Credit Information Co., 102 F.T.C. 1109 (1983); FTC v. TRW Inc., 784 F. Supp. 361 (N.D. Tex. 1991); In the Matter of I.R.S.C., Inc., 116 F.T.C. 266 (1993); In the Matter of CDB Infotek, 116 F.T.C. 280 (1993); In the Matter of Inter-Fact Inc., 116 F.T.C. 294 (1993); In the Matter of W.D.I.A.Corp., 117 F.T.C. 757 (1994); In the Matter of Equifax Credit Information Services, Inc., 120 F.T.C. 577 (1995). See also United States v. ChoicePoint, Inc., No. 1:06-cv-00198-JTC (N.D. Ga. Feb. 15, 2006); United States v. Far West Credit, Inc., No. 2:06-cv-00041-TC (C.D. Utah Jan. 17, 2006); and In the Matter of Southern Maryland Credit Bureau, Inc., 101 F.T.C. 19 (1983).

[59] In 1996, TRW Inc. sold its credit reporting business to a group of investors, who named the new company Experian.

[60] FTC has also enforced FCRA against resellers for other types of violations. For example, in 2000 FTC settled with the three nationwide credit bureaus after alleging that consumers were unable to adequately access the companies' personnel by telephone to discuss or dispute possible errors in their files. United States v. Equifax Credit Information Services, Inc., No. 1:00-CV-0087 (N.D. Ga. 2000); United States v. Experian Information Solutions, Inc., 3-00CV0056-L. (N.D. Tx. 2000); and United States v. Trans Union LLC, No. 00C 0235 (N.D. Ill. 2000). See [Hyperlink, <http://www.ftc.gov/opa/2000/01/busysignal.htm>]. A consent agreement does not constitute an admission of a violation of law.

[61] In the Matter of Equifax Credit Information Services, Inc., 120 F.T.C. 577 (1995). A consent agreement does not constitute an admission of a violation of law.

[62] In the Matter of Trans Union Corp., F.T.C. No. 9255, 2000 WL 257766 (2000), petition for review denied, 245 F.3d 809 (D.C. Cir. 2001).

[63] *United States v. ChoicePoint, Inc.*, No. 1:06-cv-00198-JTC (N.D. Ga., Feb. 15, 2006).

[64] Injunctions are judicial orders commanding a party to take an action or prohibiting a party from doing or continuing to do a certain activity. Disgorgement is having to give up profits or other gains illegally obtained.

[65] 15 U.S.C. § 1681s and 15 U.S.C. § 45(1) and (m). Regarding GLBA's prohibition against fraudulent access to financial information where a person obtains financial information relating to another person under false pretences (pretext provisions), GLBA allows FTC to seek civil penalties for violations. Specifically, FTC has authority to enforce the GLBA pretext provisions in the same manner and with the same power and authority as it has under the Fair Debt Collection Practices Act (codified at 15 U.S.C. §§ 1692 - 1692o). 15 U.S.C. § 6822(a). A violation of the Fair Debt Collection Practices Act is deemed by federal law to be an unfair or deceptive act or practice in violation of the FTC Act, which means that FTC may impose civil penalties. 15 U.S.C. § 16921(a); and *United States v. National Financial Services, Inc.*, 98 F.3d 131, 139 - 141 (4th Cir. 1996). According to FTC officials, they do not have similar civil penalty authority for violations of GLBA's privacy and safeguarding provisions.

[66] 12 U.S.C. § 1818(i)(2)(A)(i).

[67] Some exceptions may exist. For example, section 411 of the FACT Act (which amended section 604(g) of FCRA (12 U.S.C. 1681b(g))), generally limits with certain exceptions creditors' ability to obtain or use medical information pertaining to a consumer for credit purposes. This section requires the banking regulatory agencies and NCUA to issue regulations relating to the use of medical information in credit transactions. The regulations apply broadly, and the exceptions therein are available to all creditors, not just the financial institutions supervised by those agencies. See final rule published at 70 Fed. Reg. 70664, 70665 - 6 (Nov. 22, 2005).

