PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON

"Obtaining Confidential Financial Information by Pretexting"

Before the
COMMITTEE ON BANKING AND FINANCIAL SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

July 28, 1998

Mr. Chairman and members of the Committee: I am Mozelle W. Thompson, Commissioner of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of pretexting by information brokers to obtain an individual's confidential financial information.[(1)]

I. Introduction

A. Overview

"Pretexting" is a term coined by the private investigation industry, and refers to the practice of obtaining personal information under false pretenses. For example, an investigator who obtains a bank account balance by posing as the account holder would be engaged in pretexting. This tactic is perhaps as old as the private investigation industry itself. But it appears to be gaining in popularity -- especially in the burgeoning Internet marketplace -- because of the booming market for comprehensive personal information. Now, increasing numbers of high-tech private eyes, also known as "information brokers," are touting their ability to obtain surprisingly sensitive information without the subject ever knowing. The Web sites of certain companies also imply that they can retrieve this information by simply keying a few search terms into one of their many databases, and that such services are perfectly legal. Despite such claims, it appears that the companies can get this information only one way . . . through plain, old-fashioned lies, *i.e.*, through pretexting.

The Commission has long been concerned about consumer privacy and supports the Committee's efforts to address the practice of pretexting to obtain consumers' financial information. Today I will discuss four issues relating to the Commission and information brokers who engage in pretexting to obtain confidential financial information ("pretexters"): (1) the Commission's work in the area of consumer information privacy; (2) the extent to which a self-regulatory agreement entered into by one subset of the information broker industry -- "individual reference services" or "look-up services" -- addresses this issue; (3) the extent to which the Federal Trade Commission Act empowers the Commission to combat the practice of pretexting to obtain confidential information; and (4) the extent to which the Financial Information Privacy Act of 1998, if enacted,

would facilitate the Commission's ability to address these practices.

B. The Role of the FTC

The mission of the FTC is to promote and preserve consumer welfare through its jurisdiction over both consumer protection and competition issues. The Commission undertakes this mission by enforcing the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] With the exception of certain industries,[(3)] the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce, and the FTCA provides the agency with authority to gather information about such entities.[(4)] The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices. Of particular relevance here is the Commission's authority to enforce the Fair Credit Reporting Act ("FCRA"). The FCRA regulates credit reporting agencies, also known as credit bureaus or consumer reporting agencies, and establishes important protections for consumers with regard to the privacy of their sensitive financial information.[(5)] Thus, it is within the Commission's mandate and expertise to address the practice of obtaining confidential financial information through deception and offering such information for resale.

II. Consumer Information Privacy

Since 1995, the Commission has actively sought to identify and address consumer protection issues relating to the increasing availability of personal identifying information in the electronic marketplace. For example, the Commission and its staff have convened a series of public workshops on online privacy and issued several reports examining industry practices, relevant self-regulatory efforts and technological developments, consumer and business education efforts, and the appropriate role of government in protecting privacy.[(6)]

In 1997, the Commission conducted and published a study of computer database services, known as look-up services or individual reference services, that make available personal identifying information used to locate and identify people.[(7)] This study prompted the individual reference service industry to develop a self-regulatory program, which is discussed in more detail below. In addition, the Commission has held public meetings to examine and address the impact of identity theft on consumer victims.[(8)]

In March 1998, to measure the efficacy of self-regulation in protecting privacy in the online marketplace, the Commission surveyed over 1400 commercial Web sites and examined the extent to which they disclose their information practices. The agency reported its findings to Congress in June 1998, and testified last week before the House Subcommittee on Telecommunications, Trade and Consumer Protection on further findings and recommendations concerning online privacy.[(10)] The Commission also presented testimony at several prior Congressional hearings focusing on consumer information privacy issues.[(11)] The Commission has learned through its work in this area

that consumers care deeply about the privacy of their personal information.[12]

