PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

on

ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE

May 18, 2005

I. INTRODUCTION

Mr. Chairman, I am Lydia Parnes, Director of the Bureau of Consumer Protection of the Federal Trade Commission.[1] I appreciate the opportunity to appear before you today to discuss the laws currently applicable to resellers of consumer information, commonly known as "data brokers."

Data brokers provide information services to a wide variety of business and government entities. The information they provide may help credit card companies detect fraudulent transactions or assist law enforcement agencies in locating potential witnesses. Despite these benefits, however, there are concerns about the aggregation of sensitive consumer information and whether this information is protected adequately from misuse and unauthorized disclosure. In particular, recent security breaches have raised questions about whether sensitive consumer information collected by data brokers may be falling into the wrong hands, leading to increased identity theft and other frauds. In this testimony, I will briefly describe what types of information data brokers collect, how the information is used, and some of the current federal laws that may apply to these entities, depending on the nature of the information they possess.

All of this discussion takes place against the background of the threat of identity theft, a pernicious crime that harms both consumers and financial institutions. A 2003 FTC survey showed that over a one-year period nearly 10 million people – or 4.6 percent of the adult population – had discovered that they were

in this testimony, the FTC has a substantial ongoing program both to assist the victims of identity theft and to collect data to assist criminal law enforcement agencies in prosecuting the perpetrators of identity theft.

II. THE COLLECTION AND USE OF CONSUMER INFORMATION[3]

The information industry is large and complex and includes companies of all sizes. Some collect information from original sources, others resell data collected by others, and many do both. Some provide information only to government agencies or large companies, while others sell information to small companies or the general public.

A. Sources of Consumer Information

Data brokers obtain their information from a wide variety of sources and provide it for many different purposes. The amount and scope of information that they collect varies from company to company, and many offer a range of products tailored to different markets and uses. Some data brokers, such as consumer reporting agencies, store collected information in a database and allow access to various customers. Some data brokers may collect information for

---

at http://www.ftc.gov/os/2003/09/synovatereport.pdf).

[3] For more information on how consumer data is collected, distributed, and used, see generally General Accounting Office, *Private Sector Entities Routinely Obtain and use SSNs, and Laws Limit the Disclosure of this Information* (GAO-04-11) (2004); General Accounting Office, *SSNs Are Widely Used by Government and Could be Better Protected, Testimony Before the House Subcommittee on Social Security, Committee on Ways and Means* (GAO-02-691T) (statement of Barbara D. Bovbjerg, April 29, 2002); Federal Trade Commission, *Individual Reference Services: A Report to Congress* (December 1997) (available at http://www.ftc.gov/os/1997/12/irs.pdf). The Commission has also held two workshops on the collection and use of consumer information. An agenda, participant biographies, and transcript of "Information Flows, The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information," held on June 18, 2003, is available at http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html

one-time use by a single customer. For example, a data broker may collect information for an employee background check and provide that information to one employer.

There are three broad categories of information that data brokers collect and sell: public record information, publicly-available information, and non-public information.

1. Public Record Information

Public records are a primary source of information about consumers. This information is obtained from public entities and includes 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 judgments). Although these records generally are available to anyone directly from the public agency where they are on file, data brokers, often through a network of subcontractors, are able to collect and organize large amounts of this information, providing access to their customers on a regional or national basis. The nature and amount of personal information on these records varies with the type of records and agency that created them.[4]

2. Publicly-Available Information

A second type of information collected is information that is not from public records but is publicly available. This information is available from telephone directories, print publications, Internet sites, and other sources accessible to the general public. As is true with public record information, the ability of data brokers to amass a large volume of publicly-available information allows their customers to obtain information from an otherwise disparate array of sources.

[4] Specific state or federal laws may govern the use of certain types of public records. For example, the federal Driv

3. Non-Public Information

Data brokers may also obtain personal information that is not generally available to members of the public. Types of non-public information include:

- Identifying or contact information submitted to businesses by consumers to obtain products or services (such as name, address, phone number, email address, and Social Security number);

- Information about the transactions consumers conduct with businesses (such as credit card numbers, products purchased, magazine subscriptions, travel records, types of accounts, claims filed, or fraudulent transactions);

- Information from applications submitted by consumers to obtain credit, employment, insurance, or other services (such as information about employment history or assets); and

- Information submitted by consumers for contests, website registrations, warranty registrations, and the like.

B. Uses of Consumer Information

Business, government, and non-profit entities use information provided by data brokers for a wide variety of purposes. For example, the commercial or non-profit sectors may use the information to:

- Authenticate potential customers and to prevent fraud by ensuring that the customer is who he or she purports to be;

  Evaluate the risk of providing services to a particular consumer, for example to decide whether to extend credit, insurance, rental, or leasing services and on what terms;

  Ensure compliance with government regulations, such as customer verification requirements under anti-money laundering statutes;

  Perform background checks on prospective employees;

  Locate persons for a variety of reasons, including to collect child support or other debts; to find estate beneficiaries or holders of dormant accounts; to find potential organ donors; to find potential contributors; or in connection with private legal actions, such as to locate

potential witnesses or defendants;

Conduct marketing and market research; and

Conduct academic research.

