PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
"IDENTITY THEFT"

Before the

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM
AND GOVERNMENT INFORMATION

of the

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

Washington, D.C.
May 20, 1998

Mr. Chairman and members of the Committee: I am David Medine, Associate Director for Credit 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 identity theft.[(1)]

I. Introduction

A. Overview

Identity theft goes to the heart of personal privacy. It 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.[(2)] Certain perpetrators go so far as illegally obtaining professional licenses,[(3)] driver's licenses, and birth certificates,[(4)] and even committing other crimes under their assumed identities.[(5)] Others use the consumers' identifying information to submit fake medical bills to private insurers.[(6)] 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.[(7)] In the interim, the perpetrators run up debt, in some cases tens of thousands of dollars, under their assumed identities.[(8)]

The Commission supports the Committee's efforts to address this growing problem. The FTC has also taken a proactive role in identifying consumer protection issues relating to the increased availability of personal identifying information, including identity theft.[(9)] I will discuss the FTC's actions and findings in four areas that relate to identity theft. First, I will discuss what the FTC has learned about how identity theft occurs and how it affects consumers. Second, I will address how the Identify Theft and Assumption Deterrence Act of 1997, if enacted, would provide relief to consumer victims of identity

theft. Third, I will describe the FTC's efforts with respect to "individual reference services," also known as "look-up services." Individual reference services are computerized database services that are used to locate, identify, or verify the identity of individuals. These services increase the availability of personal identifying information about consumers. They are relevant to this discussion in that, while they confer societal benefits, they also have the potential to increase the incidence of identity theft if not adequately controlled. Finally, I will discuss certain steps consumers can take to avoid becoming victims of identity theft.

B. The Role of the FTC

The consumer protection mission of the FTC is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by ensuring vigorous competition. 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.[(10)] With the exception of certain industries, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce,[(11)] and with the authority to gather information about such entities.[(12)] The Commission also has responsibility under approximately thirty additional statutes governing specific industries and practices. Of particular relevance is the Commission's authority to enforce the Fair Credit Reporting Act, the Truth in Lending Act, and the Fair Credit Billing Act. The Fair Credit Reporting Act regulates credit reporting agencies, also known as credit bureaus or consumer reporting agencies, and establishes important protections for consumers with regard to the accuracy of their credit reports, or consumer reports, and the privacy of their sensitive financial information.[(13)] The Truth in Lending Act, amended by the Fair Credit Billing Act, provides for the correction of billing errors on credit accounts and limits consumer liability for unauthorized credit card use.[(14)] Because identity theft can result from the availability of sensitive identifying information from credit bureaus and can affect the accuracy of consumer credit reports and credit account records, examining the causes and consequences of identity theft and exploring potential solutions fall within the scope of the Commission's mandate.

II. Identity Theft

In an effort to learn more about identity theft, its growth, consequences, and possible responses, the Commission convened two public meetings. At an open forum held in August 1996, consumers who had been victims of this type of fraud, representatives of local police organizations and other federal law enforcement agencies, members of the credit industry, and consumer and privacy advocates discussed the impact of identity theft on industry and on consumer victims.[(15)] Subsequent press coverage helped to educate the public about the growth of consumer identity theft and the problems it creates.[(16)] In November 1996, industry and consumer representatives reconvened in working groups to explore solutions and ways to bolster identity theft prevention programs.[(17)] As a result of these two meetings, the Commission developed a substantial

base of information about identity theft.

A. The Problem

Creditworthy consumers with high incomes appear to be the preferred prey of identity thieves.[(18)] Once the perpetrators identify their victims, they seek relevant identifying information, such as their Social Security numbers. The Social Security number is the one piece of information that most facilitates identity theft, as it opens the door to an individual's financial life -- providing access to checking accounts, savings accounts, brokerage accounts, etc.[(19)] Social Security numbers and other unique identifiers can be gleaned from a variety of sources, including public records (like certain department of motor vehicle records),[(20)] student transcripts, medical insurance records,[(21)] survey response forms,[(22)] and even warranty cards.[(23)]