The Commission also has extensive experience enforcing the FCRA, which gives consumers certain privacy protections regarding their sensitive financial information. Congress enacted the FCRA to address privacy concerns associated with the sharing of consumers' financial and credit history, typically contained in consumer credit reports.[13] The FCRA provides that consumer credit reports may be distributed only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or similar purposes) under specified conditions (such as certification from the user of the report), and provides for certain consumer rights in connection with the information maintained by consumer reporting agencies.[14]

III. Applicability of the IRSG Principles

In addition to this extensive work on consumer privacy, the Commission has also worked closely with industry on a self-regulatory initiative by the "individual reference services group," a subset of the information broker industry. Individual reference services are database services that make available personal identifying information, such as an individual's name, address, aliases, Social Security number, and date of birth, for use in locating and identifying people. In 1997, the Commission conducted a study of concerns associated with individual reference services. In particular, the Commission considered whether the increasing availability of this information poses various risks of harm to consumers' privacy and financial interests, including the possibility of increasing the incidence of identity theft. In response, 14 companies, comprising most of the industry, developed and agreed to a set of self-regulatory principles, the "IRSG Principles."[15]

The IRSG Principles, which become effective December 31, 1998, impose obligations on signatories regarding how they collect and provide access to information.[16] While the Principles specifically address only personal identifying information, and not the more comprehensive financial information at issue here, we are hopeful they nevertheless will limit the extent to which information brokers can engage in "pretexting" to obtain financial information.

First, if the IRSG Principles work as we anticipate, they will prevent signatories from engaging in pretexting to obtain information for resale.[17] The Principles require IRSG participants to obtain information only from "sources known as reputable in the government and private sectors" and to maintain a policy of "openness" regarding the types of information they have, their sources, and how information is collected.[18] Obtaining confidential information under false pretenses would therefore be inconsistent with the spirit, if not the letter, of the Principles.

Second, by limiting access to identifying information, the IRSG Principles should make it more difficult for others to engage in pretexting. Indeed, pretexters need identifying information, such as Social Security number or date of birth, to convince third-party custodians (like banks) that they are entitled to obtain the more sensitive information, and they may try to obtain that information from individual reference services.[19] However, the

Principles provide that if such identifying information is obtained from *non-public* or *proprietary* sources,[(20)] a customer may access it only if: (1) the customer meets qualification requirements establishing it as an "appropriate"[(21)] user of the information sought and (2) reasonable measures are employed to ensure that the information is actually used "appropriately."[(22)] The practice by an IRSG participant of selling information to pretexters who use it to obtain confidential information would be inconsistent with the IRSG Principles.

Finally, because IRSG participants include suppliers of information to the reference services industry (including the national credit reporting agencies), the IRSG Principles should have broad application. The Principles prohibit information suppliers from selling non-public information to individual reference services whose practices are inconsistent with the Principles, whether or not they participate as signatories. Thus, the suppliers would be prohibited from selling information to any individual reference services that offer for resale information obtained through pretexting, as well as to individual reference services whose customers use the information for pretexting. Moreover, the risk of losing the ability to purchase proprietary personal identifying information for resale should deter individual reference services from themselves engaging in pretexting and from selling information to customers who do.

Notwithstanding whether the IRSG Principles succeed in preventing pretexting under the circumstances described above, their effect will still be limited to individual reference services, just a subset of the information brokering industry, and those that deal directly with that industry. More specifically, the Principles will not apply where the information broker (1) is not itself an individual reference service; or (2) does not obtain information from an individual reference service; or (3) obtains from an individual reference service information that is not from a non-public source, *e.g.*, public records.

IV. FTC Authority to Combat the Act of Pretexting to Obtain Confidential Information

Given the limitations of the IRSG Principles, the Commission will need to address the problem of pretexting by doing what it does best -- law enforcement. Indeed, although the Commission encourages industry self-regulation, the Commission is first and foremost a civil law enforcement agency, whose mandate is to combat unfair and deceptive practices. And the practice of obtaining confidential information for resale under false pretenses appears to be just that -- unfair and deceptive.

