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 existing accounts; and (2) the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims, in both the time and

---

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.

to opt out of the disclosure. GLBA also requires these businesses to implement appropriate safeguards to protect the security and integrity of their customer information.[8]

In addition, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair or deceptive acts or practices in or affecting commerce."[9] Under the FTC Act, the Commission has broad jurisdiction to prohibit 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.[10] To date, the Commission has brought five cases against companies for deceptive security claims.[11] These actions alleged that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information, but because they allegedly failed to take such steps, their claims were deceptive. The consent orders settling these cases have required the companies to implement appropriate information security programs that generally conform to the standards that the Commission set forth in the GLBA Safeguards Rule.

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

---

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); *MTS Inc., d/b/a Tower Records/Books/Video* (FTC Docket No. C-4110) (May 28, 2004); *Guess?, Inc.* (FTC Docket No. C-4091) (July 30, 2003); *Microsoft Corp.* (FTC Docket No. C-4069) (Dec. 20, 2002); *Eli Lilly & Co.* (FTC Docket No. C-4047) (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

by consumers nor offset by countervailing benefits to consumers or competition.[12] The Commission has used this authority to challenge a variety of injurious practices that threaten data security.[13]

As the Commission has testified previously, an actual breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate.[14] It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution.[15]

Despite the existence of these laws, recent security breaches have raised questions about whether data brokers and other companies that collect or maintain sensitive personal information are taking adequate steps to ensure that the information they possess does not fall into the wrong hands, as well as about what steps should be taken when such data is acquired by unauthorized individuals. Vigorous enforcement of existing laws and business education about the requirements of existing laws and the importance of good security can go a long way in addressing these concerns. Nonetheless, recent data breaches have prompted Congress to

---

[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 (RZX) (filed C.D. Cal. July 24, 2003), *available at* http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[14] *See* Statement of the Federal Trade Commission Before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform (Apr. 21, 2004) at 5, *available at* http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

[15] *Id.* at 4.

consider legislative proposals, and the Commission has been asked to comment on the need for new legal requirements.

III. INCREASING CONSUMER INFORMATION SECURITY

The Commission recommends that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions.

Further, the Commission recommends that Congress consider requiring companies to notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft.[16] Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. As discussed below, the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required.

In addition, many have raised concerns about misuse of Social Security numbers. It is critical to remember that Social Security numbers are vital to current information flows in the granting and use of credit and the provision of financial services. In addition, private and public entities routinely have used Social Security numbers for many years to access their voluminous records. Ultimately, what is required is to distinguish between legitimate and illegitimate collection, uses, and transfers of Social Security numbers.

---

[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 information with our foreign counterparts, and give us additional mechanisms to help protect the security of U.S. consumers' data whether it is located abroad or in the United States.

A. Require Procedures to Safeguard Sensitive Information

One important step to reduce the threat of identity theft is to increase the security of certain types of sensitive consumer information that could be used by identity thieves to misuse existing accounts or to open new accounts, such as Social Security numbers, driver's license numbers, and

---

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

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 provides a strong but flexible framework for companies to take responsibility for the security of information in their possession, and it reflects widely accepted principles of information security, similar to those contained in the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems and Networks.[19]

Currently, the Safeguards Rule applies only to "customer information" collected by "financial institutions."[20] It does not cover many other entities that may also collect, maintain and transfer or sell sensitive consumer information. Although we believe that Section 5 already requires companies holding sensitive data to have in place procedures to secure it if the failure to

---

[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.

do so is likely to cause substantial consumer injury, we believe Congress should consider whether new legislation incorporating the flexible standard of the Commission's Safeguards Rule is appropriate.

B. Notice When Sensitive Information Has Been Breached

Unfortunately, even if the best efforts to safeguard data are made, security breaches can still occur. The Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified. Prompt notification to consumers in these cases can help them mitigate the damage caused by identity theft. Notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves.

The challenge is to require notices only when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, notices may be more common than would be useful. As a result, consumers may become numb to them and fail to spot or act on those risks that truly are significant. In addition, notices can impose costs on consumers and on businesses, including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally.

