

Testimony of Dennis M. Lormel, Chief, Terrorist Financial Review Group, FBI
Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and
Government Information
July 9, 2002
Hearing On S. 2541, "The Identity Theft Penalty Enhancement Act"

Good afternoon Madam Chairman and members of the Subcommittee on Technology, Terrorism and Government Information. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to the Subcommittee for affording us the opportunity to participate in this forum and to provide comment to the Subcommittee regarding the proposed legislation in S 2541. The FBI is very supportive of this bill which enhances the penalties for convictions on certain felony violations where identity theft was used in relation to the offenses and adds some wording to Section 1028 of Title 18, United States Code.

As this Subcommittee is well aware, the FBI, along with other federal law enforcement agencies, investigates and prosecutes individuals who use the identities of others to carry out violations of federal criminal law. These violations include bank fraud, credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, computer crimes, and fugitive cases. These crimes carried out using a stolen identity makes the investigation of the offenses much more complicated. The use of a stolen identity enhances the chances of success in the commission of almost all financial crimes. The stolen identity provides a cloak of anonymity for the subject while the groundwork is laid to carry out the crime. This includes the rental of mail drops, post office boxes, apartments, office space, vehicles, and storage lockers as well as the activation of pagers, cellular telephones, and various utility services.

Identity theft is not new to law enforcement. For decades fugitives have changed identities to avoid capture and check forgers have assumed the identity of others to negotiate stolen or counterfeit checks. What is new today is the pervasiveness of the problem. The Federal Bureau of Investigation does not view identity theft as a separate and distinct crime problem. Rather, it sees identity theft as a component of many types of crimes which we investigate.

Advances in computer hardware and software along with the growth of the Internet has significantly increased the role that identity theft plays in crime. For example, the skill and time needed to produce high-quality counterfeit documents has been reduced to the point that nearly anyone can be an expert. The same multimedia software used by professional graphic artists is now being used by criminals. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents. The tremendous growth of the Internet, the accessibility it provides to such an immense audience coupled with the anonymity it allows result in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme. This is particularly true with identity theft related crimes. Computer intrusions into the databases of credit card companies, financial institutions, on-line businesses, etc. to obtain credit card or other identification information for individuals have launched countless identity theft related crimes. This proposed legislation would act as a strong deterrent to not only those committing the initial intrusion, but to the vast potential users of that information who would utilize it to commit their own criminal fraud schemes.

The impact is greater than just the loss of money or property. As the victims of identity theft well know, it is a particularly invasive crime that causes immeasurable damage to the victim's good name and reputation in the community; damage that is not easily remedied. The threat is made graver by the fact that terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.

For example, an Al-Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification

would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc. Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan, Afghanistan, etc.

The FBI has implemented a number of initiatives to address the various fraud schemes being utilized by terrorists to fund their terrorist activities. One involves targeting fraud schemes being committed by loosely organized groups to conduct criminal activity with a nexus to terrorist financing. The FBI has identified a number of such groups made up of members of varying ethnic backgrounds which are engaged in widespread fraud activity. Members of these groups may not themselves be terrorists, but proceeds from their criminal fraud schemes have directly or indirectly been used to fund terrorist activity and/or terrorist groups. By way of example, the terrorist groups have siphoned off portions of proceeds being sent back to the country from which members of the particular group emigrated. We believe that targeting this type of activity and pursuing the links to terrorist financing will likely result in the identification and dismantlement of previously unknown terrorist cells. Prior to 9/11, this type of terrorist financing often avoided law enforcement scrutiny. No longer. The FBI will leave no stone unturned in our mission to cut off the financial lifeblood of terrorists.

Another initiative has been the development of a multi-phase data mining project that seeks to identify potential terrorist related individuals through Social Security Number misuse analysis. The FBI, through its Terrorist Financial Review Group, is taking SSNs identified through past or ongoing terrorism investigations and providing them to the Social Security Administration for authentication. Once the validity or non-validity of the number has been established, investigators look for misuse of the SSNs by checking immigration records, Department of Motor Vehicles records, and other military, government and fee-based data sources. Incidents of suspect SSN misuse are then separated according to type. Predicated investigative packages are then forwarded to the appropriate investigative and prosecutive entity for follow-up.

Given the alarming nature of the threat posed by identity theft and the potential nexus to terrorism, the FBI is grateful for the efforts of Congress and this Subcommittee in pursuing this legislation which will considerably aid law enforcement efforts to address the threat. Enhancing the penalties for identity theft makes it clear that identity theft is a serious crime with serious consequences. It will encourage law enforcement to more aggressively investigate this type of crime and for it to be prosecuted. All of which will likely serve as a deterrent and slow the growth rate of identity theft related crimes. Thank you.