Historically, identity thieves have accomplished their crimes through simple means -- pickpocketing wallets, stealing pre-approved credit applications from mailboxes, or raiding trash dumpsters for discarded receipts and files.[(24)] Recently, more sophisticated schemes are gaining popularity. One such method is securing low-level employment with a financial institution or other entity that gives the perpetrator access to consumer credit reports or other identifying data, for their personal exploitation or for use by organized identity theft rings.[(25)] For example, one fraud ring used such credit reports quickly to acquire fake I.D. cards, open "instant credit" accounts, and then run up thousands of dollars in debt.[(26)] A recent case brought by the United States Secret Service demonstrates how computer-savvy identity thieves may exploit information available over the Internet. In that case, the defendants were a Maryland couple who pled guilty in September 1997 to running up debt exceeding $100,000 under their stolen identities. They admitted to routinely using Internet databases to select their victims.[(27)]

B. Impact on Consumers and Inadequacy of Remedies

The harm to consumer victims of identity theft tends to be significant and long-lasting, yet it may not be readily apparent or easily quantifiable. The perpetrators' failure to make credit card and loan payments on victims' hijacked accounts or new accounts opened fraudulently in victims' names severely damages the victims' credit ratings.[(28)] Until consumer victims can clear their names (which could take years), they may be denied loans, mortgages, security clearances, promotions, and employment.[(29)] The following identity theft examples are illustrative: One victim, a NASA engineer, was refused a loan by his bank of eleven years, and had to use his retirement funds to finance his son's education.[(30)] A second victim, who spent three years trying to repair her damaged credit rating, was deprived of the chance to buy what she describes as her dream home.[(31)] Another was the target of an arrest warrant for a domestic battery crime she did not commit.[(32)] A fourth victim, a department store clerk whose identity had been assumed by a shoplifter, spent years unsuccessfully seeking employment in the retail industry.[(33)]

These and other consumer victims of identity theft suffer real harm. That harm, however, is underestimated because consumers typically do not bear the initial financial brunt of

identity theft.[34] Federal law limits a consumer's liability for credit card fraud to $50 per account in these situations,[35] and lenders often forgo even that amount.[36] Accordingly, financial institutions tend to be viewed as the primary victims of identity theft and their direct financial loss tends to be viewed as the only loss.[37] Such a measure of injury fails to reflect not only the loss of potential benefits described above but also the years of aggravation suffered by consumer victims.

It is often difficult for consumers to cleanse their credit reports of the perpetrators' bad acts.[38] The victims must go through the time-consuming process of (1) trying to prove to lenders and credit reporting agencies that they were in fact victimized by identity theft, and did not personally incur or authorize the perpetrators' charges; (2) having the erroneous information removed from their credit reports; and (3) preventing the perpetrators' future activities from further damaging their records.[39] Consumer victims may request that their credit bureau files be flagged with a fraud alert, to ensure that creditors take extra precautions to verify the legitimacy of any future credit applicant associated with the flagged file. However, such alerts do not necessarily prevent the fraud from resuming for three reasons: (1) they may not be displayed prominently enough to draw the creditors' attention; (2) they may not be picked up by credit-scoring or other automated credit application systems; and (3) creditors who see the alerts may not take sufficient precautions to verify an applicant's legitimacy.[40] Some consumer victims have such a difficult time cleaning up their credit histories that they resort to the expensive and time consuming effort of suing credit reporting agencies, banks, and lenders.[41]

Consumer victims who turn to law enforcement also report having difficulty obtaining help.[42] Criminal laws for the most part, including three sections of the United States Code that criminalize conduct integral to identity theft,[43] do not recognize wronged consumers as victims of identity theft. In addition, due to the nature of this type of fraud, consumers have little evidence to offer to law enforcement.[44] Creditors who can write off losses from identity theft, or pass them on to customers in the form of higher interest rates, fees, and costs, may not routinely pursue prosecution of identity thieves although they may be better situated than consumers to do so.[45] Even when creditors refer cases to law enforcement, consumer advocates and victims report that the cases that do not meet significant dollar thresholds (typically $50,000) fall through the cracks.[46]

Finally, identity theft poses indirect costs as well. To the extent identity theft leads to higher interest rates, fees, and costs for customers of financial institutions, all consumers are harmed.