In cases of unfairness or deception, the Commission can issue administrative complaints, conduct administrative adjudications, and issue cease and desist orders.[(23)] Further, in cases of fraud and other serious misconduct, Section 13(b) of the FTCA authorizes the Commission to seek injunctive and other equitable relief in federal court.[(24)] In a Section 13(b) action, a court may exercise the full breadth of its equitable authority, including the issuance of a permanent injunction and "any ancillary relief necessary to accomplish complete justice."[(25)] This authority includes the power to order consumer redress and to compel disgorgement of a defendant's ill- gotten gains.[(26)] The Commission has filed over

500 Section 13(b) cases in federal court.

We believe the act of pretexting by information brokers likely violates the FTCA's prohibition of "unfair or deceptive acts or practices in or affecting commerce" and would warrant filing a Section 13(b) action in federal court to obtain equitable relief.[(27)] First, making misrepresentations to a financial institution to obtain confidential information for resale may be a *deceptive* act affecting commerce.[(28)] Second, representing to customers that information will be obtained legally, when in fact it can be obtained only through actions that likely violate the FTCA and certain other statutes[(29)] may also be a *deceptive* act affecting commerce.[(30)]

In addition, obtaining and reselling a consumer's confidential financial information may be *unfair* acts, in violation of Section 5. To establish an unfairness theory, the Commission must show (1) that the practice of obtaining consumers' private financial information without permission or under false pretenses causes, or is likely to cause, substantial injury; (2) that the injury is not outweighed by countervailing benefits to consumers or competition; and, (3) that consumers could not have avoided the injury.[(31)]

First, we believe that the invasion to consumers' privacy observed here may constitute substantial injury.[(32)] In some instances, the ability of a third party to use a consumer's financial information can cause substantial monetary harm. In assessing injury, a court may consider, among other things, whether the conduct violates public policy as established by "statute, common law, industry practice, or otherwise."[(33)] The value our society places on protecting the privacy of financial information is demonstrated by federal statutes that protect the confidentiality of individuals' financial information such as the Fair Credit Reporting Act,[(34)] the Right to Financial Privacy Act,[(35)] the Electronic Fund Transfer Act,[(36)] as well as numerous state statutes,[(37)] state court decisions holding that banks have an implied duty to maintain the confidentiality of financial information,[(38)] and the precautionary practices employed by the banking industry to protect their account holders' information.[(39)]

Second, harmed consumers, because they typically have no way of knowing that an information broker was attempting to access their financial information, cannot avoid the injury. Finally, using false pretenses to obtain confidential bank account information appears to provide no countervailing benefit to consumers or competition.[(40)]

In short, we believe the Commission likely would succeed in a law enforcement action against pretexters, either on a deception or unfairness theory. We also believe that we could obtain significant remedial relief, including a permanent injunction against the practices, disgorgement of ill-gotten gains, and/or consumer redress.

V. The Financial Information Privacy Act

The Commission believes the legislation proposed by Chairman Leach, H.R. 4321, the Financial Information Privacy Act of 1998 (the "Act"), if enacted, it would (1) specify expressly for courts and information brokers that pretexting to obtain confidential financial

information violates the FTCA; and (2) deter information brokers from pretexting by authorizing the imposition of civil and criminal sanctions.[41]

The Act would add an important tool to the Commission's arsenal in a case against pretexters -- the ability to obtain to civil penalties.[42] Since 1975, the Commission had authority to seek civil penalties for violations of its trade regulation rules.[43] In addition, the Commission enforces several statutes, including the Equal Credit Opportunity Act, the Fair Debt Collection Practices Act, and the Fair Credit Reporting Act, which give the Commission civil penalty authority.[44] It has been the Commission's experience that sanctions that go beyond merely ordering future compliance with the law, such as civil penalties, provide stronger incentives for compliance.

