PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

U.S. SENATE

on

DATA BREACHES AND IDENTITY THEFT

June 16, 2005

I. INTRODUCTION

Mr. Chairman, I am Deborah Platt Majoras, Chairman of the Federal Trade Commission.[1] My fellow Commissioners and I appreciate the opportunity to appear before you today as we work to ensure the safety and security of consumers' personal information.

As we have testified previously, advances in commerce, computing, and networking have transformed the role of consumer information. Modern consumer information systems can collect, assemble, and analyze information from disparate sources, and transmit it almost instantaneously. Among other things, this technology allows businesses to offer consumers a wider range of products, services, and payment options; greater access to credit; and faster transactions.

Efficient information systems – data that can be easily accessed, compiled, and transferred – also can lead to concerns about privacy and security. Recent events validate concerns about information systems' vulnerabilities to misuse, including identity theft.

II. BACKGROUND

One particular focus of concern has been "data brokers," companies that specialize in the collection and distribution of consumer data. Data brokers epitomize the tension between the benefits of information flow and the risks of identity theft and other harms. Data brokers have emerged to meet the information needs of a broad spectrum of commercial and government users.[2] The data broker industry is large and complex and includes companies of all sizes. Some

---

[1] This written statement reflects the views of the Federal Trade Commission. Our oral statements and responses to any questions you may have represent the views of individual Commissioners and do not necessarily reflect the views of the Commission.

[2] For more information on how consumer data is collected, distributed, and used, see generally Government Accountability Office, *Private Sector Entities Routinely Obtain and use SSNs, and Laws Limit the Disclosure of this*

collect information from original sources, both public and private; 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 smaller companies or the general public as well. The amount and scope of the information that they collect varies from company to company, and many offer a range of products tailored to different markets and uses. These uses include fraud prevention, debt collection, law enforcement, legal compliance, applicant authentication, market research, and almost any other function that requires the collection and aggregation of consumer data. Because these databases compile sensitive information, they are especially attractive targets for identity thieves.

Identity theft is a crime that harms both consumers and businesses. A 2003 FTC survey estimated that nearly 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated $48 billion in losses, and costing consumers an additional $5 billion in out-of-pocket losses.[3] The survey looked at the two major categories of identity theft: (1) the misuse of exi

---

Information (GAO-04-11) (2004); Government Accountability Office, *Social Security Numbers: Use is Widespread and Protections Vary, Testimony Before the House Subcommittee on Social Security, Committee on Ways and Means* (GAO-04-768T) (statement of Barbara D. Bovbjerg, June 15, 2004); 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 also has held two workshops on the collection and use of consumer information: "Information Flows, The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information," was held on June 18, 2003; and "The Information Marketplace: Merging and Exchanging Consumer Data," was held on March 13, 2001. An agenda, participant biographies, and a transcript for these workshops are available at http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html and http://www.ftc.gov/bcp/workshops/infomktplace/index.html, respectively.

[3] Federal Trade Commission, *Identity Theft Survey Report* (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

money spent resolving the problems. For example, although people who had new accounts opened in their names made up only one-third of the victims, they suffered two-thirds of the direct financial harm. The ID theft survey also found that victims of the two major categories of identity theft cumulatively spent almost 300 million hours – or an average of 30 hours per person – correcting their records and reclaiming their good names. Identity theft causes significant economic and emotional injury, and we take seriously the need to reduce it.

As detailed in our recent testimony on this subject,[4] there are a variety of existing federal laws and regulations that address the security of, and access to, sensitive information that these companies maintain, depending on how that information was collected and how it is used. For example, the Fair Credit Reporting Act ("FCRA")[5] regulates credit bureaus, any entity or individual who uses credit reports, and the businesses that furnish information to credit bureaus.[6] The FCRA requires that sensitive credit report information be used only for certain permitted purposes. The Gramm-Leach-Bliley Act ("GLBA")[7] prohibits financial institutions from disclosing consumer information to non-affiliated third parties without first allowing consumers

---

4 *See, e.g.*,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), *available at* http://www.ftc.gov/opa/2005/05/databrokertest.htm.

5 15 U.S.C. §§ 1681-1681x.

6 Credit bureaus are also known as "consumer reporting agencies."

7 15 U.S.C. §§ 6801-09.

[8] The FTC's Safeguards Rule implements GLBA's security requirements for entities under the FTC's jurisdiction. *See* 16 C.F.R. pt. 314 ("GLBA Safeguards Rule"). The federal banking regulators also have issued comparable regulations for the entities under their jurisdiction.

[9] 15 U.S.C. § 45(a).

[10] Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1984).

[11] *Petco Animal Supplies, Inc.* (FTC Docket No. C-4133) (Mar. 4, 2005); *(M*

[12] 15 U.S.C. § 45(n).

[13] 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), *available at* http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZXD7dlaedit card numbers, bank account

[16] Commissioner Harbour is concerned about the use of the term "significant" to characterize the level of risk of identity theft that should trigger a notice to consumers.

