PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

"FINANCIAL PRIVACY"

Before the

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

of the

HOUSE COMMITTEE ON THE JUDICIARY

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

March 4, 1999

Mr. Chairman and members of the Subcommittee, I am David Medine, Associate Director for Financial Practices, Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of financial privacy.[1]

I. Introduction

We live in a burgeoning information economy. The personal computer revolution of the 1980s, and the explosive growth of interactive technologies in the 1990s, have made it possible for businesses to collect, aggregate, store, and market personal information in ways unthinkable only a generation ago. The commercial use of this information can have great benefits for consumers; but it is also a matter of great concern because information can be aggregated and disseminated so readily.

It is not surprising to learn that, of all the types of information collected about them, American consumers view their financial information as most sensitive, indeed as sensitive as their medical histories.[2] As custodians of sensitive financial information, banks must strike a balance between addressing their customers' privacy concerns and guarding against fraud and other criminal uses of banking services. Last December, the Federal Reserve Board,[3] the Office of the

---

[1] My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any Commissioner.

[2] Testimony of Alan F. Westin on "Electronic Payment Systems, Electronic Commerce, and Consumer Privacy" before the Subcommittee on Financial Institutions and Consumer Credit, House Committee on Banking and Financial Services, at 4 (September 18, 1997).

[3] Know Your Customer, 63 Fed. Reg. 67,516 (1998) (to be codified at 12 C.F.R. pts. 208, 211, and 225) (proposed Dec. 7, 1998).

Comptroller of the Currency,[4] the Office of Thrift Supervision,[5] and the Federal Deposit Insurance Corporation[6] announced similar proposals to promulgate "Know Your Customer" regulations intended to curb money laundering. The proposed rules would, among other things, require banks to establish procedures to ascertain the identity of their customers and the sources of funds deposited in their accounts, and to monitor patterns in their customers' banking activities to identify suspicious transactions. Based on the comments thus far submitted on the proposed rules, it appears that some consumers are concerned with the unauthorized disclosure of their personal financial information to any third party, including the government.[7] It further appears that large numbers of commenters perceive the proposed rules to pose a new type of privacy intrusion, one initiated by government. As discussed below, this is not the type of privacy concern we have traditionally examined because it does not involve privacy protections that arise when consumers deal with businesses. Such comments demonstrate the tension between erecting safeguards that detect and deter criminal activities and protecting individuals' privacy interests. Striking the correct balance in this context presents a significant challenge to government, financial institutions, and the public.

---

[4] Know Your Customer, 63 Fed. Reg. 67,524 (1998) (to be codified at 12 C.F.R. Pt. 21) (proposed Dec. 7, 1998).

[5] Know Your Customer, 63 Fed. Reg. 67,536 (1998) (to be codified at 12 C.F.R. Pt. 563) (proposed Dec. 7, 1998).

[6] Know Your Customer, 63 Fed. Reg. 67,529 (1998) (to be codified at 12 C.F.R. Pt. 326) (proposed Dec. 7, 1998).

[7] The Commission notes that federal law already limits the government's access to an individual customer's bank records, and that that statutory protection would be unaffected by the proposed Know Your Customer rules. *See* Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq*.

The Commission has extensive experience dealing with consumer protection issues related to the financial services industry as well as consumer privacy issues, and I am pleased to present the Commission's perspective on these complex areas.

II. The Commission's Consumer Protection Role

A. The FTC's Law Enforcement Authority

The FTC is a law enforcement agency whose mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[8] With certain exceptions, including banks and other depository institutions to the extent they are regulated by the federal bank regulatory agencies, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce[9] and with

[8] 15 U.S.C. § 45(a).

[9] The Commission does not have criminal law enforcement authority. Further, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

the authority to gather information about such entities.[10] The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices.[11]

B. The FTC's Activities in the Financial Services Industry

The Commission has extensive experience in addressing consumer protection issues that arise in the financial services industry, involving, for example, the use of credit cards, lending practices, and debt collection.[12] The Commission also provides consultation to Congress and to

---

[10] 15 U.S.C. § 46(a). However, the Commission's authority to conduct studies and prepare reports relating to the business of insurance is limited. According to 15 U.S.C. § 46(a): "The Commission may exercise such authority only upon receiving a request which is agreed to by a majority of the members of the Committee on Commerce, Science, and Transportation of the Senate or the Committee on Energy and Commerce of the House of Representatives. The authority to conduct any such study shall expire at the end of the Congress during which the request for such study was made."

[11] These include, for example, the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[12] For example, in 1992, Citicorp Credit Services, Inc., a subsidiary of Citicorp, agreed to settle charges that it aided and abetted a merchant engaged in unfair and deceptive activities. Citicorp Credit Services, Inc., 116 F.T.C. 87 (1993). In 1993, the Shawmut Mortgage Company, an affiliate of Shawmut Bank Connecticut, N.A., and Shawmut Bank, agreed to pay almost one million dollars in consumer redress to settle allegations that it had discriminated based on race and national origin in mortgage lending. United States v. Shawmut Mortgage Co., 3:93CV-2453AVC (D. Conn. Dec. 13, 1993). The Commission brought the Shawmut case jointly with the United States Department of Justice. In 1996, the J.C. Penney Company entered into a consent decree and paid a civil penalty to resolve allegations that the company failed to provide required notices of adverse actions to credit applicants. United States v. J.C. Penney Co., CV964696 (E.D.N.Y. Oct. 8, 1996). In 1998, in conjunction with the law enforcement efforts of several state attorneys general, the Commission finalized a settlement agreement with Sears, Roebuck and Company that safeguards at least $100 million in consumer redress based on

(continued...)

the federal banking agencies about consumer protection issues involving financial services. The Commission periodically provides comments to the Federal Reserve Board regarding the Fair Credit Reporting Act, and the implementing regulations for the Truth in Lending Act, the Consumer Leasing Act, the Electronic Funds Transfer Act, and the Equal Credit Opportunity Act.[13]

In addition, the Commission has recently reported to or testified in Congress regarding the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, identity theft, and the implications of electronic payment systems for individual privacy. On July 28, 1998, for example, the Commission presented testimony before the House Committee on Banking on "pretexting." This term refers to information brokers' practice of obtaining confidential financial information for resale under false pretenses, *e.g.*, by telephoning banks and posing as the account holder.[14] The Commission believes that the act of pretexting by information brokers, which has profound implications for both financial institutions and their customers, likely violates the FTCA's prohibition of "unfair or deceptive acts or practices in or affecting commerce" and would warrant

---

[12] (...continued)
allegations that the company engaged in unfair and deceptive practices in its collection of credit card debts after the filing of consumer bankruptcy. Sears, Roebuck and Co., C-3786, 1998 FTC LEXIS 21 (Feb. 27, 1998). The Commission also worked with state attorneys general in resolving allegations against other companies that involved practices in the collection of credit card debts after the debtors had filed for bankruptcy. Montgomery Ward Corp., C-3839 (Dec. 11, 1998); May Department Stores Co., File No. 972-3189, 1998 FTC LEXIS 117 (Nov. 2, 1998).

[13] Commission staff participates in numerous task forces and groups concerned with, for example, fair lending, leasing, subprime lending, electronic commerce, and commerce on the Internet, all of which have an impact on the financial services industry.

[14] Testimony of the Commission on "Obtaining Confidential Financial Information by Pretexting" before House Committee on Banking (July 28, 1998).

filing an action in federal court to obtain injunctive and other equitable relief under Section 13(b) of the FTCA.[15]

Two of the Commission's statutory mandates are particularly relevant to the issues presently before the Subcommittee: (1) the Commission's authority to enforce the Fair Credit Reporting Act ("FCRA"); and (2) the Commission's new consumer protection role under the Identity Theft and Assumption Deterrence Act of 1998. The FCRA regulates consumer reporting agencies, also known as credit bureaus, and establishes important protections for consumers with regard to the privacy of their sensitive financial information.[16] The Commission has extensive experience enforcing the FCRA, which Congress enacted, in part, to address privacy concerns associated with the sharing of consumers' financial and credit history contained in consumer credit reports.[17] The FCRA limits the disclosure of consumer credit reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or similar purposes) and under specified conditions (such as certification from the user of the report).[18] In these ways, the FCRA operates generally to limit disclosure of consumer reports primarily to instances where a consumer initiates a transaction, such as an application for credit,

---

[15] Section 13(b) of the FTCA authorizes the Commission to seek equitable relief in federal court in cases of fraud and other serious misconduct. 15 U.S.C. § 53(b).

[16] 15 U.S.C. §§ 1681 et seq.

[17] *See, e.g.*, 15 U.S.C. § 1681(a)(4)("There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.") (emphasis added).

[18] 15 U.S.C. § 1681-1681u.

employment, or insurance.[19] The FCRA also provides consumers with certain rights in connection with the information maintained by consumer reporting agencies.[20]

The FCRA imposes civil liability for both willful and negligent noncompliance by consumer reporting agencies and parties who procure reports from (or furnish information to) such agencies.[21] It grants civil enforcement authority to the Commission, other federal agencies, and the states, to seek both monetary penalties and injunctive relief for violations of the Act.[22] The potential monetary penalties include, for those who knowingly violate the FCRA, up to $2,500 per violation in a civil action brought by the Commission in district court.[23]

---

[19] 15 U.S. C. § 1681b.

[20] 15 U.S.C. §§ 1681-1681u.

[21] 15 U.S.C. §§ 1681n-1681o.

[22] 15 U.S.C. § 1681s.

[23] 15 U.S.C. §1681s(a)(2). The Act creates a private right of action for actual damages proven by a consumer, plus costs and attorneys fees. In the case of willful violations, the court may also award punitive damages to a consumer. 15 U.S.C. § 1681n(a)(2). Any person who procures a consumer report under false pretenses, or knowingly without a permissible purpose, is liable for $1000 or actual damages (whichever is greater) to both the consumer and to the consumer reporting agency from which the report is procured. 15 U.S.C. § 1681n(b).

The FCRA also provides for criminal sanctions against parties who infringe on citizen privacy by unlawfully obtaining credit reports. The FCRA provides that "(a)ny person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses ..." may be fined and imprisoned for up to 2 years. 15 U.S.C. § 1681q. The Computer Fraud and Abuse Act prohibits unauthorized entry into credit bureau files, providing for fine and imprisonment (up to one year for a first offense, up to ten years for a second offense) of a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in . . . a file of a consumer reporting agency on a consumer, as such terms are defined in the [FCRA]." 18 U.S.C. § 1030(a)(2).

Issues relevant to the FCRA are currently pending before the Commission. In Matter of

(continued...)

Two points are worth mentioning: First, under the FCRA, merchants are free to distribute without limitation information about their own experiences with a customer.[24] In the event that large numbers of individual merchants choose to report information on their transactions with consumers directly to other merchants, it may be possible to create detailed financial profiles on consumers without the privacy safeguards provided by the FCRA.[25]

Second, the 1996 amendments to the FCRA include a provision that permits affiliated companies to share consumer information, even credit reports, free from many of the FCRA's restrictions.[26] These lessened requirements for affiliated companies sharing information may raise special concerns in the electronic banking or electronic payments context, where detailed and sometimes sensitive information about consumers is gathered.

---

[23] (...continued)
Trans Union Corporation, the Commission is currently considering an appeal from an initial decision of an administrative law judge concerning whether Trans Union's sale of target marketing lists violates the FCRA. Initial Decision of Administrative Law Judge James P. Timony, F.T.C. Docket No. 9255, ___ F.T.C. ___ (July 31, 1998).

[24] Section 603(d) of the FCRA, 15 U.S.C. § 1681a(d) ("The term "consumer report" . . . does not include (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report.").

[25] In 1997, the Commission conducted a study of database services, known as "look-up services" or "individual reference services," that make commercially available personal information used to locate and identify individuals. The study examined how such services operate and, more importantly, whether and how they may create detailed profiles on consumers containing financial and other sensitive personal information. It culminated in a report to Congress summarizing what the Commission had learned about the individual reference services industry and assessing the viability of a proposed set of industry self-regulatory principles, which portend to provide some controls on the disclosure of sensitive personal information. *Individual Reference Services: A Federal Trade Commission Report to Congress* (December 1997) [hereinafter "*IRSG Report*"].

[26] 15 U.S.C. § 1681a(d)(2)(A).

In addition to its responsibilities under the FCRA, the Commission has a new, important role to play in combating identity theft, a practice that goes to the heart of personal financial privacy. Identity theft occurs when an individual appropriates another's name, address, Social Security number, or other identifying information to commit fraud. Identity thieves may use consumers' identifying information to open new credit card accounts, take out loans in the victim's name, or to steal funds from existing checking, savings, or investment accounts.[27] Certain perpetrators go so far as illegally obtaining professional licenses,[28] driver's licenses, and birth certificates,[29] and even committing other crimes under their assumed identities.[30] Others use the consumers' identifying information to submit fake medical bills to private insurers.[31] Identity thieves often have lenders send bills to an address different from that of the victim, to conceal their activities from the victim for a prolonged period of time.[32] In the interim, the perpetrators run up debt, in some cases tens of thousands of dollars, under their assumed identities.[33]

Recently, the Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime and authorized the FTC to serve as a central clearinghouse to receive complaints

---

[27] B. Givens, The Privacy Rights Handbook 231-32 (1997).

[28] Official Transcript of "FTC Consumer Identity Fraud Meeting," August 20, 1996 [hereinafter "ID Theft Transcript"] at 12-13. A copy of the transcript is available online at *<http://www.ftc.gov/ftc/conferences/htm>*.

[29] *See, e.g., IRSG Report,* at 17.

[30] Givens, *supra* note 2, at 231.

[31] E. Hendricks, *Identity Theft Key to Major Medical Fraud Operation*, Privacy Times, Feb. 6, 1998, Vol. 18, No. 3, at 3-4.

[32] ID Theft Transcript at 11-12.

[33] *See, e.g., IRSG Report* at 17; Givens, *supra* note 2, at 232.

from, and provide information to, victims of identity theft.[34] Specifically, the Act requires the Commission to establish procedures to (1) log the receipt of complaints by victims of identity theft; (2) provide these victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.

To meet these new statutory responsibilities, Commission staff has begun work on a plan that centers on three principal components: (1) creating a toll-free telephone number to assist consumers who have been victims of identity theft;[35] (2) maintaining a database to track and analyze identity theft complaints received by the FTC and others, and to assist law enforcement authorities in their investigations; and (3) preparing educational materials to provide guidance to consumers on how to prevent identity theft and what to do if they become an identity theft victim.

C. The FTC's Role in Online Privacy

Commerce on the Internet falls squarely within the scope of the Commission's statutory authority under the FTCA. The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace and has held a series of workshops and hearings on such issues, including the special privacy concerns raised by the online collection of

---

[34] PL 105 - 318, 112 Stat. 3007, amending 18 U.S.C. § 1028 (1998).

[35] It is estimated that public and private entities, including the three major credit bureaus, receive over 500,000 identity theft complaints a year. This help line will supplement, but is not intended to replace entirely, these existing means of receiving complaints.

financial information.[36] Throughout, the Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online. The Commission's efforts to encourage self-regulation have included bringing industry and consumer and privacy advocates together to address online privacy issues at our workshops, and meeting with, and encouraging, industry leaders to adopt effective self-regulatory programs. These efforts have been based on (1) the understanding that personal information can be collected and widely disseminated on the World Wide Web with unprecedented ease, and (2) the belief that greater protection of personal privacy on the Web will not only protect consumers, but also increase consumer confidence and ultimately consumers' participation in the online marketplace.

---

[36] The Commission held its first public workshop on privacy in April 1995. In a series of hearings held in October and November 1995, the FTC examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers' personal information, including sensitive medical and financial information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission published a summary of the workshop testimony in a December 1996 staff report entitled *Consumer Privacy on the Global Information Infrastructure*. The agency also held a four-day workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

These FTC efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g.*, *IRSG Report*; FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996; FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, May 1996.

In June 1998 the Commission issued a comprehensive report on Internet privacy, *Privacy Online: A Report to Congress* (the "Report").[37] The Report described four fair information practice principles: that consumers be given **notice** of how information collected from them is used by online companies and **choice** regarding intended uses of their information; the need for **consumer access** to personal information maintained in online companies' files; and online companies' responsibility to take steps to ensure the **security and integrity** of the personal information they maintain. The Report set out the findings of the Commission's extensive March 1998 survey of the information practices of some 1,400 commercial Web sites, and assessed the effectiveness of self-regulatory efforts to date in protecting consumer privacy.

The survey included a subsample of 125 sites operated by banks, credit unions, mortgage companies, real estate agencies, security and stock brokerages, investment and asset management firms, venture capital firms, and other companies offering financial products and services. Commission staff found that although almost all of these sites were collecting identifying personal information together with very sensitive financial information, very few were disclosing their information practices.

The Commission's survey findings, as well as its review of then existing industry information practice guidelines, led it to conclude that, at least as of June 1998, an effective self-regulatory system had yet to emerge. The Report recommended that the Congress consider legislation governing the online collection of personal information from consumers generally, if

---

[37] The Report is available on the Commission's Web site at www.ftc.gov/reports/privacy3/index.htm.

effective self-regulation does not take hold.[38] Since the Report was issued, several major self-regulatory initiatives have emerged to develop industry guidelines to protect the privacy of personal information, including the important work of the Banking Industry Technology Secretariat (B.I.T.S.).[39] In addition, a privately funded study of commercial Web sites' information practices is scheduled to take place later this month. We are hopeful that this study will provide an objective measure that informs the Commission's views on the current state of self-regulation to implement online privacy protections. The Commission is monitoring these developments with great interest and will keep the Congress informed of their results.

III. Conclusion

It is clear that consumers are extremely concerned about the privacy of their sensitive financial information. In addition, it would appear that large numbers of commenters perceive that the Know Your Customer proposals contemplate government invasion of privacy. These

---

[38] Both in the Report and in subsequent Congressional testimony, the Commission recommended that Congress consider legislation to address the online collection of identifying personal information from young children. Report at 42-43; Testimony on "Consumer Privacy on the World Wide Web" before Subcommittee on Telecommunications, Trade and Consumer Protection, House Committee on Commerce (July 21, 1998) at 13-19. On October 21, 1998, President Clinton signed the Children's Online Privacy Protection Act (COPPA), which requires that Web sites that collect identifying personal information from children under the age of thirteen implement safeguards to ensure parental involvement and control in the collection and use of their children's personal information. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1999, Pub. Law 105-277, 112 Stat. 2681, ___ (October 21, 1998). The COPPA authorizes the Commission to promulgate regulations to effectuate the statutory principles of parental notice and consent, as well as other required fair information practices. The Commission soon will initiate a rulemaking proceeding under the Act.

[39] B.I.T.S. was established in 1996 by the Bankers Roundtable, a consortium of the 125 largest banks in the United States, to examine issues related to electronic payment systems, including infrastructure security issues and consumer privacy.

perceptions are significant. At the same time, the Commission is mindful of the importance of establishing mechanisms to prevent crimes such as money laundering and fraud. The public response to the Know Your Customer proposals highlights the tension between potential regulatory initiative and privacy concerns. The Commission is pleased to serve as a resource as this Subcommittee and others consider how to strike the proper balance between these important competing interests.