

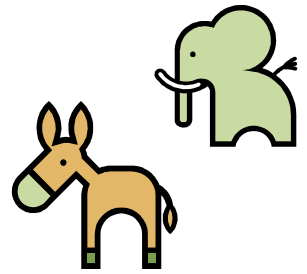
July 7, 2006



FRAUD TIP OF THE WEEK

Businesses and Governmental Agencies Contribute to the Identity Theft Problem

By Detective Paul Henninger



Most people think of an identity thief as an unemployed drug-crazed “Methhead” who steals your personal information from your home, car, mail, garbage or computer. This statement is only partially true.

The relationship between methamphetamine and identity theft is true. Over 90% of the persons I arrest for fraud or identity theft are involved with methamphetamine. I believe this arrest statistic would be true anywhere in the United States. I recently talked with a person in prison who had been the mastermind of a major identity theft ring operating throughout Oregon. I asked him about the relationship between “meth” and the people who commit identity theft. He told me, “They are as husband and wife.”

The myth that most personal information is stolen directly from the victim is not true. A national study showed that 70% of all stolen personal information is taken from a business. I have found that personal information is easily stolen from businesses because of bad employees or poor business practices in protecting banking or personal information. It is common for me to arrest an identity thief who has stolen victim profiles while working for a private business or governmental agency. I am currently conducting such an investigation. Why?

- ✓ Many businesses and government agencies do not do background checks on persons they hire. This practice includes not doing a background check on a person who will have access to personal information of customers, clients or employees. Some private businesses and government agencies have knowingly, or unknowing, hired convicted felons. I know of felons who have been hired by both private businesses and government agencies, even though they have been arrested or convicted of fraud or identity theft.
- ✓ Many businesses and government agencies do not have mandatory random drug testing.
- ✓ Some businesses and government agencies allow employees to take home laptop computers with customer or employee databases on them. Some of the laptops are stolen out of the employee’s car or from their home.
- ✓ Many businesses have few or inadequate controls in place to prevent theft of personal information by employees or persons breaking into the business. Many do not enforce the controls that are in place.

- ✓ Even with all the publicity, there are still businesses that throw into the trash the personal information of their customers or contacts. Every night there are “dumpster divers” in the trash behind businesses looking for information and credit card receipts.
- ✓ Some businesses still use unlocked mailboxes for their incoming and outgoing mail. It is common for mail thieves to check mailboxes first thing in the morning and just after delivery.

ADVICE to Businesses and Government Agencies:

- A criminal history and background check should be done on all employees who handle money or have access to the personal information of others.
- A random drug-testing program should be in place for all persons who have access to money or the personal information of others. This should be a standard for government agencies.
- If employees are allowed to take laptop computers out of the office or to their home, and the computer contains any sensitive or personal information of others, there should be strict guidelines as to how the computer is secured when not at the office. In addition, and most importantly, the information should be encrypted, not just password-protected, to reduce the impact if it is lost or stolen.
- Develop and strictly enforce security protocol for all banking and personal information maintained. Have a plan of action to notify victims if a breach occurs.
- Shred all paperwork that contains sensitive or personal information.
- Never use an unlocked mailbox for incoming or outgoing mail.
- Have the capability to review computer logs of all inquires or viewing of banking and personal information databases.
- Password protect all computers in the workplace.
- Relatively inexpensive encryption software is available. The upcoming “Vista” operating system from Microsoft is supposed to include some new encryption capabilities.
- If you deal with a business, ask them about their security protocol regarding personal information and whether they share that information with anyone. Ask them if they do background checks on employees who have access to your personal information.
- Ask the same questions of your local, state and federal government agencies .
- The FTC is a great resource. They have current information about Identity Theft. The FTC’s website concerning Identity Theft can be found at www.consumer.gov/idtheft. Click on the Business link, then “Dealing with a Data Breach.” It will take you to a printable brochure called “Information Compromise and the Risk of Identity Theft: Guidance for Your Business.”

Side Note: Did you know that if you call the Oregon DMV information call center using the published number, there is a good chance you will be talking with an Inmate (convicted felon) at the Coffee Creek Correctional Facility (prison) in Wilsonville. This is part of the State of Oregon prisoner work plan. You won’t be told you’re talking to a prisoner unless you ask. They have computer access to some of your personal information. DMV officials have told me they have set up strictly enforced protocols to prevent prisoners from using the system to commit identity theft.