Board of Governors of the Federal Reserve System

Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud

Submitted to the Congress pursuant to section 2422
of the Economic Growth and Regulatory Paperwork Reduction Act
of 1996

March 1997

FEDERAL RESERVE BOARD REPORT CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD

I. Introduction

The availability of sensitive consumer identifying information became an issue of concern for the Congress in the summer of 1996 after a widely-publicized incident in which a large reference service offered for sale personal information about consumers, including Social Security numbers, from one of its electronic databases.[1] At about the same time, the Federal Trade Commission held hearings regarding privacy and the misuse of personal identifying information by third parties; and a number of newspaper and magazine articles discussed the increased use of this information for illegal purposes. In light of these concerns, the Congress directed the Board of Governors of the Federal Reserve System to conduct a study concerning the availability to the public of sensitive identifying information about consumers, whether such information could be used to commit financial fraud, and if so whether there is an undue potential for risk of loss to insured depository institutions.[2] The Congress instructed the Board to submit its findings within six months, including any recommendations for legislative or administrative action that the Board determines to be appropriate.

---

[1] The reference service has since discontinued the practice of making Social Security numbers available, but continues to permit subscribers to search for information about consumers by their Social Security number.

[2] The Consumer Credit Reporting Reform Act of 1996, Pub. L. No. 104-208, §2422, 110 Stat. 3009 (1996).

The Board has gathered information for this privacy study in various ways. First, it issued a press release and published a request for comment in the Federal Register.[3] The Board asked members of the public to address specific questions concerning the availability and use of sensitive identifying information for financial fraud. In response, it received more than 100 letters from consumers, financial institutions, information providers, privacy advocates, private investigators, trade associations, and government agencies. Second, the Board's staff held discussions with representatives from direct marketing and information industry trade associations, reference service providers, credit bureaus, and public-interest privacy groups. The Board also consulted with the Federal Trade Commission and the federal financial institutions regulatory agencies. Third, the staff reviewed prior studies conducted by other federal agencies, industry and privacy group statements to federal agencies, trade association guidelines and studies, privacy group discussion papers, and scholarly works. This report contains the results of the Board's findings.

Issues of privacy touch on some of the most fundamental individual freedoms that have grown out of the American experience. It is privacy, in a broad sense, that nourishes individual conscience, provides the foundation for family, friendships, and associations, and assures individuals the right to be secure in their persons, homes, papers, and effects. Yet at the same time, it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy. Reconciling these sometimes competing interests requires balancing the individual's legitimate expectation of privacy with the information needs of business and government, for

---

[3] 61 Federal Register 68,044 (December 26, 1996).

example, to administer the laws and provide for public safety. Striking the proper balance between a desire for absolute privacy and a legitimate need for access to information, even if it intrudes into personal matters, is an old and troubling dilemma. This problem has been made more immediate by the dramatic pace of technological change and its capacity to significantly increase the dissemination of personal information about individuals.

Privacy in all its manifestations is a subject that raises many complex and difficult public policy issues, and numerous efforts have been undertaken or are underway to study these questions in other forums.[4] The charge from the Congress for the Board's study is narrow: it is to consider the availability of sensitive identifying information about consumers, whether that information could be used to commit financial fraud, and if so whether there is an undue potential for risk of loss to insured depository institutions. Given this focused charge, the limited time for conducting the study, and the ongoing work of numerous other governmental bodies, the Board's contribution to the privacy policy debate will be similarly narrow in scope. The report explains how information becomes available, and discusses some aspects of financial fraud, but provides no conclusions about whether legislation is needed at this time.

Even in a study as narrow as this one, however, it is useful to consider how the information industry operates as a whole. Thus, Part II of the report begins with a broad

---

[4] For example, the Federal Trade Commission recently announced that it will conduct a study concerning the types of information that consumers perceive to be sensitive, as well as their level of concern regarding the access to such information. 62 Federal Register 10,271 (March 6, 1997). The Commission will hold at least one public workshop focusing on the types of information available from computer databases. At the conclusion of the study, the Commission will report its findings to the Congress. (See Appendix A for a list of recent government studies).

look at the information industry, including what information is available about consumers, the sources of that information, and the ways in which the information may be used by third parties. Part III examines what constitutes sensitive identifying information, how much information is publicly available, and the risk of fraud associated with its availability. The conclusion in Part IV highlights some important issues related to fraud and consumer identifying information, which may assist the Congress in considering these matters.

II. Overview of the information industry

Information about a consumer -- everything from age and address to favorite breakfast cereal -- has value. How valuable the information is depends in part on how descriptive it is and how it can be used. For example, knowing that a person has recently purchased a home and knowing the amount of the mortgage loan that secures the home may be quite valuable information to a financial institution offering home-secured credit products, but is unlikely to be of particular use to a direct marketer selling tennis equipment. The more descriptive or unique the information is, the more uses it likely has and thus the more valuable it is likely to be. A person's Social Security number, for example, may be useful not only to a credit card company (to help verify the applicant's identity) but also as to a direct marketer (to ensure that only one solicitation is sent to each person). Yet this same information, standing alone, may have little value since, for example, a Social Security number does not convey information about a person's characteristics, interests, buying habits, etc. Because information has value, value that may be increased through aggregation with other data, its collection and use has been commercialized through development of an information industry.

A. The information industry participants

Fundamentally, there are three distinct participants in the information industry -- government entities (federal, state, and local), direct marketers, and reference services. Typically these participants both gather and distribute personal identifying information. In many instances, the information may be gathered for one purpose, then sold and used for another. For example, a consumer may need to provide the county recorder of deeds information about the purchase price of a home and the identity of any lien holder in order to have the title recorded. The county may then sell this information, or provide it for free, to members of the public, including direct marketers and reference services. A direct marketer might merge the information from county recorders with other information, such as a list of subscribers to a home furnishings magazine, to develop a targeted mailing list for household related products and services. A reference service might take the same information from county recorders and sell it as part of a broader database that can be searched by the person's name or address.

