PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON THE JUDICIARY

U.S. SENATE

on

SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE

April 13, 2005

I. INTRODUCTION

Mr. Chairman, I am Deborah Platt Majoras, Chairman 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 victims of some form of identity theft.[2] As described

[1] This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2]

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 one-time use by a single customer. For example, a data broker may collect information for an

[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

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.

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

- 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

"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 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

---

[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 (such as credit worthiness, credit capacity, character, general reputation, personal characteristics, or mode of living), it must also be *used* in determinations to grant or deny credit, insurance, employment, or in other determinations regarding permissible purposes. *Trans Union*, 81 F.3d at 234.

[12] The FCRA defines a "consumer reporting agency" as an entity that regularly engages in "assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

[13] As discussed more fully below, the "permissible purposes" set forth in the FCRA generally allow CRAs to provide consumer reports to their customers who have a legitimate business need for the information to evaluate a consumer who has applied to the report user for credit, employment, insurance, or an apartment rental. 15 U.S.C. § 1681b(a)(3).

resellers of consumer report information violated Section 607(a) of the FCRA when they provided consumer report information without adequately ensuring that their customers had a permissible purpose for obtaining the data.[23] In settling these charges, the resellers agreed to employ additional verification procedures, including verifying the identities and business of current and prospective subscribers, conducting periodic, unannounced audits of subscribers, and obtaining written certifications from subscribers as to the permissible purposes for which they seek to obtain consumer reports.[24] In 1996, Congress amended the FCRA to impose specific duties on resellers of consumer reports.[25]

In addition to the reasonable procedures requirement of Section 607(a), the FCRA also imposes civil liability on users of consumer report information who do not have a permissible purpose and criminal liability on persons who obtain such information under false pretenses.

B. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act imposes privacy and security obligations on "financial institutions."ing the h-B.oTgresr.a434on "s.0007 l72aer4 Tw(B. The Griec0Grsu0 T)]TJcedur"f.jten ceng threa

its accompanying regulations.[28] These activities include traditional banking, lending, and insurance functions, as well as other activities such as brokering loans, credit reporting, and real estate settlement services. To the extent that data brokers fall within the definition of financial institutions, they would be subject to the Act.

business to carry out the activity covered by the exception under which . . . the information [was received]."[33]

Data brokers may receive some of their information from CRAs, particularly in the form of identifying information (sometimes referred to as "credit header" data) that includes name, address, and Social Security number. Because credit header data is typically derived from information originally provided by financial institutions, data brokers who receive this information are limited by GLBA's reuse and redisclosure provision. For example, if a data broker obtains credit header information from a financial institution pursuant to the GLBA exception "to protect against or prevent actual or potential fraud,"[34] then that data broker may not reuse and redisclose that information for marketing purposes.

2. Required Safeguards for Customer Information

GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they receive from customers directly or from other financial institutions.[35] The FTC's Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,[36] requires financial

---

[33] *Id.*

[34] 15 U.S.C. § 502(e)(3)(B).

[35] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

[36] The Federal Deposit Insurance Corporation, the National Credit Union 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,

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 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.

2001). The FTC has jurisdiction over entities not subject to the jurisdiction of these agencies.

[37] *Sunbelt Lending Services*, (Docket No. C-4129) (consent order); *Nationwide Mortgage Group, Inc.*, (Docket No. 9319) (consent order).

[38] 15 U.S.C. § 6805(a)(7). In enforcing GLBA, the FTC may seek any injunctive and other equitable relief available to it under the FTC Act.

[39] 15 U.S.C. § 45(a).

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 by consumers nor offset by countervailing benefits to consumers or competition.[43] The

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

Commission has used this authority to challenge a variety of injurious practices.[44]

The Commission can obtain injunctive relief for violations of Section 5, as well as consumer redress or disgorgement in appropriate cases.

D. Other Laws

Other federal laws not enforced by the Commission regulate certain other specific classes of information. For example, the Driver's Privacy Protection Act ("DPPA")[45] prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to fourteen "permissible uses," including law enforcement, motor vehicle safety, and insurance.

The privacy rule under the Health Information Portability and Accountability ("HIPAA") Act allows for the disclosure of medical information (including patient records and billing statements) between entities for routine treatment, insurance, and payment purposes.[46] For non-routine disclosures, the individual must first give his or her consent. As with the DPPA, the HIPAA Privacy Rule provides a list of uses for which no consent is required before disclosure. 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

---

[44] These include, for example, unauthorized charges in connection with "phishing," which are high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. *See FTC v. Hill*, Civ. No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[45] 18 U.S.C. §§ 2721-25.

[46] 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

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

Idendedicaa prwebsite; 6(ation3(nd4l ltainidenprovide6(atioo.idenCom)8learideho ond p cd aralizata breb

placed on them; (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and, if possible, obtain a police report. A police report is helpful both in demonstrating to would-be creditors and debt collectors that the consumers are victims of identity theft, and also serves as an "identity theft report" that can be used for exercising various rights under the newly enacted Fair and Accurate Credit Transactions Act.[49] The FTC's identity theft website, www.consumer.gov/idtheft, has an online complaint form where victims can enter their complaint into the Clearinghouse.[50]

The FTC has also taken the lead in the development and dissemination of consumer education materials. To increase awareness for consumers and provide tips for minimizing the risk of identity theft, the FTC developed a primer on identity theft, *ID Theft: What's It All About?* Together with the victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*, the two publications help to educate consumers. The FTC alone has distributed more than 1.4 million copies of the *Take Charge* booklet since its release in February 2000 and has recorded more than 1.8 million visits to the Web version. The FTC's consumer and business education campaign 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

49

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 815,000 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 1,100 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.

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

[51] Federal Trade Commission - National and State Trends in Fraud & Identity Theft (Feb. 2005) (available at

Department of Justice, the U.S. Postal Inspection Service, the U.S. Secret Service, and the American Association of Motor Vehicle Administrators, initiated full day identity theft training seminars for state and local law enforcement officers. To date, this group has held 17 seminars across the country. More than 2,200 officers have attended these seminars, representing over 800 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,*