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 standard.[21] Under that standard, notice to the federal regulatory agency is required as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. In addition, notice to consumers is required when, based on a reasonable investigation of an incident of unauthorized access to sensitive customer information, the financial institution determines that misuse of its information about a customer has occurred or is reasonably possible.[22]

The second approach is found in the California notice statute.[23] Under that approach, all businesses are required to provide notices to their consumers when a defined set of sensitive data, in combination with information that can be used to identify the consumer, has been or is reasonably likely to have been acquired by an unauthorized person in a manner that "compromises the security, confidentiality, or integrity of personal information."[24]

The California "unauthorized acquisition" approach to requiring consumer notice does not compel notice in every instance of improper access to a database. Instead, it allows businesses some flexibility to determine when a notice is necessary, while also providing a fairly objective standard against which compliance can be measured by the broad range of businesses subject to

---

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).

the law. Under guidance issued by the California Office of Privacy Protection, a variety of factors can be considered in determining whether information has been "acquired," such as (1) indications that protected data is in the physical possession and control of an unauthorized person (such as a lost or stolen computer or other device); (2) indications that protected data has been downloaded or copied; or (3) indications that protected data has been used by an unauthorized person, such as to open new accounts.[25] One issue that is not directly considered is what action to take in cases in which, prior to sending consumer notification, the business already has taken steps that remedy the risk. For example, one factor to consider in deciding whether to provide notice is whether the business already has canceled consumers' credit card accounts and reissued account numbers to the affected consumers.

We have growing experience under both models to inform consideration of an appropriate national standard. Because formulating any standard will require balancing the need for a clear, enforceable standard with ensuring, to the extent possible, that notices go to consumers only where there is a risk of harm, we believe that if Congress decides to enact a notice provision, the best approach would be to authorize the FTC to conduct a rulemaking under general statutory standards. The rulemaking would set the criteria under which notice would be required for data breaches involving non-regulated industries. The rulemaking could address issues such as the circumstances under which notice is required, which could depend on the type of breach and risk of harm, and the appropriate form of notice. This approach would also allow the Commission to adjust the standard as it gains experience with its implementation.

---

[25] These factors are discussed in the California Office of Privacy Protection's publication, *Recommended Practices on Notification of Security Breach Involving Personal Information*, at 11 (Oct. 10, 2003), *available at* http://www.privacy.ca.gov/recommendations/secbreach.pdf.

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 Security numbers also are one of the primary tools that credit bureaus use to ensure that the data furnished to them is placed in the right file and that they are providing a credit report on the right consumer.[27] Social Security numbers are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. Social Security number databases are used to fight identity fraud – for example, they can confirm that a Social Security number belongs to a particular loan applicant and is not stolen.[28] Without the ability to use Social Security numbers as personal identifiers and fraud prevention tools, the granting of credit and the provision of other financial services would become riskier and more expensive and inconvenient for consumers.

While Social Security numbers have important legitimate uses, their unauthorized use can facilitate identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims. Currently, there are various federal laws that place

---

[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. The problem of how to strengthen or expand existing protections in ways that would not interfere with the beneficial uses of Social Security numbers is challenging.

Although the Commission has extensive experience with identity theft and the consumer credit reporting system, restrictions on disclosure of Social Security numbers could have a broad impact on areas where the Commission does not have expertise. These areas include public health, criminal law enforcement, and anti-terrorism efforts. Morever, efforts to restrict disclosure of Social Security numbers are complicated by the fact that among the primary sources of Social Security numbers are the public records on file with many courts and clerks in cities and counties across the nation. Regulation or restriction of Social Security numbers in public records thus poses substantial policy and practical concerns.

Ultimately, what is required is to distinguish between legitimate and illegitimate collection, uses, and transfers of Social Security numbers. The Commission would appreciate the opportunity to work with Congress to further evaluate the costs and benefits to consumers and the economy of regulating the collection, transfer, and use of Social Security numbers.

IV. CONCLUSION

New information systems have brought benefits to consumers and businesses alike. Never before has information been so portable, accessible, and flexible. Indeed, sensitive personal financial information has become the new currency of today's high tech payment systems. But with these advances come new risks, and identity thieves and other bad actors have begun to take advantage of new technologies for their own purposes. As the recent focus on information security has demonstrated, Americans take their privacy seriously, and we must ensure that the

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.