1. Governmental entities

Federal, state, and local governments are sources of vast amounts of information about consumers and businesses. Public records are generally available to anyone, and contain information such as name, address, and spouse's name. Examples of these records include:

- Drivers' licenses[5]
- Driving records
- Marriage and divorce records
- Motor vehicle title and registration
- Vital statistics
- Voter registration records
- Political contributions records
- Firearms permits
- Property tax records
- Land records
- Filings with the Securities and Exchange Commission (SEC)
- Court and law enforcement records
- Postal service address records[6]
- Boat, aircraft, and other vehicle titles
- Financial and ethics disclosures
- Occupational and recreational licenses

These records often can provide extensive information such as race, gender, date of birth, date of marriage, date of divorce, and professional license number or place of business, as well as information related to bankruptcies and asset holdings. For example, information in land records typically includes property address and description, dates of sales, sales prices, size of mortgages, and sellers' and purchasers' names.

Copies of these records are usually available for a nominal fee. Some public records, such as SEC filings, are available free of charge. Public information can be accessed in a

---

[5] Currently, a significant amount of information about an individual can be obtained from drivers' license records. Those records make available in one place a consumer's name, address, height, weight, gender, eye color, date of birth, Social Security number, and any visual impairments. Access to this information will be somewhat more limited beginning in September 1997 when the Driver's Privacy Protection Act of 1994 goes into effect. The law will give individuals ways to control whether certain information can be released, such as through the use of "opt-outs." 18 U.S.C. §§2721-2725 (1994).

[6] The Postal Service provides, for a fee, national change of address files to a number of companies (such as the direct marketing and credit reporting industries). Prior to 1995, the Postal Service provided this information to any person willing to pay the fee. (59 Federal Register 67,223 (December 19, 1994).)

number of ways including by bulk purchase on magnetic tape, in person, by telephone, by facsimile, and, increasingly, over the Internet.

2. Direct marketers

According to a 1996 Gallup poll, 77 percent of commercial firms in the United States use direct marketing to inform consumers about products and services by telephone and mail (including e-mail). A wide variety of other organizations also use direct marketing. Educational, professional, political, and nonprofit organizations use direct marketing, for example, to raise money, recruit new members, and alert consumers to issues important to the organization. To determine who should be solicited for a particular product, service, or fundraiser, direct marketers rely on lists that are designed to target individuals who are likely to respond to the solicitations. For example, people who have purchased household items from a home furnishings mail-order catalog might be a good market for a furniture store's credit card.

The descriptive lists that direct marketers use may be broad -- such as individuals age 35 and older -- or narrow -- such as persons who have donated to Alzheimer's disease prevention and research organizations. The lists may be created from information that direct marketers have obtained from consumer surveys, warranty or response cards, and customer purchase data (such as information gathered when a consumer purchases a catalog item over the telephone). The lists may also be merged with other lists or with information that the direct marketer obtains from other sources, such as public records or magazine subscription lists.

Frequently, direct marketers use preexisting lists from a list broker that handles many different kinds of lists. Typically, list information is not sold, but is "rented" for a limited number of uses and for specific identified solicitations. List brokers make available thousands of types of lists by grouping information such as similar interests, characteristics, and purchasing habits of the population. List brokers derive information from numerous sources.[7] There are no federal restrictions on who can rent a list or the purposes for which the list may be used. The cost of renting a list varies depending on factors such as the number of addresses on the list and the amount of information conveyed about the people on the list. Lists can range in price widely, generally anywhere from $35 to $250 per thousand names.

3. Reference services

Reference services offer "one-stop shopping" for anyone looking for information about a person. These services gather in one place a variety of facts. For example, one Internet reference service sells what it calls a "comprehensive dossier report." The service provides the name, age, date of birth, Social Security number (including the state and date of issuance), any alias, current and previous address, and telephone listing, as well as the names, telephone numbers, and addresses of relatives and neighbors. The information sold by the company comes from public records and other information providers.

---

[7] For example, common sources for information include surveys, public records, warranty and response cards, mail-order or other customer purchase data, professional or other membership associations, magazine subscription lists (current and past), and attendance records for conferences.

Consumer reporting agencies are a source of detailed information about a person's financial life: employer, credit card and loan account numbers, amount of available credit, amount of outstanding debt, payment histories, and default, judgment and bankruptcy information. Under the Fair Credit Reporting Act (FCRA), however, consumer reporting agencies are prohibited from disclosing these consumer reports to anyone who does not have a permissible purpose. (See Appendix B for further discussion of consumer reporting agencies and the FCRA.)

Consumer reports also contain identifying information about consumers often called "header information," that is not so restricted. Header information includes name, current and previous address, any alias, date of birth, and Social Security number. Consumer reporting agencies are free to sell this header information. Neither the FCRA nor any other federal law regulates how or to whom the information may be provided, unlike other financial information in the consumer report (such as repayment history on a loan). Reference services often get information by purchasing credit headers that are then put in a searchable database and sold to businesses or other organizations wanting to find out specific information about a person. Often, the reference service will also have merged information from public records with credit header information, so that it can provide more detailed information about a person.

Common users of reference services include law firms, private investigators, and local, state, and federal law enforcement agencies. There are generally no federal laws restricting who can access information through a reference service (or the purposes for which the information may be used), although some services provide certain information only to

licensed private investigators and law enforcement officials. Reference services may require persons using the service to be subscribers and may monitor usage to detect any significant changes in use. Some may conduct a "background" check on potential users -- for example, to verify that the person has a legitimate purpose for obtaining the data. Other providers place few, if any, restrictions on access or intended use of information, and may permit immediate access over the Internet.

