Specifically, the Act amends 18 U.S.C. § 1028 ("Fraud and related activity in connection with

sense of the extent of identity theft activity and the forms it is taking (e.g.,credit card vs. phone fraud, latest scams, etc).

(3) Consumer education. The FTC has taken the lead in coordinating with other government agencies and organizations the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime.[(13)] The results of the FTC's extensive, multi-media campaign include print materials, media mailings and interviews and a website, located at www.consumer.gov/idtheft. This collaborative consumer education effort is ongoing; the Commission hopes to continue this effort with many of the private sector financial institutions that have an interest in preventing and remedying identity theft.

The FTC's comprehensive consumer education booklet, Identity Theft: When Bad Things Happen to Your Good Name, has been a tremendous success. The 22-page booklet covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. The FTC has distributed more than 100,000 copies of the booklet since February 2000. The Social Security Administration and the Federal Deposit Insurance Corporation have also distributed When Bad Things Happen. Further, the online booklet received more than 142,000 hits from February 2000 through July 2000.

The identity theft website includes the booklet, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources.[(14)] T-4(s)-itou1 Tbut Tc8e0( )-1001 Tm4( )-k0 csv theitou1 e on-

Unavoidable. Although there are many steps consumers can take to minimize their risk of identity theft, there is no way to completely avoid it. One out of eight victims that call the Commission's identity theft hotline report that they have been victimized by someone they know -- either a family member, a neighbor or workplace acquaintance, someone employed by a financial institution they do business with, or in some other way known to them. Incidences of workplace identity theft appear to be increasing. Since November 1999, the Commission has received reports of hospitals, schools, and other employers whose personnel records had been compromised by an identity thief. Each such instance has the potential to translate into hundreds of identity theft victims. In these cases, where someone has access to personal information because of their relationship to the victim, identity theft is practically unavoidable.

The majority of victims do not know how their identifying information was compromised. The question these victims most commonly ask when they call the FTC's identity theft hotline is, "how could this have happened to me?" Our answer is that it could have arisen in a multitude of ways. For example, identity theft can arise from simple, low-tech practices such as stealing someone's mail or "dumpster diving" through their trash to collect credit card offers or obtain identifying information such as account numbers or social security numbers. There are also far more sophisticated practices being employed. In a practice known as "skimming," identity thieves use computers to read and store the information encoded on the magnetic strip of an ATM or credit card when that card is inserted through either a specialized card reader or a legitimate payment mechanism (e.g.,

Unstoppable. For victims of identity theft, the costs can be significant and long-lasting. Where the identity thief has committed a crime in the victim's name, the harm is especially pernicious. In the worst cases, the negative consequences are never completely eradicated. For example, one consumer who called the FTC identity theft hotline reported that her income tax refund was withheld due to past child support she was believed to have owed. She found out that a child was born to a person using her name and social security number in a state she had never even visited. Another consumer reported that he is unable to renew his driver's license or register to vote because, due to crimes committed in his name by another person, he is considered to be on probation for federal law violations including possession of drugs with intent to distribute and fraud. More than one consumer has been denied employment when a background check or security clearance showed criminal records relating to an offense committed by someone using their names and social security numbers. Another consumer lost his job when, as part of his promotion review, a background check indicated that he had a criminal record. Although the consumer went to court and obtained a declaration that he did not have a criminal record, he lost his job because the company that performed the background check said that it could not clear his record.

Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even where the individual consumer is not legally liable for these debts,[(15)] the consequences to the consumer are often considerable. A consumer's credit history is frequently scarred and he or she typically must spend numerous hours over the course of months or even years contesting bills and correcting credit reporting errors. Creditors for the fraudulent accounts often continue to harass the consumer. In the interim, the consumer victim may be denied loans, mortgages and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts are tainted and a new account is

- Fraudulent Loans - Approximately 11% reported that the identity thief obtained a loan, such as a car loan, in their name.

Of consumer identity theft complaints related to credit cards, 72% involved the establishment of a new credit card account in the victim's name and 24% involved the takeover of an existing account. Among reports of identity theft related to a checking or savings account, 44% involved the use of unauthorized checks, 28% involved the establishment of a new checking account in the victim's name and 19% involved unauthorized electronic funds transfer.

Not surprisingly, the states with the largest populations account for the largest numbers of complainants and suspects. California, New York, Florida, Texas and Illinois, in descending order, represent the states with the highest number of complainants. About 55% of victims calling the identity theft hotline report their age. Of these, 40% fall between 30 and 44 years of age. Approximately 27% are between age 45 and 64 and another 22% are between age 19 and 29. About 8% of those reporting their ages are 65 and over; and over 3% are age 18 and under.

Consumers also report the harm to their reputation or daily life. The most common non-monetary harm reported by consumers is damage to their credit report through derogatory, inaccurate information. The negative credit information leads to the other problems most commonly reported by victims, including loan denials, bounced checks and rejection of credit cards. Identity

complimentary process to allow identity theft victims to share the details of their complaints simultaneously with the FTC and the national consumer reporting agencies.

knowledge and billed consumers' accounts for unordered or fictitious Internet services), later proceedings at FTC v. J.K. Publications, Inc., et al, 99 Civ 00044 (C.D. Cal. Aug. 30, 2000)(final order awarding $37.5 million in redress); FTC v. Rapp, No. 99-WM-783 (D. Colo. filed Apr. 21, 1999) (alleging that defendants obtained private financial information under false pretenses)(Stipulated Consent Agreement and Final Order entered June 23, 2000). The practices the Commission expects to focus its law enforcement resources on are those where the effect is widespread and where civil remedies are likely to be effective.

7. These fraud alerts require that the consumer be contacted when new credit is requested in that consumer's name.

8. 15 U.S.C. §§ 1681 et seq.

9. 15 U.S.C. § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

10. 15 U.S.C. §§ 1601 et seq

11. 15 U.S.C. §§ 1692 et seq

12. The Commission has been working closely with other agencies to establish a coordinated effort to identify the factors that lead to identity theft, work to minimize those opportunities, enhance law enforcement and help consumers resolve identity theft problems. The first such event was the Commission's April 1999 meeting with representatives of approximately a dozen federal agencies as well as the National Association of Attorneys General to discuss the implementation of the consumer assistance provisions of the Identity Theft Act. FTC staff works with the Identity Theft Subcommittee of the Attorney General's Council on White Collar Crime to coordinate law enforcement strategies and initiatives. FTC staff coordinates with staff from the Social Security Administration's Inspector General's Office on the handling of social security number misuse complaints, a leading source of identity theft problems. The FTC staff also assisted the Department of Treasury in planning the National Identity Theft Summit, held in March of 2000.

13. Among the organizations the FTC has brought into this effort are the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of Thrift Supervision, the Department of Justice, the U.S. Secret Service, the Federal Bureau of Investigation, the Postal Inspection Service, the Internal Revenue Service, the Social Security Administration, the Federal Communications Commission, the Securities and Exchange Commission, the U.S. Trustees, and the National Association of Attorneys General.

14. www.consumer.gov is a multi-agency "one-stop" website for consumer information. The FTC hosts the server

Institution Type	refused to corre ct information/close account	personnel not helpful	security procedures inadequate
bank credit card issuer	27%	24%	23%
bank creditor	24%	30%	19%
Depository Institution	22%	22%	42%