Government may use information collected by data brokers for:

General law enforcement, including to investigate targets and locate witnesses;

Homeland security, including to detect and track individuals with links to terrorist groups; and

Public health and safety activities, such as locating people who may have been exposed to a certain virus or other pathogen.

These are just some examples of how these entities use information collected by data brokers.

It is important to understand that the business of data brokers could cover a wide spectrum of activities, everything from telephone directory information services, to fraud data bases, to sophisticated data aggregations.

III. LAWS CURRENTLY APPLICABLE TO DATA BROKERS

There is no single federal law that governs all uses or disclosures of consumer information. Rather, specific statutes and regulations may restrict disclosure of consumer information in certain contexts and require entities that maintain this information to take reasonable steps to ensure the security and integrity of that data. The FTC's efforts in this area have been based on three statutes: the Fair Credit Reporting Act ("FCRA"),[5] Title V of the Gramm-Leach-Bliley Act ("GLBA"),[6] and Section 5 of the Federal Trade Commission Act

[5] 15 U.S.C. §§ 1681-1681u, as amended.

[6] 15 U.S.C. §§ 6801-09.

1. Overview

In common parlance, the FCRA applies to consumer data that is gathered and sold to businesses in order to make decisions about consumers. In statutory terms, it applies to "consumer report" information,[11] provided by a CRA,[12] limiting such provision for a "permissible purpose."[13] Although the most common example of a "consumer report" is a credit report and the most common CRA is a credit bureau, the scope of the FCRA is much broader. For example, there exist many CRAs that provide reports in specialized areas, such as tenant screening services (that report to landlords on consumers who have applied to rent apartments) and employment screening services (that report to employers to assist them in evaluating job applicants).

CRAs other than credit bureaus provide many different types of consumer reports. They may report information they have compiled themselves, purchased from another CRA, or both. For example, a tenant screening service may report only the information in its files that it has

[11] What constitutes a "consumer report" is a matter of statutory definition (15 U.S.C. § 1681a(d)) and case law. Among other considerations, to constitute a consumer report, information must be collected or used for "eligibility" purposes. That is, the data must not only "bear on" a characteristic of the consumer (suc

received from landlords, only a consumer report obtained from another CRA, or a combination of both its own information and resold CRA data, depending on the needs of the business and the information available. Data brokers are subject to the requirements of the FCRA only to the extent that they are providing "consumer reports."

2. "Permissible Purposes" For Disclosure of Consumer Reports

The FCRA limits distribution of consumer reports to those with specific, statutorily-defined "permissible purposes." Generally, reports may be provided for the purposes of making decisions involving credit, insurance, or employment.[14] Consumer reporting agencies may also provide reports to persons who have a "legitimate business need" for the information in connection with a consumer-initiated transaction.[15] Target marketing – making unsolicited mailings or telephone calls to consumers based on information from a consumer report – is generally not a permissible purpose.[16]

There is no general "law enforcement" permissible purpose for government agencies. With few exceptions, government agencies are treated like other parties – that is, they must have a permissible purpose to obtain a consumer report.[17] There are only two limited areas in which

[14] 15 U.S.C. § 1681b(a)(3)(A), (B), and (C). Consumer reports may also be furnished for certain ongoing account-monitoring and collection purposes.

[15] 15 U.S.C. § 1681b(a)(3)(F). This subsection allows landlords a permissible purpose to receive consumer reports. It also prov

the FCRA makes any special allowance for governmental entities. First, the law has always allowed such entities to obtain limited identifying information (name, address, employer) from CRAs without a "permissible purpose."[18] Second, the FCRA was amended to add express provisions permitting government use of consumer reports for counterintelligence and counter-terrorism.[19]

3. "Reasonable Procedures" to Identify Recipients of Consumer

"financial activities" described in Section 4(k) of the Bank Holding Company Act of 1956[27] and its accompanying regulations.[28]

under the GLBA Privacy Rule, even if those enti

institutions to develop a written information security plan that describes their programs to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires a plan that accounts for each entity's particular circumstances – its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps (for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers) in implementing their plans. Since the GLBA Safeguards Rule became effective in May 2003, the Commission has brought two law enforcement actions against companies that violated the Rule by not having reasonable protections for customers' personal information.[37]

To the extent that data brokers fall within GLBA's definition of "financial institution," they must maintain reasonable security for customer information. If they fail to do so, the Commission could find them in violation of the Rule. The Commission can obtain injunctive relief for such violations, as well as consumer redress or disgorgement in appropriate cases.[38]

C. Section 5 of the FTC Act

In addition, Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or

---

Administration, the Securities Exchange Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, and state insurance authorities have promulgated comparable information safeguards rules, as required by Section 501(b) of the GLBA. 15 U.S.C. § 6801(b); *see, e.g.*, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616-41 (Feb. 1, 2001). The FTC has jurisdiction over entities not subject to the jurisdiction of these agencies.