The price for information depends upon a number of factors including how detailed the information is, how quickly it can be provided, and how frequently the purchaser uses the service. Simple requests for information about an individual can cost as little $2 while more detailed information can cost $100 or more; some services may charge a fee to subscribe to and access the service as well as a fee for on-line time.

B. The information marketplace

Information about a consumer can make its way into the marketplace in a number of ways and, once there, can be sold repeatedly for many different uses. The information marketplace can be thought of as two distinct markets: a primary market, where information flows from the original source (the individual) to the primary source (the entity that collects the information directly from the individual); and a secondary market, where the information is sold by the primary source to secondary sources that then sell or use the information themselves.

1. The primary market

The original source for any personal identifying information is the consumer, who provides information in a variety of ways. For example, the consumer may be required or requested to provide information to a primary source (such as a retailer) in order to transact business. To make a purchase (even in cash) some retailers ask the consumer to provide an address or telephone number. To make the same purchase by check, the consumer may be asked to provide the retailer with an address, telephone number, and a driver's license or credit card number.

In some cases a consumer may believe that providing the information is necessary to obtain a benefit. Warranty registration cards, often included with the purchase of household appliances, are a good example of this. The card may indicate that the consumer should complete and return the card to put the warranty coverage in place, when typically the sales receipt or other proof of purchase may be all that is needed to ensure that the product is covered by the warranty. Thus, "warranty" cards are usually designed more for obtaining information about the consumer, such as household income and family size, than for warranty purposes.

There are other ways in which the consumer may provide information to the primary source without realizing that the information will be used for a purpose other than the one that the consumer intended. For example, when a consumer purchases an item from a catalog over the telephone, some information is necessary to ensure that the correct merchandise is sent to the right address. What the consumer may not realize, however, is that the date, specific item purchased, means of payment, and other information may be

retained in a database that the company rents to other direct marketers or uses for its own direct marketing purposes. Similarly, information may be retained from a variety of consumers' activities including subscribing to magazines, requesting information from companies, joining professional or other associations, and making donations to political or nonprofit organizations.

The growth in consumers' use of the Internet to visit sites on the World Wide Web ("the Web") has created the potential for additional accumulation of information. Web sites can obtain e-mail addresses, the name of the visitor, and other information.[8]

The government too collects consumer data in a variety of ways. For example, to obtain a drivers license an individual typically must provide the state licensing bureau with name, address, height, weight, gender, eye color, any visual impairments, and Social Security number. This information allows the state to keep an accurate file on the individual for driving related purposes (renewal notices, accident records, etc.) Currently, many states will provide this information to the public or businesses free of charge, or for a nominal fee.[9]

2. The secondary market

Once information leaves the individual's control, the primary source can offer it for sale to secondary sources that will package and sell it. With the development of new

---

[8] Consumers can also be requested to complete questionnaires to visit a particular web site that, just like a paper or other form of questionnaire or survey completed by the consumer, can provide identifying information.

[9] As discussed earlier, the Driver's Privacy Protection Act of 1994, which goes into effect in September 1997, requires that consumers be able to "opt-out" if they do not want this information provided to direct marketers and others who purchase such information in bulk. 18 U.S.C. §§2721-2725.

technologies the costs of collecting, duplicating, updating, storing, and accessing data have plummeted. Information such as property tax records can now be obtained in a matter of seconds or minutes rather than hours or days.

Technology also makes it possible for a secondary source to bring together in one place information that otherwise would be held by primary sources in several different locations. Previously, for example, one had to go to the state registrar's office to find someone's date of birth and birthplace, the county clerk's office to find a person's date of marriage and spouse's name, and the county recorder's office to find out real property ownership. Now, all this information and much more can be obtained from a single source on the Internet from one's home or office computer. As the information is compiled, combined, and edited by secondary sources in new and different proprietary ways, it becomes more valuable.

An example will help illustrate how this market works. Say that a city has information on its employees, available to the public. For a relatively low price, anyone can buy the city's database containing the employees' names, home addresses, and salaries. Credit header information purchased from consumer reporting agencies can provide current and previous addresses, date of birth, Social Security number, and other information. Information about real property ownership can be obtained from county recorders' offices. By combining the city employee data with credit header data and property information, a new and far more detailed database on these city employees can be created for sale. This new database could be used -- along with other information -- for example, by a news reporter investigating city employees. It could also be purchased by a list broker, further merged

with other lists (such as subscription lists and political or nonprofit contribution lists) and sold to a direct marketer.

III. Publicly available data and risk of fraud

The specific questions asked by the Congress are whether there are information industry participants that make "sensitive information" available to the public; whether their activities create a potential for fraud; and, if so, whether there is an undue potential for risk of loss to insured depository institutions. This section discusses those questions in turn.

A. Defining sensitive information

The first part of the congressional mandate to the Board was to look at whether participants in the information industry "are engaged in the business of making sensitive consumer identifying information, including Social Security numbers, mothers' maiden names, prior addresses, and dates of birth, available to the general public."[10] In its request for public comment, the Board specifically asked commenters to identify what they believe constitutes sensitive information. Not surprisingly, there were widely varying answers, reflecting commenters' personal beliefs about what constitutes information that may be "sensitive."

1. What is sensitive information?

Some commenters suggested that sensitive information includes only those matters identified by the Congress -- Social Security number, mother's maiden name, prior addresses, and date of birth. Others believed strongly that the definition should be widened to include some or all of the following: place of birth, names of family members, names of schools attended, telephone numbers (listed and unlisted), employment information (past and present),

---

[10] Pub. L. No. 104-208, §2422, 110 Stat. 3009 (1996).

medical records, voter registration information, passport number, driver's license number, car registration, loan and credit card numbers, other financial account numbers, personal identification numbers (PINs), and insurance policy numbers.[11]

On the other hand, information that most commenters believed should be considered sensitive, such as Social Security numbers, was not seen by some commenters as sensitive because the mere numbers do not reveal anything about a person. For example, an information industry trade association asserted that Social Security numbers should not be considered sensitive because they appear on all sorts of documents, such as drivers' licenses (in some states), and are routinely provided by consumers in transactions as mundane as cashing a check.

A determination of what is sensitive information is largely subjective. What is sensitive in one context may not be sensitive in another. For example, a mother's maiden name may be considered valuable information, but not at all sensitive, in the context of genealogical research, while in a credit-granting process it may be both very important to verify a consumer's identity and sensitive. Similarly, information that one person considers not to be sensitive, because it reveals little, may be sensitive to another person. Thus, while a current telephone number may not be considered sensitive, or even private, to people who have their numbers listed in the local telephone directory, it may be highly sensitive for someone who has an unlisted number.

---

[11] Commenters suggested numerous other items that they considered sensitive information such as associations (including professional, social, military), telephone records, utility use records, and asset ownership. The Board also solicited comment on what sorts of information might be considered sensitive in the future. Among the items suggested were retinal scans, encryption keys, and digitized fingerprints.

2. Sensitive information for purposes of the study

For purposes of this study the Board has "defined" sensitive information by focusing on the information that appears to be most commonly used to commit financial fraud. The Board solicited comment on the specific types of information that are most often used in granting and verifying credit, since this is often the key to fraudulently obtaining credit. The items most often identified by the commenters included Social Security number, mother's maiden name, prior addresses, date of birth, employment information (including salary), and credit card, loan, and other financial account numbers. Commenters had significant concerns about the availability of any one of these pieces of information because of the ease with which additional pieces of information can be obtained once one piece is known. There was particular concern about the availability of Social Security numbers because they often are the best gateway to other information. There also was heightened concern about the availability of aggregations of this information, such as in credit headers. Commenters noted that it is possible to commit financial fraud so long as there is enough information to deceive a creditor about the perpetrator's true identity, even when the aggregation does not contain all of the data typically requested on a credit application.

B. Obtaining and using sensitive information for financial fraud

1. Sources and uses of sensitive information

Sensitive information about consumers can be obtained by a number of means, both lawful and unlawful. As discussed above, sensitive identifying information may be purchased from primary sources such as government databases, or from secondary sources such as reference services. While several federal laws regulate access to certain types of information,

there is no comprehensive federal law governing privacy or access to sensitive information.[12] And, there are few restrictions on who can access personal identifying information.

The exhibits in Appendix C illustrate some of the types of information that are available, and just how easy it can be to access. The first example in Appendix C is a copy of a state's marriage and divorce records that were accessed over the Internet at no cost. The next example in the appendix is a copy of information retrieved from a database search using a subscriber-accessed reference service (Reference Service A). Next is a partial list of searches advertised by a reference service on the Internet (Reference Service B). The last two examples illustrate the types of lists direct marketers purchase and use (Direct Marketing List A and B).

As the examples illustrate, information is readily available from a variety of sources. And while some information providers may verify whether the party buying the information has a legitimate purpose, there are information services that provide easy access over the Internet, without any real verification of the purchaser's use. Arguably, the cost of access to certain information may somewhat limit the likelihood of its being used for illegal purposes.

---

[12] Federal laws that specifically address privacy issues or access to information include: the Fair Credit Reporting Act, 15 U.S.C. §1681 (dealing with financial information in consumer reports), the Privacy Act of 1974, 5 U.S.C. §552 (dealing with information held by the federal government), the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §1232g (dealing with privacy rights for student records), the Right to Financial Privacy Act of 1978, 12 U.S.C. §3401 (dealing with protection of individuals' bank records), the Cable Communications Policy Act of 1984, 47 U.S.C. §521 (dealing with cable television subscriber information), the Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510 (dealing with electronic mail and voicemail communications), the Video Privacy Protection Act of 1988, 18 U.S.C. §2710 (dealing with video rental records), the Driver's Privacy Protection Act of 1994, 18 U.S.C. §2721 (dealing with information contained in state motor vehicle records), and the Telecommunications Act of 1996, 47 U.S.C. §153 (dealing with customer information held by telecommunications carriers).

However, it is clear that other information, which too might be used in financial fraud, is readily available.[13]

While the study focuses on legitimate data sources that may be used for "identity theft,"[14] unlawful access to sensitive information may often be the precursor to this type of fraud. For example, persons who have access to sensitive information through their employer

---

[13] In light of current industry practices, renting a list is likely not an effective way to obtain personal identifying information. First, direct marketers and other persons who purchase information from list brokers typically are not provided with the names and addresses of persons to whom a solicitation is sent. Usually, the renter of the list does not get physical control of the list; all mailings are done by a third party. (Often, the mailing label on the solicitation will include a code reference for the list.) Thus, a marketer can learn who is on the list only if a consumer responds to the solicitation and provides the code. Second, many brokers typically require the renter to give the list owner a copy of the intended solicitation to help ensure that the list is being used for lawful purposes. There appear to be a number of list brokers, however, that do not require list-purchasers to provide a copy of the intended solicitation before conducting the mailing. (In addition, some reference services advertise that they have access to mailing lists, and use that information when conducting searches for customers.)

[14] "Identity theft" typically refers to the illegal use of personal identifying information -- including name, address, Social Security number, financial account numbers, and birth date -- to commit financial fraud. One particular type of identity theft occurs when the criminal "takes over" a consumer's account, for example, by changing the consumer's address for an existing account or submitting a fraudulent credit application to open an account in the consumer's name, but giving a different address as the place to send the card. Even if the creditor tries to verify the identity of the applicant, the imposter may have sufficient information about the consumer to deceive the creditor. Once the address is changed or the new account opened, the consumer may not learn of the deception until the account becomes delinquent and the creditor begins a collections action, or until the consumer reviews a copy of his consumer report.

The number of ways in which a person can illegally obtain information that will enable fraud to be committed is virtually limitless. In addition, a person can obtain information without violating a law, but through questionable means. For example, sensitive consumer information may be obtained if a consumer carelessly discards credit card and checking account statements and other personal records.

(such as the Social Security numbers of colleagues or customers) have the capacity to use the information (or sell it to someone else) to commit identity theft or other financial fraud.

2. Losses associated with the use of sensitive information

Financial fraud can occur in many ways, such as obtaining a credit card under an assumed name, using another person's credit or debit card without authorization, applying for and receiving a loan using an assumed identity, or making unauthorized withdrawals or transfers from another person's checking or deposit account. While some financial institutions distinguish between losses due to fraud and overall losses, many others do not. As a result, there are little data on aggregate losses to insured depository institutions due to fraud.[15] There is, however, fraud loss information for particular products, such as credit cards and checks. For example, in 1995, gross fraud "charge-offs" for MasterCard and Visa credit and debit cards totaled $790 million, with total outstanding balances of $321 billion. (In 1994, gross fraud charge-offs for these products totaled $712 million, with total outstanding balances of $257 billion.)[16] In a recent report to the Congress, the Board estimated that losses due to check fraud for commercial banks, savings institutions, and credit unions totaled $615.4 million in 1995, less than 0.001 percent of the total value of checks deposited.[17] Fraud losses

---

[15] Some information is available on overall losses to the banking system. For 1996, insured commercial banks and savings institutions "charged-off" $21.5 billion. (Net charge-offs were $15.6 billion, after recovery of $5.9 billion.) This includes not only losses charged-off due to fraud, but all other amounts charged-off by these institutions. This does not include charge-offs by insured credit unions, uninsured financial institutions, and other businesses.

[16] American Bankers Association, 1996 Bank Card Industry Survey Report.

[17] Board of Governors of the Federal Reserve System, Report to the Congress on Funds Availability Schedules and Check Fraud at Depository Institutions (1996).

attributable to the use of sensitive information likely make up a very small portion of any of these figures.

Just as fraud is often not tracked separately from other losses by many financial institutions, losses due to identity theft (that is fraud from using sensitive identifying information) is often not tracked separately from other types of fraud. A few commenters provided rough estimates of fraud losses related to the use of sensitive information, but were able to provide only educated guesses, because they do not separate such loss from general losses due to fraud.[18] Thus, it is not possible to estimate losses solely due to the use of sensitive information in a reliable way. Although anecdotal information seems to suggest that this type of fraud is increasing, these losses likely play a relatively small role in overall fraud losses and pose no significant threat to insured depository institutions.[19]

IV. Conclusion

Information about consumers is widely available from both government sources and commercial services. Through technology, many databases can be merged to provide detailed information about consumers. These data have numerous legitimate purposes. Few legal constraints are currently in place regarding the collection, use, and dissemination of

---

[18] For example, a regional bank with $11 billion in assets suggested that fraudulent use of sensitive information might account for 30 percent of its total losses from fraud.

[19] While the Congress asked the Board to determine whether the availability of sensitive information poses an undue risk of loss to insured depository institutions, other parties may suffer losses due to fraud. For example, consumers risk some losses due to unauthorized use of credit or debit cards, though losses are limited by the Truth in Lending Act (15 U.S.C. §§1601-1666j) (1994) and the Electronic Fund Transfer Act (15 U.S.C. §§1693-1693r) (1994). Persons who accept credit or debit cards for the payment of goods or services also risk losses due to fraud. Similarly, the fraudulent use of checks can pose losses to both consumers and others. (See generally, Article 3 of the Uniform Commercial Code (1996).)

information about individuals. Some of this information is sensitive and can be used to facilitate illegal activities, including identity theft. There is little "hard" evidence on how fraud due to the usage of sensitive information occurs, the frequency with which it occurs, or the amount of associated losses. However, at present, losses attributed to identity theft do not appear to pose a significant risk to insured depository institutions. Nevertheless, fraud related to identity theft appears to be a growing risk for consumers and financial institutions, and the relatively easy access to personal information may expand the risk.

In considering whether any legislation is desirable, the Congress must carefully evaluate whether the availability of sensitive information poses a sufficient risk to consumers and institutions to justify new laws. Privacy interests should be balanced against the legitimate need for information by law enforcement agencies, businesses, and others in both the public and the private sectors. Care should be taken not to impair the flow of information that is crucial for legitimate purposes.

A number of commenters expressed concern that the consumer is often required to give up sensitive information in exchange for little benefit, without either adequate notice of how the information may be used or an effective means to control whether the information is released to secondary sources. Given the ongoing advance of technological changes, the need for individuals to be able to control confidential information to ensure it is not used for illegal purposes has taken on greater importance.

There are steps that financial institutions and consumers can take to limit the likelihood of fraud, even absent legislation. For example, commenters noted that one way to slow the growth of fraudulent financial activity is for financial institutions to tighten their security

growth of fraudulent financial activity is for financial institutions to tighten their security measures. Similarly, some commenters urged increased consumer education as another way to prevent fraud. (See Appendix D for a discussion of fraud prevention measures for both financial institutions and consumers.)

The Board's study has focused on the availability of sensitive identifying information in terms of a commodity that can be bought and sold and that can facilitate illegal activity. But a number of the commenters viewed the issues more broadly. Most commenters stated their belief that legislation is not needed, suggesting that regulation would infringe on a basic right to information. Other commenters argued as strongly that legislation is necessary to protect an individual's basic right to information privacy. The debate about fundamental rights and information is a critical one, but to date the jurisprudence in this area is relatively undeveloped.[20] These matters will be debated in the numerous other government forums examining privacy concerns, which may provide further guidance to the Congress.

---

[20] To date, the Supreme Court does not recognize a constitutional right to information privacy, or a constitutional right of access to information. Compare, Whalen v. Roe, 429 U.S. 589, 606 (1977) (Stewart, J., concurring, "Whatever the ratio decidendi of Griswold, it does not recognize a general interest in freedom from disclosure of private information.") with, Houchins v. KQED, Inc., 438 U.S. 1, 15 (1978) ("Neither the First Amendment nor the Fourteenth Amendment mandates a right of access to government information or sources of information within the government's control.") See also, Arizona v. Evans, No. 93-1660, 1995 U.S. LEXIS 1806, at *1838 (U.S. March 1, 1995) (1995) (Stevens, J., dissenting, noting "the reality that computer technology has changed the nature of threats to citizens' privacy over the past half century.")

Appendix A

List of Recent Government Studies Addressing Privacy Issues

In addition to several studies by private entities (including industry, privacy groups, educational institutions, etc.) there are a number of recent federal government studies dealing with a wide array of privacy issues. The following list is a sample of studies issued since 1995.

Department of Commerce and other governmental agencies, National Information Infrastructure Task Force, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (June 1995).

Department of Commerce, National Technical Information Service, Freedom of Information and Privacy (February 1995).

Department of Commerce, National Telecommunications and Information Administration, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (October 1995).

Federal Trade Commission. Forthcoming study on the collection, compilation, sale and use of data from computer databases. A workshop on consumer privacy issues to be held in June 1997, will gather information for the study.

Federal Trade Commission, Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure (December 1996).

General Accounting Office, U.S. Postal Service Improved Oversight Needed to Protect Privacy of Address Changes (August 1996).

National Research Council, Computer Science and Telecommunications Board, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, FOR THE RECORD Protecting Electronic Health Information (March 5, 1997, Prepublication Copy).

National Research Council, Computer Science and Telecommunications Board, Committee to Study National Cryptography Policy, Cryptography's Role in Securing the Information Society (1996).

Appendix B

Consumer Reports, Consumer Reporting Agencies and the Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) regulates the credit reporting industry, places certain responsibilities on users of consumer reports, limits the circumstances in which consumer reporting agencies (CRAs) may provide consumer reports to businesses and other persons, and requires CRAs to investigate consumer report information the consumer claims is inaccurate or incomplete.[21]

Consumer reporting agencies (sometimes called credit bureaus) are companies that collect and sell credit information about consumers. A consumer report contains identifying information, credit information, public record information and inquiries. Identifying information includes the consumer's name (and any prior name), current and previous address, birth date and Social Security number. The report may also include a person's current and previous employers and other information. Consumer reports contain credit information, including accounts with banks, retailers, credit card issuers, and other lenders. The report lists accounts by type, opening date, credit limit and current debt, payment histories, and other information. The report also provides public record information, which includes records concerning bankruptcy, tax liens and judgments. Finally, the report lists

[21] 15 U.S.C. §§1681-1681t (1994). Extensive amendments were made to the FCRA in September 1996, which generally become effective September 30, 1997. Pub. L. No. 104-208, §§2401-2422, 110 Stat. 3009 (1996). Several of the changes to the FCRA seek to provide greater privacy rights to consumers, for example, by giving consumers the right to "opt-out" of certain solicitations. However, one provision of the law (§2416) might significantly weaken consumer protections because it generally prohibits federal agencies from examining whether banks, savings associations, and credit unions have complied with the law.

inquiries, including the names of parties who have recently obtained copies of the consumer report.

Banks, finance companies, merchants, credit card companies, and other creditors regularly send credit information on their customers to CRAs. This includes the type of credit extended, the amount and terms of the credit and payment history.

Appendix C

Samples of Available Consumer Identifying Information[22]

Information from the Government

Sample State Government Information[23]

Marriage Index File Retrieval:

Groom: John Adams
Groom Race: White
Groom Residence (County): Monroe
Bride: Cindy Jones
Bride Race: White
Bride Residence (County): Jefferson
Date of Marriage Certificate: 11-02-93
County of Marriage: Jefferson

Divorce Index File Retrieval:

Husband: George Smith
Husband Race: White
Husband Residence (County): Putnam
Wife (maiden name): Linda Grant
Wife Race: White
Wife Residence (County): Putnam
Year of Marriage: 1971
County of Marriage: Putnam
Date of Divorce: 06-12-90
County of Divorce: Putnam

[22] Due to the sensitive nature of this information, the actual names, addresses, telephone numbers, etc., in these samples have been redacted and replaced with fictitious ones.

[23] This information can be obtained on the Internet, free of charge. The state providing this information notes that the information may not be used for any commercial purpose, including reselling the information.

Information from Reference Service A

Georgia Real Property Ownership Search By Name

Search Criteria: SMITH JANE

Owner(s):	SMITH JOHN C & JANE L
Mailing Address:	1234 Mulberry Ave Macon Ga 98765-4321
Property Address:	1234 Mulberry Ave Macon Ga 98765-4321
Owner(s) Phone No.:	---
Parcel No.:	1111111111
County:	BIBB

Sale Information: **Assessor Information:**

Sale Date:	01/10/1996	Exemption(s):	---
Document No.:	22222	Tax Amount:	$1,432
Sale Amount:	$142,000	Assessed Value:	$142,000
Sale Full/Part:	FULL	Percent Improved:	55.5%
Loan Amount (1st):	$20,000	Year Sold to State:	---
Loan Amount (2nd):	$15,692	Map Page Old:	AA
Loan Type:	CONVENTIONAL	Map Grid Old:	8F
Multi or Port:	---	Map Page New:	3333
Lender:	SELLER	Map Grid New:	E
Interest Rate Type:	FIXED	X Coordinates:	4.444
Transaction Type:	RESALE	Y Coordinates:	55.555
Census Tract:	7777.77	Census Block:	9
Tract Number:	6666	Lot Number:	777
Zoning:	R		