[68] In addition to the responsibilities assigned to financial institution regulators and FTC, FCRA assigns enforcement authority to the Departments of Transportation and Agriculture for entities subject to their oversight, such as transportation carriers.

[69] The various banking agency GLBA and FCRA regulations can be found at 12 C.F.R. Parts 40 and 41 (OCC); 12 C.F.R. Parts 216, 222, and 232 (FRB); 12 C.F.R. Parts 332 and 334 (FDIC); 12 C.F.R. Parts 573 and 571 (OTS); and 12 C.F.R. Parts 716 and 717 (NCUA).

[70] 65 Fed. Reg. 35162 (June 1, 2000); and 65 Fed. Reg. 31722 (May 18, 2000). OCC, FRB, OTS, and FDIC issued their rules jointly. All of the rules were substantively identical but contained differences to account for differences between the agencies' legal authorities and, as appropriate, for the types of institutions within each agency's jurisdiction.

[71] 66 Fed. Reg. 8616 (Feb. 1, 2001) ("Interagency Guidelines Establishing Standards for Safeguarding Customer Information") (renamed "Interagency Guidelines Establishing Information Security Standards," 70 Fed. Reg. 15736 (Mar. 29, 2005)).

[72] 70 Fed. Reg. 15736 (Mar. 29, 2005) ("Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice").

[73] Pub. L. No. 108-109, 117 Stat. 1952 (Dec. 4, 2003).

[74] See 15 U.S.C. § 1681w; 69 Fed. Reg. 77610 (Dec. 28, 2004); and 69 Fed. Reg. 68690 (Nov. 24, 2004).

[75] The examinations are risk-based and conducted in cycles depending on the institution's condition and size. Banking regulators are required by law, 12 U.S.C. § 1820(d), to examine insured institutions for safety and soundness at least once during each 12-month period, except for smaller institutions that meet specified conditions that can be examined each 18-month period. We use the term "thrifts" to refer to savings associations.

[76] Banking regulators have broad enforcement powers and can take formal actions (cease and desist orders, civil money penalties, removal orders, and suspension orders, among others) or informal enforcement actions (such as memoranda of understanding and board resolutions). Informal actions are generally not publicly disclosed.

[77] 65 Fed. Reg. 40334 (June 29, 2000), codified at 17 C.F.R. Part 248. SEC, NASD, and NYSE Regulation regulate broker-dealers by, among other things, examining their operations and reviewing customer complaints. SEC evaluates the quality of NASD and NYSE oversight in enforcing their members' compliance with federal securities laws through self-regulatory organization oversight inspections and broker-dealer oversight examinations. SEC is the primary regulator of investment companies and investment advisers registered with the SEC.

[78] 17 C.F.R. § 248.30.

[79] An examination finding would be any compliance deficiency (including an internal control weakness) or violation requiring corrective action.

[80] NASD Notice to Members 00-66 (September 2000).

[81] NASDR Regulatory and Compliance Alert (Summer 2001).

[82] NYSE Information Memoranda Nos. 01-10 (June 19, 2001) and 01-13 (June 21, 2001).

[83] 15 U.S.C. § 6805(a)(6). State insurance authorities may enforce GLBA and may establish privacy regulations. However, GLBA mandates that state insurance authorities establish standards for safeguarding customer information and that the standards be implemented by rules. 15 U.S.C. §§ 6801(b) and 6805(b)(2). Moreover, if a state insurance authority fails to adopt regulations to carry out GLBA's privacy and safeguarding provisions, the state forfeits its eligibility under GLBA to override certain customer protection regulations promulgated by the federal depository institution regulators applicable to insurance sales by or at depository institutions. 15 U.S.C. § 6805(c).