The imposition of civil penalties would be particularly appropriate against pretexters, given the invasive and deliberate nature of their practices. Further, because a civil penalty could easily exceed the amount a pretexter would have to pay for disgorgement or consumer redress,[45] it could more effectively deter the practices at issue. Indeed, deterring the practices from occurring in the first place is especially important here, where the real consumer injury -- *i.e.*, the serious privacy invasion to individuals being investigated -- may be difficult to quantify and therefore to redress.[46]

In addition to bolstering the Commission's authority, the Act would enable states and private individuals to bring civil actions, and criminal agencies to impose sanctions. While the possibility of facing criminal sanctions would provide an important deterrent to potential offenders, it would not obviate the need for the FTC's civil penalty authority. In an era of limited resources and increasing caseloads, civil penalty enforcement by the Commission would both complement and provide an effective alternative to criminal prosecution.[47]

In sum, although the Commission's current authority would allow it to obtain significant injunctive and remedial relief against pretexters, we believe that a law specifically designating the act of obtaining confidential financial information through pretexting as an FTCA violation subject to civil penalties would enhance our effectiveness in combating this practice.

VI. Conclusion

Pretexting is a troubling, and apparently growing, problem facing consumers. The disclosure of a consumer's sensitive bank account or other sensitive information is a significant privacy invasion, with potentially serious financial consequences. While the Commission is able to stop many of these practices and obtain significant remedial relief, civil penalty authority would make the Commission's enforcement actions even more effective and would substantially increase the deterrent effect of such actions. The Commission looks forward to working further with this Committee to respond to the problem of pretexting.

1. The views expressed in this statement represent the views of the Federal Trade Commission. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission.

2. 15 U.S.C. § 45(a).

3. 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).

4. 15 U.S.C. § 46.

5. 15 U.S.C. §§ 1681 *et seq.*

6. The Commission held its first public workshop on Internet 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 and consumer protection issues, including privacy concerns. This workshop culminated in an FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, May 1996. At a public workshop in June 1996, the Commission examined a wide range of consumer privacy issues, including Web site practices with respect to the collection and use of consumers' personal information. FTC staff issued a report summarizing this workshop. FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996. The agency held a four-day workshop in June 1997 to explore issues relating to unsolicited commercial e-mail, online privacy, children's online privacy, and individual reference services.

7. In connection with the Commission's study of this industry, the Commission solicited public comment and held a Public Workshop in June 1997, which served as a forum for dialogue among suppliers of personal identifying information such as credit reporting agencies, the direct providers of look-up services, commercial users of the services, government representatives, and consumer and privacy advocates. The study culminated in a report from the Commission to Congress in December 1997. The report summarized what the Commission had learned about the individual reference services industry; examined the benefits, risks, and potential controls associated with these services; assessed the viability of an industry self-regulatory proposal; and concluded with recommendations that address concerns left unresolved by the proposal. *See generally Individual Reference Services*: A *Federal Trade Commission Report to Congress*, December 1997 (hereinafter "IRSG Report").

8. In August 1996, the FTC brought together consumer victims of identity theft, law enforcement representatives, members of the credit industry, and consumer and privacy advocates to discuss the impact of identity theft.[(9)]

9. *Id.*

10. *Privacy Online: A Federal Trade Commission Report to Congress*, June 1998 (hereinafter "Privacy Online Report"); *see* Hearing on "Consumer Privacy on the World Wide Web" before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, July 21, 1998 (Statement of the Federal Trade Commission).