[37] *Sunbelt Lending Services*

affecting commerce."[39] Under the FTC Act, the Commission has broad jurisdiction to prevent unfair or deceptive practices by a wide variety of entities and individuals operating in commerce.

Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information.[40] To date, the Commission has brought five cases against companies for deceptive security claims, alleging that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information. Because they allegedly failed to take such steps, their claims were deceptive.[41] The consent orders settling these cases have required the companies to implement rigorous information security programs generally conforming to the standards set forth in the GLBA Safeguards Rule.[42]

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable

---

[39] 15 U.S.C. § 45(a).

[40] Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances.

by consumers nor offset by countervailing

Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[47]

IV. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

In addition to its regulatory and enforcement efforts, the Commission assists consumers with advice on the steps they can take to minimize their risk of becoming identity theft victims, supports criminal law enforcement efforts, and provides resources for companies that have experienced data breaches. The 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act") provides the FTC with a specific role in combating identity theft.[48] To fulfill the Act's mandate, the Commission implemented a program that focuses on collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; maintaining and promoting the Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and providing outreach and education to consumers, law enforcement, and industry.

A. Working with Consumers

The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft. We receive about 15,000 to 20,000 contacts per week on the hotline, or via our website or mail from victims and consumers who want to learn about how to avoid becoming a victim. The callers to the hotline receive counseling from trained personnel who provide information on prevention of identity theft, and

---

[47] 45 C.F.R. § 164.530(c).

[48] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

includes other materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

The Commission has also developed ways to simplify the recovery process. One example is the ID Theft Affidavit, which is included in the *Take Charge* booklet and on the website. The FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. To date, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit and has recorded more than 809,000 hits to the Web version.

B. Working with Law Enforcement

A primary purpose of the Identity Theft Act was to enable criminal law enforcement agencies to use a single database of victim complaints to support their investigations. To ensure that the database operates as a national clearinghouse for complaints, the FTC accepts complaints from state and federal agencies as well as from consumers.

With over 844,000 complaints, the Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. The Commission publishes annual charts showing the prevalence of identity theft complaints by states and cities.[51] Law enforcement and policy makers use these reports to better understand identity theft.

Since the inception of the Clearinghouse, more than 1,200 law enforcement agencies have signed up for the database. Individual investigators within those agencies can access the system from their desktop computers 24 hours a day, seven days a week.

---

[51] Federal Trade Commission - National and State Trends in Fraud & Identity Theft (Feb. 2005) (available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf).

The Commission also encourages even greater use of the Clearinghouse through training seminars offered to law enforcement. Beginning in 2002, the FTC, in cooperation with the Department of Justice, the U.S. Postal Inspection Service, and the U.S. Secret Service, initiated full day identity theft training seminars for state and local law enforcement officers. To date, this group has held 18 seminars across the country. More than 2,550 officers have attended these seminars, representing over 890 different agencies. Future seminars are being planned for additional cities.

The FTC staff also developed an identity theft case referral program. The staff creates preliminary investigative reports by examining patterns of identity theft activity in the Clearinghouse. The staff then refers the investigative reports to Financial Crimes Task Forces and other law enforcers for further investigation and potential prosecution.

C. Working with Industry

The private sector can help tackle the problem of identity theft in several ways. From prevention of identity theft through better security and authentication, to helping victims recover, businesses play a key role in addressing identity theft.

The FTC works with institutions that maintain personal information to identify ways to keep that information safe from identity theft. In 2002, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to a roundtable discussion of what steps entities can and do take to prevent identity theft and ensure the security of personal information in employee and customer records. This type of informal event provides an opportunity for the participants to share information and learn about the practices used by different entities to protect against identity theft.

The FTC also provides guidance to businesses about information security risks and the precautions they must take to protect or minimize risks to personal information. For example, the Commission has disseminated guidance for businesses on reducing risks to their computer systems,[52] as well as guidance for complying with the GLBA Safeguards Rule.[53] Our emphasis is on preventing breaches before they happen by encouraging businesses to make security part of their regular operations and corporate culture. The Commission has also published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, which is a business education brochure on managing data compromises.[54] This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

V. CONCLUSION

Data brokers collect and distribute a wide assortment of consumer information and may therefore be subject to a variety of federal laws with regard to the privacy and security of consumers' personal information. Determining which laws apply depends on the type of information collected and its intended use. The Commission is committed to ensuring the continued safety of consumers' personal information and looks forward to working with you to explore this subject in more depth.

---

[52] *Security Check: Reducing Risks to Your Computer Systems*, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

[53] *Financial Institutions and Customer Data: Complying with the Safeguards Rule*, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[54] *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf.