
Identity Theft

(Sunday, 29 August 2004) - Contributed by Norm Weber - Last Updated (Wednesday, 09 March 2005)

Identity theft is the fastest growing crime in America. It is now getting tackled at the federal level, but it might not be enough, as perpetrators are still having a field day. "We have grown into an epidemic of 9.9 million new victims last year," said Mari Frank, author of the Identity Theft Survival Kit. "You can't blame law enforcement, because it's after the fact – cleanup, not prevention or protection. Anyone who collects information and who has improper handling practices can be a culprit."

In 1998 Congress passed the Identity Theft Assumption Deterrence Act (ITADA), making it a federal crime when anyone knowingly transfers or uses, without lawful authority, a means of identification of another person with intention to aid, abet or commit any unlawful activity that constitutes a violation of any law.

At the end of last year President Bush signed the Fair and Accurate Transactions Act (FACTA) into law. Under the act, every American is entitled to receive a free credit report once per year to help monitor possible theft, as well as protection from identity theft before it occurs by requiring merchants to better handle customer information. FACTA also implements a national system of fraud detection and calls for credit agencies to take action before a victim even knows the crime has occurred. However, experts in the identity theft prevention arena are in doubt over whether FACTA will have any affect. of all of the fraud at no cost to the victim," she said.

However, there are loopholes and the enforcement of the act is going slow. The financial industry is facilitating the crime, which is the industry with the heaviest hitting lobbyists in D.C.

Companies can sell information if the individual does not "opt-out" of databases that are sold. Opting out typically means calling the number in the fine print of long statements sent out by banks regarding privacy protections. Unfortunately, most people just throw away these statements without reading the fine print.

Most companies are not required by state or federal law to shred sensitive information, so paper records go into the dumpster, where "dumpster divers" retrieve the information and use it to set up accounts.

Also, IT people at large companies will be more concerned with "security" than they are with "privacy."

"They're not thinking in overall privacy consciousness," Frank said. "High tech people are guarding the systems with their lives. They are blind to the offline stuff, which is where most of the stuff is stolen and used to make checks, steal money out of your bank and use your ATM card."

Frank has put together a video on identity theft for PBS and is coming out with a book in December, which will first go as a PBS pledge item and then go to the bookstores in January.

Frank is not a big fan of FACTA, but admits it's going to be some help.

"Some of the people who have our information have negligent information handling practices," she said. "I doubt FACTA will make a difference."

Credit card companies often send out blank credit checks to cardholders. The checks can be written against their credit card account. Thirty-five percent of those checks are used fraudulently, Frank said.

"You can't even call it (identity theft) the new crime of the century any more," said Linda Foley, president of the Identity Theft Resource Center. "There's nothing new about it. We need to put a lid on it and document handling and document disposal is a part of the picture. Identity theft is a crime of opportunity."

Foley addresses both the mishandling of paper and electronic information.

"Because we are a multi-media world now, we must consider document disposal as a multi-media problem," Foley said. "The document disposal industry can influence the other industries. We have the business side of it that collects tons of information on it that is completely unnecessary. Why do employers ask for your social security number on an application? Don't they just need it when they get ready to hire you?"

If the company did not collect this information, they would be less liable for the information they collect, because there would be less of it.

"People look over your shoulder when you fill out information; people know how to lip read," said Foley. "This is their business the same way a pickpocket spends hours learning how to lift a wallet. Every company should have two receptacles at each station, one should be trash and one should be documents that should be disposed of properly."

Landlords and mortgage brokers are two business people who collect information on people they wind up not doing business with. Sometimes that information is thrown into the dumpster. Big companies with lots of information in their trash are the big targets of identity thieves.

"Why should they get dirty with my chicken juices and kitty litter when they can go dumpster diving behind companies?" said Foley. "It's far more profitable because they are going to have large quantities of information when they find the treasure chest. Usually the dumpsters aren't on private property."

Shredding companies, lock box companies and others like them are part of the solution, according to Foley. But not the

total solution.

“There are going to be some studies coming out soon,” said Foley. “They are quantifying that more than half of all identity theft cases begin with some kind of breach of information in the workplace. It could be a customer service person, someone handling an application, or from mishandling document disposal.”

Instances exist where under the same social security number, credit reports have been issued under two different names - the real person and an illegal immigrant who might have stolen the social security number and created an identity for herself. In another case, a baby had a credit report two months before it was born.