[84] We did not corroborate or independently verify NAIC's analysis.

[85] GAO, Financial Privacy: Status of State Actions on Gramm-Leach-Bliley Act's Privacy Provisions, GAO-02-361 (Washington, D.C.: Apr. 12,

2002).

[86] District of Columbia, Department of Insurance, Securities and Banking, Preliminary Report: Status of Insurance Industry Practices and Procedures to Protect the Privacy of Customer Information (September 2005). According to department staff, the final report is pending. The staff said the preliminary and final results should not differ because the preliminary results included responses of more than 90 percent of the companies, including all of the large companies.

[87] FTC's GLBA and FCRA regulations can be found at 16 C.F.R. Parts 313 and 314 and 16 C.F.R. Parts 600 through 698.

[88] FTC v. 30 Minute Mortgage, Inc., No. 03-60021-CIV (S.D. Fla. 2003); FTC v. Sainz Enterprises LLC, No. 04WM-2078 (CBS) (D. Co. 2004); In the Matter of Superior Mortgage Corp., F.T.C. No. 052-3136 (2005); In the Matter of Sunbelt Lending Servs., FTC No. C-4129 (2005); In the Matter of Nationwide Mortgage Group, Inc., F.T.C. No 9319 (2005); FTC v. Nat'l. Consumer Council, Inc., No. SACV04-0474CJC (JWJX) (C.D. Cal. 2005); FTC v. Debt Mgmt. Found. Serv., Inc., No. 8:04-cv-01674-EAK-MSS (M.D. Fla. 2005). A consent agreement does not constitute an admission of a violation of law.

[89] See 12 U.S.C. § 1867 (FRB, FDIC, and OCC); and 12 U.S.C. § 1464(d)(7) (OTS).

[90] In January 2006, we reported on contractors' access to and sharing of Social Security numbers and federal oversight of regulated entities that contract for services. See GAO, Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs, GAO-06-238 (Washington, D.C.: Jan. 23, 2006).

[91] NCUA had temporary authority to examine third-party service providers under the Examination Parity and Year 2000 (Y2K) Readiness for Financial Institutions Act, Pub. L. No. 105-164, 112 Stat. 32 (Mar. 20, 1998) but that authority expired as of December 31, 2001. 12 U.S.C. § 1786a(c) and (f).

[92] GAO, Credit Unions: Financial Condition Has Improved, but Opportunities Exist to Enhance Oversight and Share Insurance Management, GAO-04-91 (Washington, D.C.: Oct. 27, 2003).

[93] NASD Notice to Members 05-48 (July 2005).

[94] NASD Notice to Members 05-49 (July 2005).

[95] SR-NYSE-2005-22, Proposed Rule 340, Outsourcing: Due Diligence and Conditions in the Use of Service Providers, and Proposed Amendments to Rule 342, Offices - Approval, Supervision and Control (Mar. 16, 2005).

[96] See Testimony of the Federal Trade Commission before the Senate Committee on Science, Commerce, and Transportation at p. 7, available at [Hyperlink, <http://www.ftc.gov/opa/2005/06/datasectest.htm>].

[97] Id. at p. 9, n.18.

[98] To date, the Commission has brought 13 legal actions against entities that allegedly failed to implement reasonable and appropriate data security for sensitive consumer data. See [Hyperlink, <http://www.ftc.gov/privacy/index.html>].

GAO's Mission:

The Government Accountability Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony:

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone:

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office

441 G Street NW, Room LM

Washington, D.C. 20548:

To order by Phone:

Voice: (202) 512-6000:

TDD: (202) 512-2537:

Fax: (202) 512-6061:

To Report Fraud, Waste, and Abuse in Federal Programs:

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470:

Public Affairs:

Jeff Nelligan, managing director,

NelliganJ@gao.gov

(202) 512-4800

U.S. Government Accountability Office,

441 G Street NW, Room 7149

Washington, D.C. 20548: