PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT

Before the

COMMITTEE ON BANKING AND FINANCIAL SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

September 13, 2000

Mr. Chairman, and members of the Committee, I am Betsy Broder, Assistant Director for the Division of Planning and Information of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[(1)] I appreciate the opportunity to present the Commission's views on the important issue of identity theft, and describe to you the Commission's efforts to help victims, alert industry and equip law enforcement to deal with this harrowing crime.[(2)]

In my remarks today, I will discuss the growing phenomenon of identity theft, the measures the Commission has taken to meet the goals of the Identity Theft and Assumption Deterrence Act ("the Identity Theft Act") and what we see as major challenges for the coming year in combating identity theft.

Identity theft often seems unavoidable, undetectable and unstoppable. Public concern over identity theft is understandably enormous. This is in part because it seems to be widespread and in part because the consequences can be devastating. Consumers feel particularly vulnerable knowing that no matter how careful they are, they may nonetheless become identity theft victims.

The Identity Theft Act addressed these concerns in several concrete ways. It directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. As the Commission staff have strived to meet the responsibilities of the Identity Theft Act, we have learned much about the crime, its victims and its perpetrators.

I. The Federal Trade Commission's Role in Combating Identity Theft

A. The Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act of 1998 addresses identity theft in two significant ways. First, the Act strengthens the criminal laws governing identity theft.

Specifically, the Act amends 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents") to make it a federal crime to:

knowingly transfer [] or use [], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.[(3)]

The second way in which the Act addresses the problem of identity theft is by focusing on consumers as victims.[(4)] In particular, the Act provides for a centralized complaint and consumer education service for victims of identity theft and gives the responsibility of developing this function to the Commission. The Act directs that the Commission establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[(5)]

B. ***The FTC's Response to Identity Theft***

In enacting the Identity Theft Act, Congress recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from private businesses. Accordingly, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[(6)]

In order to fulfill the purposes of the Act, the Commission has developed and begun implementing a plan that centers on three principal components:

(1) *Toll-free telephone hotline*. The Commission has established a toll-free telephone number, 1-877-ID THEFT (438-4338), that consumers can call to report identity theft. Consumers who call the hotline receive telephone counseling from specially trained personnel to help them resolve credit-related problems that may have resulted from the misuse of their identities. In addition, the hotline counselors enter information from consumers' complaints into the Identity Theft Data Clearinghouse (the "Clearinghouse") - a centralized database used to aid law enforcement and prevent identity theft.

The identity theft hotline has been in operation since November 1, 1999. The hotline answered an average of over 1000 calls per week in the months of July and August, 2000.

About forty percent of consumers who call the FTC identity theft hotline inquire about how to guard against identity theft. The counselors suggest steps consumers should take to minimize their risk. This information has been developed from the Commission's extensive experience in advising consumers on how to avoid credit and charge card fraud and maintain financial privacy.

Around sixty percent of consumers who call the FTC identity theft hotline have already become victims of identity theft. The counselors give them specific information about preventing additional harm to their finances and credit histories. Consumers are instructed to contact each of the three national consumer reporting agencies to obtain copies of their credit reports and request

that a fraud alert be placed on their credit reports.[7] The counselors also advise consumers to review carefully the information on the reports to detect any additional evidence of identity theft. Consumers are informed of their rights under the Fair Credit Reporting Act[8] and are given the procedures for correcting misinformation on their credit reports. Consumers are also advised to contact each of the creditors or service providers where the identity thief has established or accessed an account to request that the account be closed. The counselors also inform consumers of their rights under the Fair Credit Billing Act[9] and the Truth in Lending Act,[10] which, among other things, limit their responsibility for unauthorized charges to fifty dollars in most instances. Consumers who have been contacted by a debt collector concerning debts incurred by the identity thief are advised of their rights under the Fair Debt Collection Practices Act,[11] which prescribes debt collectors' practices.

The FTC counselors advise consumers to notify their local police departments, both because local law enforcement may be in the best position to catch and prosecute identity thieves, and because a police report often helps consumers demonstrate to would-be creditors and debt collectors that they are genuine victims of identity theft. Nearly 75% of the states have enacted their own identity theft laws and counselors, in appropriate circumstances, will refer consumers to other state and local authorities.

Lastly, where investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers are referred to those agencies. For example, consumers who complain that someone has been using their Social Security number for employment are advised to report this to the Social Security Administration's fraud hotline and to request a copy of their Social Security Statement to verify the accuracy of the earnings reported to their Social Security number.

(2) *Identity theft complaint database*. Detailed information from the complaints received on the FTC's identity theft hotline is entered into the FTC's Identity Theft Data Clearinghouse. The information in the Clearinghouse is available to law enforcement agencies nationwide via the FTC's secure law enforcement website, *Consumer Sentinel*. Access to the Clearinghouse information supports law enforcement agencies' efforts to combat identity theft by providing a range of complaints from which to spot patterns of illegal activity. For example, federal law enforcement agencies may be able to more readily identify organized or large-scale identity theft rings. The Commission expects that the Clearinghouse will allow the many agencies involved in combating identity theft to share data, enabling these offices to work more effectively to track down identity thieves and assist consumers.[12]

In addition, the Clearinghouse facilitates the referral process mandated by the Identity Theft Act. Clearinghouse members can access directly the database from their desktops in order to support their investigations and identify emerging trends and patterns in identity theft in their geographic areas. The Commission also plans to disseminate complaint information through customized reports, extracting for our law enforcement partners the Clearinghouse complaints that meet the criteria they have designated. For agencies that have their own sophisticated data-mining tools, Commission staff will provide large batches of raw data for further analysis. Staff will notify our law enforcement partners when we identify trends or patterns in the data that appear to have ramifications for them. Finally, the Clearinghouse information provides policy makers with a

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 on-line 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)] The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Identity Theft Data Clearinghouse.

II. What the Clearinghouse Tells Us About Identity Theft

A. *A Serious Problem*

By now, many people have encountered, directly or indirectly through another person, some form of identity theft: Someone has used their name to open up a credit card account; their identifying information -- name, social security number, mother's maiden name, or other personal information -- has been used by another to commit fraud or engage in other unlawful activities. Other common forms of identity theft include taking over an existing credit card account and making unauthorized charges on it (typically, the identity thief forestalls discovery by the victims by contacting the credit card issuer and changing the billing address on the account); taking out loans in another person's name; writing fraudulent checks using another person's name and/or account number; and opening a telephone or wireless service account in another person's name. In extreme cases, the identity thief may completely take over the victim's identity -- opening a bank account, obtaining multiple credit cards, buying a car, getting a home mortgage and even working under the victim's name.

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.,* the card reader used to pay for gas at the pump in a gas station). Once stored, that information can be re-encoded onto any other card with a magnetic strip, instantly transforming a blank card into a machine-readable ATM or credit card identical to that of the victim.

The Internet has dramatically altered the potential occurrence and impact of identity theft. First, the Internet provides access to identifying information, through both illicit and legal means. The global publication of identifying details that previously were available only to a select few increases the potential for misuse of that information. Second, the ability of the identity thief to purchase goods and services from innumerable e-merchants expands the potential harm to the victim through numerous purchases. The explosion of financial services offered on-line, such as mortgages, credit cards, bank accounts and loans, provides a sense of anonymity to those potential identity thieves who would not risk committing identity theft in a face-to-face transaction.

Undetectable. In many instances, identity theft goes undetected by creditors, law enforcement and the victims for months or even years. One caller to the FTC's identity theft hotline reported that his wallet was stolen in 1992. This consumer was unaware that he was the victim of identity theft until seven years later, when, in the summer of 1999, he was arrested on an outstanding warrant for an offense committed by the identity thief in 1993. The consumer spent several nights in jail and was forced to post $15,000 bond. He was also shocked and dismayed to discover multiple outstanding criminal charges against him in several states as a result of the identity thief's activities. This example, while unusual, is not unique. The FTC has received numerous reports from consumers who were not aware that they had been victimized by an identity thief until four or more years after the first fraudulent transaction.

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 essential. Moreover, even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer.

B. ***Patterns and Practices: Specific Complaint Data***[(16)]

The Identity Theft Data Clearinghouse provides law enforcement with the first opportunity to collect and consolidate identity theft complaints on a nationwide basis. The fruits of this effort are already evident. The basic complaint data show that the most common forms of identity theft reported during the first ten months of operation were:

- *Credit Card Fraud* - Approximately 55% of consumers reported credit card fraud -- *i.e.,* a credit card account opened in their name or a "takeover" of their existing credit card account;

- *Communications Services* - Approximately 28% reported that the identity thief opened up telephone, cellular, or other utility service in their name;

- *Bank Fraud* - Approximately 18% reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written; and

- *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 theft victims also report repeated contacts by debt collectors for the bad debt incurred by the identity thief. Many consumers report that they have to spend significant amounts of time resolving these problems.

Consumers also report problems with the banks and other institutions that provided the credit, goods or services to the identity thief in the consumer's name. These institutions often attempt to collect the bad debt from the victim, or report the bad debt to a consumer reporting agency, even after the victim believes that he or she has demonstrated the fraud. Of consumers lodging identity theft-related complaints with the Clearinghouse, 29% reported complaints about a bank credit card issuer, 25% reported complaints about a bank creditor[(17)] and 22% reported complaints about a depository institution.[(18)]

The majority of consumer complaints related to bank credit card issuers, bank creditors and depository institutions fall into three categories: (1) the institution refused to correct information or close the disputed account; (2) customer service personnel were not helpful; and (3) the institution's security procedures were inadequate.[(19)]

The Clearinghouse data also reveal that consumers are often dissatisfied with the consumer reporting agencies. The leading complaints by identity theft victims against the consumer reporting agencies are that they provide inadequate assistance over the phone, or that they will not reinvestigate or correct an inaccurate entry in the consumer's credit report.

IV. Next Steps

A. *The Identity Theft Prevention Act of 2000*

The Commission has made great strides in assisting consumers and law enforcement to combat identity theft but recognizes that much remains to be done. Earlier this year, the Identity Theft Prevention Act of 2000, H.R. 4311, was introduced in the House of Representatives. The Commission has expressed its support of S. 2328, the Senate version of this bill. The Identity Theft Prevention Act of 2000 would effectively address many areas of identity theft vulnerability and would protect many consumers from becoming victims of this very serious crime. The Act would provide consumers with access to information that may reveal indicia of identity theft or the source of erroneous information resulting from identity theft. Such measures enable consumers to better protect themselves against identity theft and avoid some of the frustrations that often accompany their efforts to undo the harm inflicted by the identity thief. Providing for free annual credit reports and requiring that a credit card issuer advise a consumer of a request to change the address on a credit account will help consumers help themselves. Further, requiring clear and conspicuous fraud alerts on credit reports will help to thwart the ability of identity thieves to commit ongoing fraud. The Commission is confident that these proposals will assist consumers who contact the Commission's Identity Theft Data Clearinghouse.

B. *Gramm-Leach-Bliley Act Implementation*

Section 521(a) of the Gramm-Leach-Bliley Act (the "GLB Act") prohibits obtaining or attempting to obtain customer information of a financial institution relating to another person by fraud or misrepresentation -- a practice often referred to as "pretexting" or "pretext calling." Pretexting by an identity thief who seeks consumers' account information for the purpose of defrauding the consumer would likely constitute a violation of both the Identity Theft Act and the GLB Act. The Identity Theft Data Clearinghouse collects information, if known by a complainant, as to how an identity thief obtained the complainant's personal information. This information is useful to law enforcement prosecuting identity theft under both statutes. Indeed, the Commission is beginning to receive complaints that identity thieves have accessed private information by pretexting financial institutions or by otherwise forging documents provided to a financial institution. The GLB Act provides for enforcement by the Commission for entities under its jurisdiction and provides criminal penalties for use by criminal law enforcement. While the law has been in effect for a little over half a year, Congress, as you know, has required the Commission to submit an annual report on enforcement actions under the Act's pretexting provisions in January of 2001.

C. *Working with Industry*

The Identity Theft Act authorizes the Commission to refer consumer identity theft complaints and information to the three major national consumer reporting agencies and other appropriate entities. The Commission envisions a streamlined process that would decrease the amount of time spent by consumer victims correcting credit report errors. Paramount in this process would be the ability of a consumer to make a single call to report him or herself as a victim of identity theft to the FTC or one of the three major national consumer reporting agencies and to have a fraud alert posted on the credit reports from each of the reporting agencies. Currently, a victim of identity theft must notify each of the three national consumer reporting agencies separately and then typically make additional calls to the FTC and to all creditors. The Commission looks forward to working with the three major national consumer reporting agencies to develop a

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

Further, the Commission will soon begin sharing certain limited information from its Identity Theft Clearinghouse with banks, creditors and other businesses whose practices are frequently associated with identity theft complaints. The goal is to encourage and enable industry and individual companies to develop better fraud prevention practices and consumer assistance techniques. To that end, the Commission will convene a workshop for industry, consumer groups, the public and law enforcement on identity theft victim assistance on October 23-24, 2000. This workshop follows the National Summit on Identity Theft of March 2000, which initiated a dialogue between the public and private sectors on identity theft. The Social Security Administration Inspector General's Office, the Department of Justice and the U.S. Secret Service will convene later workshops on identity theft prevention and prosecution.

V. Conclusion

The Identity Theft Data Clearinghouse demonstrates that identity theft is a serious and growing problem, but it also reveals ways to halt this growth. The Clearinghouse, the toll-free hotline counselors and the consumer education campaign have begun to address the serious problems associated with identity theft. Heightened awareness by consumers and businesses will also help reduce the occurrences of this fraud. The Commission looks forward to continued collaboration and cooperation between government agencies, law enforcement and the private sector in these efforts. The FTC also looks forward to working with the Subcommittee to find further ways to prevent this crime and to assist its victims.

Endnotes

1. The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

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

3. 18 U.S.C. § 1028(a)(7). The statute further broadens "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.,* credit cards), electronic identification number or routing code and telecommunication identifying information.

4. Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

5. Pub. L. No. 105-318 § 5, 112 Stat. 3010 (1998).

6. Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. J.K. Publications, Inc., et al,* 99 F. Supp.2d. 1176 (C.D. Cal. Apr. 10, 2000)(granting summary judgment for the FTC in case alleging that defendants obtained consumers' credit card numbers without their

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 and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from more than 170 federal agencies. The consumer.gov project received the Hammer Award from Vice President Al Gore's National Performance Review Team in March1999.

15. The Truth in Lending Act, 15 U.S.C. § 1601 *et seq*. and the Electronic Fund Transfer Act, 15 U.S.C. § 1693 *et seq.* limit consumers' liability for fraudulent transactions in connection with credit and debit cards, respectively.

16. This data analysis covers the period between November 1, 1999 and August 30, 2000.

17. These are reports of identity theft related to a loan originated by a bank or credit union.

18. These are reports of identity theft related to a checking or savings account. This may include fraudulent ATM or debit card transactions, automatic withdrawals and checks.

19. These complaints break down as follows:

Institution Type	refused to correct 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%