III. The Identity Theft and Assumption Deterrence Act: Relief for Consumer Victims

One way to compensate consumer victims of identity theft for their undeserved hardship would be to recognize them as crime victims and to grant them rights of restitution. The legislation that Chairman Kyl introduced, S. 512, The Identity Theft and Assumption Deterrence Act of 1997, if enacted, would accomplish these important ends. It would

define the crime of identity theft, recognize consumer victims as crime victims, and provide for restitution to consumer victims for incurred costs, including costs associated with clearing their credit history.[(47)] In addition, the United States Sentencing Commission would be able to enhance sentences when identity theft occurs. More efficient and comprehensive criminal prosecution of identity theft should serve as a deterrent for those engaged in the practice. The Commission supports these efforts to address this growing problem.[(48)]

IV. Individual Reference Services

In response to growing public and Congressional concern, the Commission recently conducted a specific examination of issues raised by individual reference services, including the extent to which these services make sensitive personal identifying information available and, thus, may increase the risk of identity theft. 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.[(49)]

A. Commission's Findings

The Commission found that a vast amount of information about consumers is available to customers of individual reference services through the services' proprietary computer networks and through increasing numbers of services that are available over the Internet. Gleaned from various public and proprietary sources, this information ranges from purely identifying information, such as name and phone number, to much more extensive data, such as driving records, criminal and civil court records, property records, and licensing records.[(50)] The Commission also learned that convenient access to this type of information in some cases confers benefits on legitimate users of these services. The look-up services assist law enforcement agencies in investigations, help people find missing children and lost relatives, provide details to news reporters,[(51)] and aid credit grantors and banks in avoiding fraud.[(52)]

At the same time, however, the increasing availability of this information poses various risks of harm to consumers' privacy and financial interests. Survey research over the past 20 years indicates that increasing numbers of consumers are concerned about how personal information is being used today.[(53)] More recent research shows that consumers are particularly concerned about the sale of their Social Security numbers and other personal identifiers.[(54)] Further, anecdotal evidence indicates that increasing access to sensitive identifying information poses risks of unlawful uses. Whether initially obtained by an unscrupulous employee, a scam artist, a computer hacker, or an Internet surfer,

such information in the wrong hands can have severe repercussions, including identity theft.[(55)]

B. IRSG Principles

In December 1997, 14 companies, comprising most of the individual reference service industry, agreed to a set of principles that addresses the availability of information obtained through individual reference services. The IRSG Principles go into effect December 31, 1998.[(56)] At the FTC workshop in June 1997, a group of industry members (the "Individual Reference Services Group" or "IRSG") presented a preliminary version of the principles and announced its intent to use self-regulation to address concerns associated with its industry. Commission staff worked with members of this group to encourage them to adopt a *meaningful* self-regulatory program. In the Commission's view, self-regulation in this instance can provide more timely, flexible, and effective solutions than government regulation. Further, self-regulation can bring the accumulated judgment and experience of industry to bear on issues that may be difficult for the government to define with bright-line rules.

The look-up service industry's self-regulatory principles, called the "IRSG Principles," restrict access to certain information obtained from "non-public" sources contained in each signatory's database. This non-public information includes "credit header" information, which is the portion of a credit report that typically contains an individual's name, address, aliases, Social Security number, current and prior addresses and telephone number.[(57)] To the extent information obtained from a non-public source is publicly available, such as a home address that appears in a "credit header" but also is listed in the phone book, that information is *not* treated as non-public and therefore not restricted under the IRSG principles.

The restrictions vary according to the category of customer. Customers that have greater access to non-public information are subject to greater controls. It is noteworthy that the IRSG Principles prohibit distribution to the general public -- over the Internet or otherwise -- of certain sensitive non-public information, including the data typically used to commit identity theft: Social Security number, mother's maiden name, and date of birth. In addition, consumers will be able to request access to the non-public information maintained about them in these services and may opt out of having any non-public information distributed to the general public.[(58)]

Although the IRSG Principles prohibit the distribution of certain sensitive information to the general public, they do permit limited disclosure of such information to entities that can establish a legitimate need for it. For example, government officials may access the information necessary to carry out their law enforcement missions. Banks and credit grantors may use Social Security numbers as search terms in order to verify the identity of account holders and applicants, and thereby prevent identity theft and other types of fraud.[(59)]

The IRSG Principles show particular promise because they include a compliance

assurance mechanism and are likely to influence virtually the entire individual reference services industry. First, signatories must undergo an annual compliance review by a professional third party such as an accounting firm, 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. Second, signatories that are information suppliers (*e.g.*, the three national credit reporting agencies) are prohibited from selling non-public information to entities whose practices are inconsistent with the Principles. Therefore, non-signatories whose practices are inconsistent with the Principles likely will be unable to obtain non-public information easily for redissemination through their services. Thus, the IRSG Principles should substantially lessen the risk that information available through individual reference services will be used to commit identity theft, and they should address most consumer concerns about the privacy of their non-public information.[(60)]

C. Report Recommendations

The Commission ultimately concluded that the IRSG Principles address many of the concerns associated with the increased availability of non-public information through individual reference services -- including identity theft -- while preserving important benefits conferred by this industry. However, certain important issues remain unresolved. For example, the Principles fail to give consumers access to the public information maintained about them and disseminated by the look-up services. Accordingly, consumers will not be able to check for inaccuracies resulting from transcription or other errors occurring in the process of obtaining or compiling the public information by the look-up services. IRSG members have agreed to revisit this issue by June 1999, and to consider whether to conduct a study quantifying the extent of any such inaccuracies. The Commission has urged the IRSG to analyze whether the frequency of inaccuracies and the harm associated with them are such that consumer access to public record information or other safeguards are in fact unnecessary.[(61)]

In addition, the IRSG Principles do not place any restrictions on the availability of "public information," including data from public records (*e.g.*, real estate, motor vehicle, and court records) and other publicly available information. In its report to Congress, the Commission encouraged public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices. Finally, the Commission acknowledged and encouraged the ongoing efforts of many privacy advocates, consumer groups, government agencies, and the IRSG to educate the public about information privacy issues.[(62)]

V. Consumer Tips for Preventing Identity Theft

From our work in this area, the Commission has found that consumers can take certain steps to help protect their privacy, and thereby decrease the chances that they will fall

prey to identity theft:

- Most importantly, consumers should guard their personal identifying information. Before divulging it, they should find out how it will be used and whether it will be transferred to third parties. Consumers should find out whether they have a choice regarding the use of their information, such as opting out of having it shared with third parties, and exercise that choice.
- Consumers should ensure that items containing personal information like charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards, and credit offers received through the mail are disposed of safely.
- Consumers should disclose their Social Security numbers only when absolutely necessary. They should ask to use alternate numbers as identifiers whenever possible, including on motor vehicle licenses.
- Consumers should carry with them only credit cards and identification they actually need. Consumers who lose their credit cards or whose cards are stolen should immediately notify their creditors by phone, and call the credit bureaus to request that a "fraud alert" be placed in their file.[(63)]
- Consumers should pay attention to billing cycles and inquire about credit bills that do not arrive on time, as they may have been misdirected by identity thieves.
- Finally, consumers periodically (at personal expense)[(64)] could order a copy of their credit report from the three credit reporting agencies to ensure the accuracy of their records.

VI. Conclusion

Identity theft is an important and growing problem facing consumers. Consumers can and should take certain steps to protect their privacy, but consumer vigilance alone is not enough. With regard to the risk of identity theft posed by the look-up services industry, the Commission believes that the IRSG Principles should significantly reduce the risk of identity theft perpetrated through the use of their databases. In fact, the IRSG Principles provide a promising model not just for self-regulation, but for the benefits that can flow from government-industry cooperation. However, because identity thieves typically obtain personal identifying information the old-fashioned way -- through stolen wallets, mail, and trash -- controlling only members of the look-up services industry will not alone prevent the problem. Public agencies, another source of sensitive identifying information, also may be able to reduce risks of identity theft by considering the potential consequences associated with the increasing accessibility of such information through public records.

In addition to the need for preventive measures, certain steps should be taken to compensate consumer victims and prevent future harm. The Commission encourages the credit card industry to pursue perpetrators of identity theft and the consumer reporting agencies to continue to work with consumer victims to ensure the accuracy of their records. The Commission also believes that consumer victims need to be formally recognized as crime victims, complete with rights of restitution. The Identity Theft and

Assumption Deterrence Act of 1997 should go a long way toward lessening the harm identity theft inflicts on innocent consumers.

---

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 or any one Commissioner.

2. Beth Givens, The Privacy Rights Handbook 231-32 (1997).

3. 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 *Federal Trade Commission, Conferences, Consumer Identity Fraud Meeting*, (last modified Mar. 14, 1998) <http://www.ftc.gov/ftc/conferences.htm>.

4. *See, e.g., FTC Report to Congress: Individual Reference Services*, December 1997 [hereinafter "FTC Report"] at 17.

5. Givens, *supra* note 2, at 231.

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

7. ID Theft Transcript at 11-12.

8. *See, e.g.*, FTC Report at 17; Givens, *supra* note 2, at 232.

9. The Commission is taking a proactive approach in examining other consumer protection issues surrounding the increasing availability of personal identifying information, such as privacy on the Internet. 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 issues and consumer protection issues, including privacy concerns. At a public workshop in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers' personal 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 agency held a four-day workshop in June 1997 to explore issues relating to unsolicited commercial e-mail, online privacy, and children's online privacy. As discussed below, the workshop also examined issues raised by individual reference services.

Further, the Commission and its staff have issued reports describing various consumer privacy concerns in the electronic marketplace. 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 addition, the Commission presented testimony on September 18, 1997, 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, and on March 26, 1998 on Internet Privacy before the House Subcommittee on Courts and Intellectual Property, Committee on the Judiciary.

10. 15 U.S.C. § 45(a).

11. The Commission does not directly 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).

12. 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: " 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."

13. 15 U.S.C. §§ 1681 *et seq.*

14. 15 U.S.C. §§ 1601 *et. seq.*

15. *Id.*

16. *See, e.g.*, Lisa Fickenscher, *Credit Industry Strains to Stem Tide of Identity Theft*, American Banker, Oct. 14, 1996, at 12; Brigid McMenamin, *Invasion of the Credit Snatchers*, Forbes, Aug. 26, 1996, at 258.

17. There is no transcript of this November meeting. Attendees split into working groups with FTC staff as facilitators for each group. The groups discussed prevention, detection, and correction issues as well as consumer and business education.

18. *Are You a Target for Identity Theft*?, Consumer Reports, Vol. 62, No. 9; Sept. 1997, at 11.

19. *Id*.; Givens, *supra* note 2, at 228-32; FTC Report at 14.

20. FTC Report at 4.

21. Givens, *supra* note 2, at 230.

22. ID Theft Transcript at 51.

23. *Id*. at 52.

24. *See e.g.*, Givens, *supra* note 2, at 230; *Are You a Target for Identity Theft*?, *supra* note 18, at 11; FTC Report at 17.

25. McMenamin, *supra* note 18, at 258; *Are You a Target for Identity Theft*?, *supra* note 18, at 11; FTC Report at 16.

26. *Prime Time Live: Credit Identity Fraud* (ABC television broadcast, Sept. 11, 1996).

27. *Id.*

28. Givens, *supra* note 2, at 231-32.

29. ID Theft Transcript at 10-11.

30. McMenamin, *supra* note 16, at 256.

31. *An Identity Crisis ,An Identity Crisis*, Chicago Tribune, Sept. 24, 1996, § C ("Your Money") at 7.

32. *Are You a Target for Identity Theft*?, *supra* note 18, at 10.

33. Official Transcript of FTC Consumer Information Privacy Workshop, June 10, 1997 at 182-83. A copy of this transcript is available online at *Federal Trade Commission, Consumer Information Privacy Workshop* (last modified May 4, 1998) <http://www.ftc.gov/bcp/privacy/wkshp97/index.html>.

34. As discussed above, although the injury to consumers may not be out-of-pocket, it can be serious nonetheless.

35. Truth In Lending Act, Section 133(b), 15 U.S.C. § 1643 (1997) and its implementing Regulation Z, 12 C.F.R. § 226.

36. *Are You a Target for Identity Theft*?, *supra* note 18, at 10.