Property Characteristics:

Land Use:	SINGLE FAMILY RESIDENCE	Number of Units:	1
Lot Size:	6,100	Square Feet:	1376
Lot Width:	---	Bedrooms:	3
Year Built:	1961	Garage:	YES
Legal Description:	LOT II 3	Last Transaction Dt:	01/10/1996

Most Recent Information:

Transaction Type:	RESALE
Deed Type:	GRANT/TRUST DEED
Transaction Date:	01/10/1996
Document No.:	88888
Transaction Value:	$36,000
Buyer(s) Name:	SMITH JOHN C & JANE L
Seller(s) Name:	FRANK S JONES TRUSTEE
Lender Name:	SELLER
Loan Amount (1st):	$20,000
Loan Amount (2nd):	$15,692
Sale Full/Part:	PARTIAL
Interest Rate Type:	FIXED
Transaction Type:	RESALE
Deed Type:	GRANT/TRUST DEED
Transaction Date:	01/15/1993
Document No.:	33333
Transaction Value:	$134,000
Buyer(s) Name:	JONES FRANK S
Seller(s) Name:	TAYLOR DAVID A
Lender Name:	GUARANTEE BANK
Loan Amount (1st):	$107,200
Sale Full/Part:	FULL
Title Company:	FRANKLIN TITLE
Transaction Type:	REFINANCE
Deed Type:	GRANT/TRUST DEED
Transaction Date:	01/29/1991
Document No.:	11111
Buyer(s) Name:	TAYLOR DAVID A
Lender Name:	BANK OF BIBB
Loan Amount (1st):	$146,519
Title Company:	AMERICA TITLE
Transaction Type:	REFINANCE
Deed Type:	GRANT/TRUST DEED
Transaction Date:	02/26/1990
Document No.:	222222
Buyer(s) Name:	TAYLOR DAVID A
Lender Name:	UNITED STATES FINANCIAL
Loan Amount (1st):	$22,720
Title Company:	LOST TITLE

Information from Reference Service B

SAMPLE SEARCHES AVAILABLE

1. Social Security number tracing. Provides all names, current address and former addresses linked with social security number.

2. National Dossier. Provides addresses, Social Security and telephone numbers, neighbors' names, addresses and telephone numbers. Search by name and address.

3. Neighbor Search. Provides nine nearest neighbors to address being searched. Includes names, address, phone number, and length of residence.

4. Motor Vehicle/Driver's License Reports. Provides driving records (including suspensions, tickets, etc.), tag number, driver's license, vehicles owned, etc. (Some states have restrictions.)

5. Income/Ownership Demographics. Provides name, birth date, gender, length of residence, etc. Also provides median family income, approximate home value, etc.

6. Worker's Compensation Claims. Provides accident date, type, employer. (Some states have restrictions.)

SAMPLE STATE SEARCHES

1. New York Profile. Provides address, gender, telephone number, household occupants, Social Security number, neighbors' names and addresses, etc. Search by name or address.

2. Florida Search. *Handicap parking permit holders.* (Provides address, license number, issue date, etc.) *Teachers.* (Provides address, school name and address, hiring date, etc.) *Boat Registration.* (Provides address, lien holder, previous owner, etc.) *Professional licenses.* (Provides information about persons for over 150 categories of professional licenses issued.)

3. Texas Voter Registration. Provides address, date of birth, voter certificate number, precinct, and county.

Information from Direct Marketing List A

1. LIST MANAGER

The Experts, Inc.
3950 Ridge Ave. 9th Floor
Chicago, IL 99999
Phone: (111) 333-3333. Fax (111) 333-3334

2. DESCRIPTION

List of senior citizens, sorted by state, ZIP code, gender, etc.

3. QUANTITY AND RENTAL RATES

	Number	Price per Thousand
Total list	25,152,833	$50.00
Household income:		
Under 15,000	4,245,021	+5.00
15,000-19,999	2,518,457	"
20,000-29,999	4,165,936	"
30,000-39,999	. . .	"
40,000-49,999	2,906,539	"
50,000-74,999	4,363,608	"
75,000-99,999	1,808,662	"
100,000-124,999	1,035,692	"
125,000+	621,450	"
Affluent investors:		
Millionaires	158,509	"
Multimillionaires	9,063	"
Investors	584,982	"
Hardcore investors	466,185	"
Speculative investors	48,262	"
CD holders	139,861	"
Mail order buyers:		
Catalog	787,224	"
Merchandise	2,347,181	"
Women's Apparel	35,309	"
Crafts & sewing kit	285,057	"
Stamp, coin collectibles	468,048	"
Children's reading	63,412	"
Health, fitness, exercise	227,146	"
Entertainment	145,168	"
Books & music	3,153,586	"
Donors:		
Political	386,974	"
Religious	362,909	"
Health	77,951	"
Environment	1,020,811	"

Information from Direct Marketing List B

1. LIST MANAGER

ABCD List Management.
95 Reading Dr., Further, NY 99999-9999.
Phone: (333) 666-6666. Fax: (333) 666-6667.

2. DESCRIPTION

Selections available: age, bank card holders, children by age, dwelling type, education, ethnic, income, length of residence, marital status, occupation, retail card holders, sex, state, ZIP code, phone numbers (not available on all lists), etc.

3. LIST SOURCE

Public records, surveys, direct mail, credit information.

4. RESTRICTIONS

Sample mailing piece required for approval.

5. QUANTITY AND RENTAL RATES

	Number	Price per Thousand
Total list	84,572,290	$50.00
Mail responsive	47,657,140	+10.00
Credit card holders	51,931,000	“
African Americans	6,763,400	“
Blue collar workers	13,565,780	“
Dual income families	17,519,690	“
Empty nesters	17,411,110	“
Equity homeowners	13,235,700	“
Families w/children	19,173,060	“
Female-headed families	8,216,580	“
High income families	30,174,430	“
Hispanic Americans	5,671,430	“
Homeowners	70,108,590	“
Luxury car buyers	3,602,720	“
Metropolitan elite	7,780,140	“
Professionals at home	7,518,600	“
Recent movers	21,597,010	“
Retirees age 65	17,838,020	“
Seniors-age 50+ w/exact age	27,827,540	“
Separated, divorced, widowed	9,252,040	“
Single parent families	7,592,120	“
Single people	19,836,920	“
Ultra high income families	9,435,890	“
White collar workers	13,367,380	“
Working women	14,618,360	“

Appendix D

Fraud Prevention Measures Suggested by Commenters

Measures Financial Institutions Can Take

Theft of personal information, such as that in a credit card renewal notice, may occur at any point in the processing or distribution of the renewal notice, including when the notice and card are processed at a financial institution, handled at the postal office, or delivered to the consumer's mailbox. This information may then be used to commit financial fraud. Commenters suggested that financial institutions may use a number of security measures to control losses and stem fraud. Identifying consumers and verifying eligibility for credit using photo identification, Social Security number, current address, a personal identification number (PIN), or a signature are examples of some methods currently used. Other institutions reduce the incidence of fraud by limiting the number of employees with access to sensitive information.

Commenters noted that credit card issuers design the delivery and activation of credit cards to minimize losses. For example, when a card issuer sends a renewal notice and replacement card to a consumer, the consumer may be asked to call a toll-free telephone number to activate the card. The card issuer may use a variety of means to ensure that the consumer calling is the one reflected in the issuer's records. After an account is opened, financial institutions many review and analyze an account to identify and closely monitor unusual purchase habits which may signal unauthorized use of the card.

Commenters stated that there are also new, emerging technologies that may help financial institutions protect the security of consumer information and reduce fraud. One

example is biometric encryption. Biometric encryption is the process of using a physical characteristic -- such as the pattern in a fingerprint -- to code or "scramble" data. Because each fingerprint is unique, the way in which the data is scrambled is also unique. This makes the data both secure and private because only the person's finger pattern can unscramble the data.

Fingerprint-imaging systems, with or without encryption, are the most frequently used fraud prevention programs based on biometrics. Other new biometric products include retina and iris scanners, and voice recognition technologies. Pilot programs using these new technologies are currently underway, but thus far have not gained widespread use in financial institutions.[24]

Measures Consumers Can Take

A number of commenters stressed the need for increased consumer education as a way to both combat fraud, and to help consumers gain control over personal identifying information. In particular, commenters suggested four areas where consumers might benefit from additional education:

What happens with identifying information?

As discussed in the body of the study, the information consumers provide to government agencies, businesses and other organizations may be shared with other entities. Commenters noted that consumers might benefit from knowing how and why information about them may be shared. With a better understanding of how personally identifiable

---

[24] See, for example, Moyer, Liz, "Going Digital -- with Fingerprint ID," The American Banker (March 5, 1997); O'Sullivan, Orla, "Biometrics Comes to Life," ABA Banking Journal (January 1997).

information flows from one source to another, consumers can make choices about what information they provide, to whom, and under what circumstances.

How can consumers control the identifying information they provide?

There are a number of things consumers can do if they wish to limit identifying information about them in the marketplace. The best way to control identifying information is to limit who and under what conditions information is provided to other persons. For example, one way to control personal information is by not providing it on "warranty" cards or product surveys.

In addition, consumers can ask businesses or other organizations to whom they provide information not to share that information with others. Furthermore, consumers can contact the major credit bureaus and direct marketing trade associations to request that the consumer's name be dropped from mailing lists. "Opting-out" allows consumers to choose whether the information they provide can be released to secondary sources, such as direct marketers and reference services.[25]

[25] Many businesses and other organizations permit consumers to have their name and address removed from lists the business may rent to other parties. In addition, industry trade associations, such as the Direct Marketing Association (DMA) seek to provide opportunities for consumers to have their names removed from multiples businesses that use list for direct marketing mailings. For example, the DMA maintains a Mail Preference Service that enables consumers to receive less advertising mail. (The DMA also maintains a Telephone Preference Service that enables consumers to receive fewer home telephone solicitations.) In addition, both the DMA and other associations, such as the Information Industry Association, have established fair information practices guidelines for their members.

What can consumers do to prevent fraud and identity theft?

Consumers can limit the fraudulent use of sensitive information by a number of means. Consumers should exercise reasonable care when disposing of materials that contain sensitive information -- such as pay "stubs," credit card receipts, and bills or periodic account statements that contain account numbers or a Social Security number. In addition, consumers should not provide personally identifying information (such as credit card or other account numbers, or a Social Security number) to other persons unless they have an established relationship with the entity requesting the information, or they otherwise know the entity is legitimate.

To check for fraudulent activity, consumers can periodically order a copy of their consumer report. Consumers can limit fraud by carefully reviewing credit card, checking, and other account statements for unauthorized transactions, and promptly reporting any unauthorized use to the financial institution.

What can consumers do if they are victims of fraud or identity theft?

Consumers who are victims of fraud or identity theft can take a number of actions to help minimize the damage, including notifying the police. The consumer should immediately contact all creditors to notify them of the theft, close the accounts, and have the account numbers changed. In addition, the consumer should notify any other financial or other institutions with whom the consumer does business to alert the institution to the fraud. Consumers may also wish to contact the three major credit bureaus to report the theft.