11. *See, e.g.*, Hearing on "Effects of Consolidation on the State of Competition in the Financial Services Industry" before the House Committee on the Judiciary, June 3, 1998 (Statement of the Federal Trade Commission); Hearing on "Identity Theft" before the Senate Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, May 20, 1988 (Statement of the Federal Trade Commission); Hearing on "Internet Privacy" before the House Subcommittee on Courts and Intellectual

Property, Committee on the Judiciary, March 26, 1998 (Statement of the Federal Trade Commission); Hearing on "The Implications of Emerging Electronic Payment Systems on Individual Privacy" before the House Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services, September 18, 1997 (Statement of the Federal Trade Commission).

12. *See, e.g.*, Privacy Online Report at 3-4; IRSG Report at 13.

13. *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).

14. 15 U.S.C. §§ 1681-1681u.

15. IRSG Report at Appendix D.

16. Signatories to the agreement must undergo an annual compliance review by a professional third party, the results of which will be made public. Public examination of the results of compliance reviews and the possibility of liability for deception under the FTC Act and similar state statutes should create an incentive for compliance by signatories.

17. The Commission has no reason to believe that current signatories engage in pretexting. The personal identifying information typically sold by individual reference services is available from public records and from "credit headers" supplied by credit reporting agencies. (Credit headers typically contain name, aliases, current and former addresses, phone number, Social Security number, date of birth, and mother's maiden name). However, it is possible that an individual reference service could sell comprehensive, financial information of the type at issue here in addition to identifying information.

18. IRSG Report at Appendix D.

19. *See* IRSG Report at n. 176 (discussing private investigators who obtain identifying information from look-up services and use it for pretexting).

20. To the extent information obtained from a non-public source is publicly available, such as a home address obtained from a credit reporting agency but also listed in the phone book, that information is *not* treated as non-public and therefore not restricted under the IRSG Principles.

21. Appropriate is defined as "reasonable under the circumstances reflecting a balance between the interests in individual privacy and legitimate business, governmental, and personal uses of information, including prevention and detection of fraud." IRSG Report at Appendix D.

22. IRSG Report at Appendix D. The Principles' restrictions on access to information vary according to three categories of customers. The categories are a function of the type of information sought (*e.g.*, Social Security number vs. phone number) and how it will be used (*e.g.*, enforcing the law vs. locating an old friend). The discussion in the text focuses on access restrictions applicable to the first category, "qualified subscribers," the only category that can access the kind of specific information that is most likely to be useful in pretexting, *e.g.*, non-public Social Security number, full date of birth, and mother's maiden name. Information brokers could obtain less specific non-public information, such as a *truncated* Social Security number and the month and year of birth, under the second category -- "commercial or professional users." However, this less specific information likely would not be sufficient to enable information brokers to pretext, and they therefore would have little incentive to obtain information under this category. Moreover, because the information brokers still would be required to use the information "appropriately," using it to pretext still would still violate the Principles. Finally, the information available to the general public, the third category,

e.g., name, address, and telephone number unlikely would facilitate pretexting.

23. 15 U.S.C. § 45.

24. 15 U.S.C. § 53(b).

25. *FTC v. H.N. Singer, Inc*., 668 F.2d 1107, 1113 (9th Cir. 1982); *see also FTC v. Gem Merchandising Corp.*, 87 F.3d 466, 468-69 (11th Cir. 1996); *FTC v. U.S. Oil & Gas*, 748 F.2d 1431, 1434 (11th Cir. 1984).

26. *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1103 n.34 (1994), *cert. denied*, __ U.S. __., 115 S. Ct. 1794 (1995); *FTC v. Gem Merchandising Corp.*, 87 F.3d at 469-70. However, the FTCA does not authorize the imposition of civil penalties for an initial violation, unless the statute or rule at issue so provides.

27. The Commission could also pursue this practice administratively. However, this approach would not afford the quick relief warranted here, and would not provide for consumer redress or civil penalties in the initial proceeding. Moreover, if the Commission were to discover that entities were obtaining confidential financial information by accessing consumer credit reports without a permissible purpose, the Commission could bring an action under the Fair Credit Reporting Act to stop such practices. *See* n. 5 and accompanying text.