Finally, law enforcement activity to protect data security is increasingly international in nature. Given the globalization of the marketplace, an increasing amount of U.S. consumer information may be accessed illegally by third parties outside the United States or located in offshore databases. Accordingly, the Commission needs new tools to investigate whether companies are complying with U.S. legal requirements to maintain the security of this information, and cross-border fraud legislation would give the Commission these tools. For that reason, the Commission recommends that Congress enact cross-border fraud legislation to overcome existing obstacles to information sharing and information gathering in cross-border investigations and law enforcement actions.[17]

For example, if the FTC and a foreign consumer protection agency are investigating a foreign business for conduct that violates both U.S. law and the foreign country's law, current law does not authorize the Commission to share investigative information with the foreign consumer protection agency, even if such sharing would further our own investigation. New cross-border fraud legislation could ease these restrictions, permit the sharing of appropriate investigative informatiodatawithour foreign counterparts, and gglobaliwith 000 permrn000 1.00000 di(tionalmechpansmes tohe

[17] The U.S. Senate passed cross-border fraud legislation last year by unanimous consent: S. 1234 ("International Consumer Protection Act").

or toopeby fiewac couns,f suchas SocinalSsecue's iure

account numbers in combination with required access codes or passwords.[18] Currently, the Commission's Safeguards Rule under GLBA requires financial institutions to implement reasonable physical, technical, and procedural safeguards to protect customer information. Instead of mandating specific technical requirements that may not be appropriate for all entities and might quickly become obsolete, the Safeguards Rule requires companies to evaluate the nature and risks of their particular information systems and the sensitivity of the information they maintain, and to take appropriate steps to counter these threats. They also must periodically review their data security policies and procedures and update them as necessary. The Safeguards Rule prov8

---

18 The FTC also would seek civil penalty authority for its enforcement of these provisions. A civil penalty is often the most appropriate remedy in cases where consumer redress is impracticable and where it is difficult to compute an ill-gotten gain that should be disgorged from a defendant.

19 FTC Commissioner Orson Swindle led the U.S. delegation to the OECD Committee that drafted the 2002 OECD Security Guidelines. *See* Organization for Economic Cooperation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (July 25, 2002), *available at* http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

20 Under GLBA, a "financial institution" is defined as an entity that engages in one or more of the specific activities listed in the Bank Holding Company Act and its implementing regulations. *See* 15 U.S.C. § 6809(3). These activities include extending credit, brokering loans, financial advising, and credit reporting.

Currently there are two basic approaches in place that are used to determine when notices should be triggered. The first is the bank regulatory agency

---

[21] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736-54 (Mar. 29, 2005).

[22] Under the guidance, this determination can be made by the financial institution in consultation with its primary federal regulator.

[23] Cal. Civ. Code § 1798.82.

[24] *Id.* at § 1798.82(d).

C. Social Security Numbers

Social Security numbers today are a vital instrument of interstate commerce. With 300 million American consumers, many of whom share the same name,[26] the unique 9-digit Social Security number is a key identification tool for business. As the Commission found in last year's data matching study under FACTA, Social SecurityR

---

[26] According to the Consumer Data Industry Association, 14 million Americans have one of ten last names, and 58 million men have one of ten first names.

[27] *See* Federal Trade Commission, *Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 38-40 (Dec. 2004), *available at* http://www.ftc.gov/reports/facta/041209factarpt.pdf.

[28] The federal government also uses Social Security numbers as an identifier. For example, HHS uses it as the Medicare identification number, and the IRS uses it as the Taxpayer Identification Number. It also is used to administer the federal jury system, federal welfare and workmen's compensation programs, and the military draft registration. *See* Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), *available at* www.ssa.gov/history/reports/ssnreportc2.html.

some restrictions on the disclosure of specific types of information under certain circumstances. The FCRA, for example, limits the provision of "consumer report" information to certain purposes, primarily those determining consumers' eligibility for certain transactions, such as extending credit, employment, or insurance. GLBA requires that "financial institutions"[29] provide consumers an opportunity to opt out before disclosing their personal information to third parties, outside of specific exceptions, such as for fraud prevention or legal compliance.[30] Other statutes that limit information disclosure include the privacy rule under the Health Insurance Portability and Accountability Act of 1996,[31] which applies to health care providers and other medical-related entities, and the Drivers Privacy Protection Act,[32] which protects consumers from improper disclosures of driver's license information by state motor vehicle departments.

While these laws provide important privacy protections within their respective sectors, they do not provide comprehensive protection for Social Security numbers.[33] For example, disclosure of a consumer's name, address, and Social Security number may be restricted under GLBA when the source of the information is a financial institution,[34] but in many cases the same

---

29 *See supra* n.20 (defining financial institution).

30 GLBA protects some, but not all Social Security numbers held by financial institutions. It does not, for example, cover Social Security numbers in databases of Social Security numbers furnished by banks to credit bureaus under the Fair Credit Reporting Act (i.e., so-called "credit header" information) prior to the GLBA Privacy Rule's July 2001 effective date.

31 45 C.F.R. pts. 160 and 164 (implementing Sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191).

32 18 U.S.C. §§ 2721-25.

33 The Commission may, however, bring enforcement actions under Section 5 of the Federal Trade Commission Act against entities whose privacy or security practices are unfair or deceptive.

34 *See supra* n.30 (discussing limitations of GLBA protection).

information can be purchased on the Internet from a non-financial institution.

many benefits of the modern information age are not diminished by these threats to consumers' security. The Commission is committed to ensuring the continued security of consumers' personal information and looks forward to working with you to protect consumers.