Testimony of

Mr. Lou Cannon

March 20, 2002

Good Morning, Madam Chairman, Ranking Member Kyl, and distinguished Members of the Subcommittee on Technology, Terrorism, and Government Information. Thank you for giving me the opportunity to appear before you today. My name is Lou Cannon, and I am the President of the District of Columbia Lodge, and Chairman of the Federal Officers Committee.

I am here this morning at the request of Steve Young, National President of the Grand Lodge, Fraternal Order of Police, to speak in support of S. 1399, the "Identity Theft Prevention Act of 2001" introduced by Chairman Feinstein and Senator Kyl, and S. 1742, the "Restore Your Identity Act of 2001" introduced by Senator Cantwell. The F.O.P. is the largest law enforcement labor organization in the United States, representing more than 300,000 members.

Identity theft occurs when a criminal obtains personal identifying information, such as a social security number, date of birth, credit card account number, or bank account information, and then fraudulently uses this information for criminal purposes. Simply possessing personal information is not considered a criminal act, but the use of it is. Tracking and investigating identity theft crimes have proven difficult for law enforcement. In today's world, vast amounts of personal information, once difficult to obtain, is now easily accessible to anyone with access to the Internet. In addition, personal information is being sold on the black market. For a price, criminals can access a ready-made database of information without risk or effort of retrieval.

The sharp rise in identity theft crimes is of grave concern to the law enforcement community. The Federal Trade Commission (FTC) announced this January that identity theft was the top consumer fraud complaint of 2001, garnering forty-two percent (42%) of the complaints entered into the Consumer Sentinel database, with Internet auctions a distant second at ten percent (10%). As you know, the Consumer Sentinel database, which incorporates information submitted by law enforcement agencies, is a clearinghouse of information collected by the FTC. It is estimated that there were more than 700,000 victims of identity theft in 2001, with a reported 2,000 calls a week to the FTC identity theft hotline. A 1999 study commissioned by an identity theft prevention service found that one out of five people or family members have been victimized by identity theft. The cost to the victims, financial institutions, and law enforcement is tremendous. In 1997, the Secret Service estimated that victims lost an aggregate $745 million dollars as a result of identity theft, and this number is expected to rise.

Besides the financial losses associated with identity theft, victims may also encounter additional hardships that are not quantifiable. For example, victims might have difficulty securing educational loans or qualifying for home mortgages. When a criminal has compromised a victim's credit rating, their ability to rent an apartment, open a bank account, or apply for store credit can be irreparably damaged. Circumstances might even lead to permanent consequences, such as a criminal record for the victim. Victims of identity theft may even be denied

employment for their lack of credit worthiness. For example, as reported in a 1998 Washington Post article, a victim had his wallet stolen, followed by his identity. After committing several unrelated offenses, the identity thief was arrested. Upon his apprehension, the criminal falsely identified himself as the victim and produced corroborating identification. As a result, the victim was burdened with a criminal record and was subsequently rejected by several potential employers for this reason.

The crime of identity theft is repetitive in nature, for as long as the criminal is in possession of the victim's personal information, they can be re-victimized. Even if fraud insurance covers any financial loss, the victim will continue to suffer a flawed credit history, and will be forced to prove their innocence repeatedly to creditors, credit bureaus, and debt collectors for an indefinite period of time. According to the Identity Theft Resource Center, victims spend an average of 175 hours and $808 in out-of-pocket expenses to restore their credit and clear their names.

There are numerous means by which personal identifying information can be obtained, but there are several "tried and true" methods employed by identity thieves. These criminals often rummage through the trash of a private residence or business, steal wallets containing identification, or hijack bank and credit card statements or applications from the mail. They may complete a change of address form to direct mail to another address, use information provided on the Internet, or buy personal identifiers through the black market. Once the identity thief locates the personal identification, they have unlimited power to wreak havoc on the unsuspecting victim. The criminals may operate on a very basic level, or possess a certain degree of sophistication when using the fraudulently obtained data. Identity theft plots may be as simple as establishing new lines of credit or utility service and failing to pay, writing bad checks or counterfeit checks on a bank account in the victim's name, using the victim's identification as an alias upon arrest by law enforcement; or as complex as purchasing a home or car in the victim's name, or filing for bankruptcy to avoid unpaid debts accrued by the thief.

There are measures an individual can take to safeguard their personal information, like shredding bank statements, ripping up credit card receipts with the account number printed on them, and destroying expired credit cards in order to prevent criminals from collecting information by rummaging through the trash. Yet, despite a conscientious effort to protect personal information, potential victims have no control over how their privacy is safeguarded by those who do have access to their personal information.

For these reasons, the F.O.P. strongly supports S. 1399, the "Identity Theft Prevention Act of 2001". First, the bill mandates notification to consumers when a credit card company receives a change of address request for an existing account followed within thirty (30) days by a request for a duplicate credit card. The intent of this notification is to prevent a criminal from stealing the credit card number and related personal identifying information. By arming victims with this knowledge, they will be better able to defend against any unauthorized activity and prevent any further damage from occurring. In addition to this preventative measure, S. 1399 requires consumer reporting agencies to disclose any anomalies in the victim's file as they pertain to the address listed on the credit report to the company making the request. Creditors are thereby warned of possible fraudulent credit applications, frustrating criminal attempts to use this information. The information needed to steal an identity is easy to acquire--pilfering through

garbage to obtain credit card account information, diverting mail through a change of address, or "skimming" credit cards to record the personal data contained on the magnetic strip. Identity thieves know that their risk of apprehension is low, and even if they are convicted, the penalty for such illegal activity is minimal. The proposed legislation appropriately addresses the means by which to hold businesses and creditors accountable for the mismanagement of private information.

Second, the legislation you have introduced also permits potential victims to demand that consumer reporting agencies place a fraud alert in their file, the purpose of which is to prevent the issuance of credit without expressed permission. By definition, a fraud alert means "a clear and conspicuous statement in the file of a consumer that notifies all prospective users of a consumer report made with respect to that consumer that the consumer does not authorize the issuance or extension of credit in the name of the consumer" unless by some prearranged method mutually agreed upon between the consumer and consumer reporting agency. Enforcement of this provision will make the crime of identity theft more difficult to accomplish, and therefore less attractive to the criminal element.

Third, this legislation promotes cooperation among the three major credit bureaus through an FTC rulemaking to be conducted within 270 days after the enactment of S. 1399. Victims of identity theft will benefit from the sharing of information between these agencies. For example, as required by the rulemaking, the procedure for reporting consumer complaints about identity theft and fraud alerts will be streamlined so that victims will not have to report the same information to each credit reporting agency, saving the victim valuable time and effort. The rulemaking also requires investigation of discrepancies between a victim's credit application and credit report, should any such irregularities exist.

Finally, the bill requires all new credit card machines that print receipts electronically to leave off the expiration date of the credit card and all but the last five numbers of the account. Receipts thrown away by potential victims often end up in the hands of an imposter who uses the personal information on the receipt to make unauthorized purchases and run up debt that the victim is unaware of. Truncation of the credit card account number will effectively halt the practice of stealing information from receipts, even if the receipt is disposed of improperly. These preventative measures, combined with aggressive enforcement of identity theft legislation, will enhance the campaign to slow, and ultimately reverse, the growth of identity theft crimes.

The crime of identity theft presents a very real challenge to law enforcement to investigate and prosecute the offenders, partly because evidence of the crime is unavailable in a timely fashion. That is why the F.O.P. is pleased to support S. 1742, introduced by Senator Cantwell, which seeks to improve the cooperation among the credit reporting agencies, businesses, victims, and law enforcement. This is a critical first step to the successful investigation and prosecution of identity theft crimes. First, this bill requires a business possessing records related to an identity theft to furnish the relevant documentation within 10 days of the request, provided that the identity of the victim can be verified by the business. Many creditors have been unwilling to divulge information about open accounts or recent transactions because of liability concerns and a good faith desire to protect the privacy rights of the consumer. S. 1742 addresses this concern by exempting these businesses from liability with respect to any disclosure made to further the

investigation of identity theft or assist the victim. The disclosure of evidence to the victim aids law enforcement in pursuit of the thief. With an estimated 700,000 consumers falling prey to identity theft in 2001, and law enforcement resources and manpower stretched to their limits, the cooperation of the business community is essential to stopping these types of crimes.

Second, through an amendment to the Internet False Identification Prevention Act, local and State law enforcement will be included in the Federal Trade Commission Study examining the enforcement of identity theft laws. This is important because these agencies, not Federal authorities, are most likely to investigate these types of crimes, despite the fact that identity theft is a Federal offense. Moreover, because the stolen identities are frequently used to commit offenses in multiple jurisdictions, State and local law enforcement from around the United States may be called upon to investigate the same crime. Therefore, it is imperative that information is quickly gathered and shared, keeping the lines of communication open to effect a swift and successful arrest and prosecution.

Third, the bill also allows for aggressive prosecution of criminals engaged in fraud or identity theft crimes by making the offense under State law a Federal Racketeer Influencing and Corrupt Organization (RICO) predicate. Businesses will be better equipped to defend themselves against such criminal activity, resulting in increased penalties for those who engage in identity theft. Civil actions brought by the State Attorneys General on behalf of victims in that State are also permissible under Senator Cantwell's legislation. Whereas prosecutors may be unable to prove criminal identity theft, the victims could still see justice done through civil litigation. Fourth, alternatives to criminal punishment, such as the filing of civil suits in Federal court as set forth in S. 1742, increase the opportunity to enforce identity theft laws and hold the imposters accountable for their deception. This is a win-win situation for both victims and law enforcement, since tough enforcement of the law increases the risk of detection and thus deters crime.

Fifth, Senator Cantwell's legislation also amends the Fair Credit Reporting Act, giving victims a greater chance of recovering their good name, by providing that the two-year statute of limitations on an identity theft-related claim begins after the victim discovers the theft, not at the time the crime was actually perpetrated. Similarly, the bill requires that harmful information resulting from identity theft must be blocked from the victim's credit report, assuming the victim did not participate in the crime itself or profit directly or indirectly from it.

The reason that identity theft is on the rise is that it is an easy, profitable crime, with a low risk of being caught. Anecdotal evidence collected by Ventura County, California indicates that less than ten percent (10%) of identity theft crimes result in an arrest and conviction. The F.O.P. believes that these two bills together will reduce the opportunities of criminals or potential criminals from obtaining the personal information that makes identity theft possible. Additionally, the bills aim to increase the risk of discovery and arrest by making it easier to obtain evidence against the perpetrators and enhance the penalty for committing these types of crimes. Collectively, both pieces of legislation will frustrate purveyors of identity theft and ultimately curb the rapid progression of this costly offense.

I want to thank the Subcommittee for the opportunity to appear before you here today. I would be pleased to answer any questions you may have at this time.