28. The Commission has determined that a representation, omission, or practice is deceptive if: (1) it is likely to mislead consumers acting reasonably under the circumstances; and (2) it is material. *Stouffer Foods Corporation*, 118 FTC 746 (1994); *Cliffdale Associates, Inc*., 103 F.T.C. 110, 164-65 (1984); *see generally* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Associates, Inc*., 103 F.T.C. at 174 (1994). Here, the misrepresentation of one's identity in order to obtain account information is likely to be both misleading and material: the financial institution is led to believe that it is speaking to the account holder, and, based on this misperception, is likely to disclose the account information.

Significantly, the Commission believes that Section 5 prohibits misrepresentations to induce the disclosure of personal information, even when there is no commercial relationship between the defendant and the entity disclosing the information. *See, e.g., Equifax, Inc*., 96 F.T.C. 844, 1107 (1980) (misrepresentations to induce patients and physicians to disclose personal medical information violated Section 5). *See also FTC v. Universal Credit Corp*., No. SA CV 96-114 LHM (EEX) (C.D. Calif. Filed Feb. 7, 1996) (misrepresentations to induce consumers to disclose bank account information violated Section 5); *Beneficial Corp*., 86 F.T.C. 119 (1975), *aff'd*, 678 F.2d 611 (3rd Cir. 1976), *cert. denied*, 430 U.S. 983 (1977) (failure to disclose that financial information disclosed for tax preparation would also be used to market company's loans violated Section 5). In addition, Section 5 prohibits acts and practices that deceive businesses, not just individuals. *See Equifax*, 96 F.T.C. at 848 (misrepresentations to business users regarding the source of information contained in consumer reports violated Section 5).

29. *E.g.*, 42 U.S.C. § 408(a)(7) (criminalizing the act of falsely representing, with intent to deceive, a number as the Social Security number assigned to oneself or another); 18 U.S.C. § 1343 (criminalizing the act of wire fraud).

30. Misrepresenting the source of information gathered for resale has been found to be unfair or deceptive. *E.g., Equifax*, 96 F.T.C. at 1109 (1980) (consumer reporting agency's practice of falsifying the sources of adverse information when preparing consumer reports found to be unfair or deceptive). Further, courts have granted permanent and temporary injunctive relief based on allegations that entities misrepresenting the legality of their services violate Section 5. *E.g., FTC v. COS Co.*, Civ. No. C 92 1577 BAC (N.D. Cal. filed April 26, 1992) (permanent injunction granted against credit repair service alleged to have misrepresented the legality of service)*; FTC v. Second Federal Credit Inc.* No. 98-10348NG (D. Mass. filed Feb. 26, 1998) (TRO granted against credit repair service alleged to have misrepresented the legality of service); *FTC v. Corzine*, No. CIV-S-94-1446 (E.D. Cal. filed Sept. 12, 1994) (TRO granted against credit repair service

alleged to have misrepresented legality of service).

31. *See* Section 5(n) of the FTCA, 15 U.S.C. § 45(n), *added* by the FTCA Amendments of 1994, Pub. L. No. 103-312. *See also* FTC *Policy Statement on Unfairness, appended to International Harvester Co.*, 104 F.T.C. 1070 -76 (1980).

32. *See, e.g., Beneficial Corp.*, 86 F.T.C. 119 (1975), *aff'd*, 678 F.2d 611 (3rd Cir. 1976), *cert. denied*, 430 U.S. 983 (1977).

33. FTC *Policy Statement on Unfairness*, 104 F.T.C. at 1075 (1980); *see also* 15 U.S.C. § 45(n).

34. 15 U.S.C. § 1681 *et seq.*

35. 12 U.S.C. § 3401 *et seq.*

36. 15 U.S.C. § 1693 *et seq.*

37. *See American Banker's Association's Financial Privacy in America: A Review of Consumer Financial Services Issues*, June 1998 at App. A, *American Banker's Association, Consumer Protection Issues* (last modified 7/6/98) <http://www.aba.com/abatool/showme_rel.html?location=PR_Privacy.htm> (hereinafter "ABA Report").

38. *See, e.g., Rubenstein v. So. Denver Nat'l Bank*, 762 P.2d 755,757 (Colo. Ct. App. 1988); *Suburban Trust Co. v. Waller*, 408 A.2d 758,762 (Md. Ct. Spec. App. 1979).

39. *See generally* ABA Report.

40. The Commission has held that a breach of information privacy can form the basis of a Section 5 unfairness violation. In *In the Matter of Beneficial Corp.*, the Commission concluded that an income tax preparation service's practice of using confidential financial information from customers' tax returns to market its consumer credit services was both a deceptive and unfair practice in violation of Section 5. 86 F.T.C. at 134-36. The Commission based its finding of unfairness on society's concerns regarding the confidentiality and proper use of personal tax data and suggested that the violation of a generalized right to privacy in a commercial context would likely violate Section 5. *Id.* at 131.

41. If the Committee believes it would be helpful, the Commission is interested in working with Committee staff to refine the bill to complement the Commission's existing authority. For example, to establish a Section 5 violation, the bill as currently drafted would require the Commission to prove that a violator knowingly engaged in deception. Under our existing authority, a showing of knowledge is required only: (1) to prove the liability of officers or other individuals or (2) to impose civil penalties for rule violations or when otherwise required by statute. Thus, the knowledge requirement would be consistent with our current civil penalty authority, but would heighten our burden in obtaining equitable relief -- redress and injunctive provisions -- under the FTCA.

42. If, however, the entities were found to have violated the FCRA (as discussed at n. 26 *supra*), the Commission could seek civil penalties of up to $2500 per violation. Section 621 of the FCRA, 15 U.S.C. § 1681s.

43. *See* Section 5(m)(1)(A) of the FTCA. 15 U.S.C. 45(m)(1)(A). Thus, the FTC may obtain civil penalties for certain rule violations: *e.g.*, Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations (the "Cooling-Off Rule"), 16 C.F.R. Part 429; Mail or Telephone Order Merchandise Rule, 16 C.F.R. Part 435; Franchise and Business Opportunity Rule, 16 C.F.R. Part 436.1; Funeral Rule, 16 C.F.R.

Part 453; Holder in Due Course Rule, 16 C.F.R. Part 433; Credit Practices Rule, 16 C.F.R. Part 444. In addition, the Commission may seek civil penalties for other rule violations, as authorized specifically by certain statutes: *e.g.*, Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act of 1992 ("The 900-Number Rule"), 16 C.F.R. Part 308; and the Telemarketing Sales Rule Pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 16 C.F.R. Part 310.

44. Section 704(c) of the Equal Credit Opportunity Act; Section 814(a) of the Fair Debt Collection Practices Act; Section 621 of the Fair Credit Reporting Act.

45. The amount of consumer redress or disgorgement the defendant would have to pay would likely correspond to the amount customers pay for these services, typically a few hundred dollars per transaction. On the other hand, if the Commission had the civil penalty authority proposed in the Act, the defendants could have to pay as much as $11,000 per violation.

46. If the pretexter were making misrepresentations to customers regarding how it obtains financial information (*i.e.*, falsely stating that the information is obtained legally), the harm from such misrepresentations (*i.e.*, the fees they paid) probably would be quantifiable and possible to redress. Not all pretexters make this misrepresentation, however. Further, as discussed above, the true harm is the privacy invasion of the individuals being investigated.

47. In response to similar points raised by the Commission with respect to amendments to the Fair Credit Act, Congress decided to grant the Commission civil penalty authority for FCRA violations. Hearing on "Fair Credit Reporting Act" before the House Committee on Banking, Finance, and Urban Affairs, Sept. 13, 1989 (Statement of Federal Trade Commission).