37. *Id.*

38. ID Theft Transcript at 13-16.

39. ID Theft Transcript at 13-16 (account of consumer victim, describing his frustrating experience attempting to restore his credit report); 67, 72, 108; *Are You a Target for Identity Theft*?, *supra* note 18, at 14, 16.

40. *Id*. at 71-73, 78, 108; *Are You a Target for Identity Theft*?, *supra* note 18, at 14, 16.

41. McMenamin , *supra* note 16, at 256-58. (recounting the plight of two victims who resorted to filing such suits to clear their credit reports); *An Identity Crisis*, Chicago Tribune, Sept. 24, 1996, § C ("Your Money") at 7 (recounting the plight of a consumer victim who sued the three national credit reporting agencies for failing to remove erroneous information from her credit report).

42. ID Theft Transcript at 59-62; Givens, *supra* note 2, at 232.

43. 18 U.S.C. § 1028 (criminalizing fraud and related activity in connection with identification documents); 18 U.S.C. § 1029 (criminalizing fraud and related activity in connection with access devices); and 42 U.S.C. § 408(A)(7) (criminalizing misuse, with intent to deceive, of a Social Security number); *see also,* ID Theft Transcript at 83-84.

44. ID Theft Transcript at 60.

45. *See Are You a Target for Identity Theft*?, *supra* note 18, at 10.

46. ID Theft Transcript at 58-63; *Are You a Target for Identity Theft*?, *supra* note 18, at 10.

47. It is the Commission's understanding that certain revisions are being made to the bill. The Commission looks forward to supporting committee staff in their efforts to draft legislation that effectively combats identity theft. In the version of the bill initially provided to the Commission, consumer victims are granted limited rights of restitution for costs incurred in clearing credit history or credit rating, and for costs in connection with related civil or administrative proceedings. Because consumer victims may incur costs resulting directly from the crime that are not named here, *e.g.*, costs incurred in clearing errors from

employment and criminal records, the Commission recommends that these rights of restitution be expanded to include *but not be limited to* the specified costs.

48. In the form initially provided to the Commission, the bill would direct the Secretary of the Treasury and the Chairman of the Federal Trade Commission to conduct a comprehensive study of the nature, extent, causes, and threat posed by identity theft. The Commission understands that the provision regarding the study will be struck from the bill. Should this provision remain in the bill, the Commission would appreciate the opportunity to discuss what the Commission's most effective role could be in addressing the problem of identity theft. The Commission also understands that consideration is being given to establishing a possible central database, maintained by this agency, that would serve as a repository for consumer complaints regarding identity theft, a source of consumer education and information regarding identity theft, and a tool for law enforcement authorities. Should the proposed legislation proceed along such lines, the Commission would appreciate the opportunity for discussion.

49. *See generally* FTC Report.

50. *Id.* at 4-5.

51. *Id.* at 9-11.

52. *Id.* at 10.

53. *Id.* at 13.

54. *Id.* at 13-14.

55. *Id.* at 16-18.

56. *Id.* at 25. The 14 signatories include both direct providers of look-up services, like LEXIS-NEXIS, and the suppliers of information to the look-up services industry, including the three national credit reporting agencies, Equifax, Experian, and TransUnion.

57. *Id.* at 5-6 and n. 42. To the extent an individual reference service provides customers with consumer reports (containing, *e.g.*, credit history, financial status, and employment background information), that entity may be acting as a "consumer reporting agency" subject to the obligations and restrictions set forth in the FCRA. Dissemination of consumer reports by a consumer reporting agency is limited to the permissible purposes defined by the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1997).

58. *Id.* at 25-28.

59. *Id.*

60. *Id.* at 28-30.

61. *Id.* at 31-32.

62. *Id.* at 32-33.

63. As noted above, this practice may not always be effective. Nonetheless, consumers should take all possible measures to notify creditors of potential identity theft.

64. The FCRA, as amended in 1996, limits the amount that a consumer reporting agency may charge for a

consumer report to $8, as adjusted annually by the Consumer Price Index.