PREPARED STATEMENT OF

BETSY BRODER
ASSISTANT DIRECTOR
DIVISION OF PLANNING AND INFORMATION
FEDERAL TRADE COMMISSION

before the

SELECT COMMITTEE ON INFORMATION SECURITY
of the
PENNSYLVANIA HOUSE OF REPRESENTATIVES

on

IDENTITY THEFT AND DATA SECURITY

October 11, 2005

I. INTRODUCTION

Mr. Chairman, and members of the Committee, I am Betsy Broder, Assistant Director of the Division of Planning and Information, Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to appear before you today to present the FTC staff's views on the important issues of identity theft and data security.[1]

The information industry is large and complex and includes companies of all sizes. Recent security breaches have raised questions about whether sensitive consumer information may be falling into the wrong hands, leading to increased identity theft and other frauds. 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. And our own complaint database contains identity theft complaints from more than 7,500 Pennsylvania residents.[2] Today's discussion of information security and data protection takes place against the backdrop of the threat of identity theft – a crime that harms both consumers and businesses.

II. PROTECTING CONSUMERS' PERSONAL INFORMATION

There are a variety of existing federal laws and regulations that address the security of, and access to, consumers' sensitive information, depending on how that information was

---

1 These comments represent the views of the staff of the Federal Trade Commission. They do not necessarily represent the views of the Federal Trade Commission or any individual commissioner. The Commission, however, has authorized the staff to provide these comments.

2 FTC - National and State Trends in Fraud & Identity Theft (Feb. 2005), available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf ("FTC Fraud Trends").

collected and how it is used.[3] However, 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"),[4] Title V of the Gramm-Leach-Bliley Act ("GLBA"),[5] and Section 5 of the Federal Trade Commission Act ("FTC Act").[6]

A. The Fair Credit Reporting Act

The FCRA regulates credit bureaus, any entity or individual who uses credit reports, and the businesses that furnish information to credit bureaus.[7] Under the FCRA, credit bureaus must employ "reasonable procedures" to ensure that they supply consumer reports only to those with an FCRA-sanctioned "permissible purpose." Section 607(a) provides that credit bureaus must

---

3 *See* 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.

4 15 U.S.C. §§ 1681-1681x, as amended.

5 *Id.* §§ 6801-09.

6 *Id.* § 45(a).

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

make "reasonable efforts" to verify the identity of prospective recipients of consumer reports and that they have a permissible purpose to use the report.[8]

The Commission has implemented the general and specific requirements of this provision in a number of enforcement actions that resulted in consent orders with the major nationwide credit bureaus[9] and with resellers of consumer reports (businesses that purchase consumer reports from the major bureaus and resell them).[10] For example, in the early 1990s, the FTC charged that 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.[11] 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

---

8 15 U.S.C. § 1681e(a).

9 *Equifax Credit Info. Servs., Inc.*, 130 F.T.C. 577 (1995); *Trans Union Corp.* 116 F.T.C. 1357 (1993) (consent settlement of prescreening issues *only* in 1992 target marketing complaint; *see also Trans Union Corp. v. FTC*, 81 F.3d 228 (D.C. Cir. 1996)); *FTC v. TRW Inc.*, 784 F. Supp. 362 (N.D. Tex. 1991); *Trans Union Corp.*, 102 F.T.C. 1109 (1983). Each of these "omnibus" orders differed in detail, but generally covered a variety of FCRA issues including accuracy, disclosure, permissible purposes, and prescreening.

10 *W.D.I.A. Corp.*, 117 F.T.C. 757 (1994); *CDB Infotek*, 116 F.T.C. 280 (1993); *Inter-Fact, Inc.*, 116 F.T.C. 294 (1993); *I.R.S.C., Inc.*, 116 F.T.C. 266 (1993) (consent agreements against resellers settling allegations of failure to adequately insure that users had permissible purposes to obtain the reports).

11 *See* cases cited *supra* note 10.

seek to obtain consumer reports.[12] In 1996, Congress amended the FCRA to impose specific duties on resellers of consumer reports.

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[13] and criminal liability on persons who obtain such information under false pretenses.[14]

B. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act prohibits "financial institutions" from disclosing consumer information to non-affiliated third parties without first allowing consumers to opt out of the disclosure, subject to certain statutory exceptions.[15] GLBA also requires these businesses 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.[16] The FTC's GLBA Safeguards Rule requires financial institutions to develop a written information security plan that describes their programs to protect customer information. Given the wide variety of entities covered, the GLBA Safeguards Rule requires a plan that

---

12 A press release describing the *I.R.S.C.*, *CDB Infotek*, and *Inter-Fact* consent agreements is available at http://www.ftc.gov/opa/predawn/F93/irsc-cdb-3.htm.

13 15 U.S.C. § 1681n.

14 *Id.* § 1681q.

15 *Id.* §§ 6801-09. The FTC's Privacy Rule implements GLBA's privacy requirements for entities under the FTC's jurisdiction. *See* FTC Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313. In some circumstances, GLBA also applies to other entities that receive consumer information from financial institutions.

16 The FTC's Safeguards Rule implements GLBA's security requirements for entities under the FTC's jurisdiction. *See* FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314 ("GLBA Safeguards Rule"). The federal banking regulators also have issued comparable regulations for the entities under their jurisdiction.

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 three law enforcement actions against companies that allegedly violated the Rule by not having reasonable protections for customers' personal information.[17]

C. Section 5 of the FTC Act

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[18] 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.[19] To date, the Commission has brought five cases against companies for deceptive security claims.[20] These actions alleged that

---

17 *Sunbelt Lending Servs.*, FTC Docket No. C-4129 (consent order) (Jan.7, 2005); *Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (consent order) (Apr.15, 2005); (*Superior Mortgage Corp.*, FTC File No. 052-3136 (consent agreement placed on the public record for comment, Sept. 28, 2005). Documents related to these enforcement actions are available at http://www.ftc.gov/opa/2004/11/ns.htm and http://www.ftc.gov/opa/2005/09/superior.htm.

18 15 U.S.C. § 45(a).

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

20 *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

the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information, but because they 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 by consumers nor offset by countervailing benefits to consumers or competition.[21] The Commission has used this authority to challenge a variety of injurious practices that threaten data security.[22] Most recently, in the settlement with BJ's Wholesale Club, the FTC alleged that the company engaged in a number of practices which, taken together, did not provide reasonable security to protect consumer credit and debit card information, leading to millions of dollars in fraudulent charges.[23] The settlement requires BJ's to implement a comprehensive information

---

enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises enf.html.

[21] 15 U.S.C. § 45(n).

[22] 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*, 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.*, No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), available at http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[23] *BJ's Wholesale Club Inc.*, FTC Docket No. C-4148, (consent order) (Sept. 23, 2005). A press release describing the consent agreement is available at http://www.ftc.gov/opa/2005/06/bjswholesale.htm.

security program and obtain audits by an independent third-party security professional every other year for 20 years.

While an actual breach of security is not a prerequisite for enforcement under Section 5, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate.[24] 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.[25]

III. 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.[26] 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 Identity Theft Data Clearinghouse ("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

---

24 *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.

25 *Id.* at 4.

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

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 via the hotline, our website, and 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 also inform victims of the steps to take to resolve the problems resulting from the misuse of their identities. Victims are advised to: (1) obtain copies of their credit reports and have a fraud alert 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 obtain a police report. A police report is helpful both in demonstrating to would-be creditors and debt collectors that the consumer is a victim 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.[27] The FTC's identity theft website, www.consumer.gov/idtheft, has an online complaint form where victims can enter their complaint into the Clearinghouse.[28]

The FTC also has taken the lead in the development and dissemination of consumer

---

[27] These include the right to an extended, seven-year fraud alert, the right to block fraudulent trade lines on credit reports, and the ability to obtain copies of fraudulent applications and transaction reports. *See* 15 U.S.C. § 1681 *et seq.*, as amended.

[28] Once a consumer informs a consumer reporting agency that the consumer believes that he or she is the victim of identity theft, the consumer reporting agency must provide the consumer with a summary of rights titled "Remedying the Effects of Identity Theft," available at http://www.ftc.gov/bcp/conline/pubs/credit/idtsummary.pdf.

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 It's 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 1.7 million copies of the *Take Charge* booklet (formerly known as *ID Theft: When Bad Things Happen To Your Good Name*) since its release in February 2000 and has recorded more than 2.2 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 state laws, and other resources.

The Commission also has developed ways to simplify the recovery process for identity theft victims. 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 one million 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 940,000 complaints, the Clearinghouse provides a picture of the nature, prevalence, and trends of the complaints submitted by ID theft victims. The Commission publishes annual charts showing the prevalence of identity theft complaints by state and city.[29] Law enforcement and policymakers use these reports to better understand identity theft.

Since the inception of the Clearinghouse, more than 1,300 law enforcement agencies have signed up for the database, including more than 60 Pennsylvania state and local law enforcement agencies. 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 U.S. Secret Service, the U.S. Postal Inspection Service, the U.S. Department of Justice, and more recently 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 19 seminars across the country, the most recent of which was held in Philadelphia. Almost 3,000 officers have attended these seminars, representing over 980 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.

---

[29] FTC Fraud Trends, *supra* note 2.

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. For example, 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,[30] as well as guidance for complying with the GLBA Safeguards Rule.[31] 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 also has published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, which is a business

---

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

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

education brochure on managing data compromises.[32] This publication provides guidance on contacting law enforcement and consumers in the event of a breach.

D. ID Theft In Pennsylvania[33]

The FTC's ID Theft Data Clearinghouse offers a view into the impact of this crime on individuals, and its prevalence in a specific area. In calendar year 2004, the FTC received more than 7,500 identity theft complaints from Pennsylvania consumers, with more than 1,800 victims reporting from Philadelphia.[34] Of the Pennsylvania victims, 32% reported that their identity was used to open new credit card accounts or take over existing accounts. Nineteen percent reported that utility service, including cell phone accounts, had been opened in their names. Bank fraud, including accessing a checking or savings account, reportedly affected 15% of the Pennsylvania complainants, and 8% reported that government documents or benefits had been obtained fraudulently in their names. Finally, 7% reported employment-related fraud, 6% reported loan fraud, and 23% reported other, miscellaneous types of fraud such as use of another's name in the criminal justice system, to obtain medical services or rent a home.[35] These percentages generally track the national trends.

---

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

33 FTC Fraud Trends, *supra* note 2.

34 The top five Pennsylvania cities in descending rank order from which the FTC received identity theft complaints are Philadelphia, Pittsburgh, Allentown, Reading, and York.

35 These percentages total more than 100% because approximately 19% of the victims from Pennsylvania reported experiencing more than one type of identity theft.

IV. CONCLUSION

The Commission is committed to ensuring the continued security of consumers' personal information and will continue its work with the public and private sectors to protect consumers. Vigorous enforcement of existing laws and consumer and business education about the requirements of these laws and the importance of good security can help improve data security practices and minimize consumers' risk of identity theft.