May 2004
Volume 2, Issue 1

Inside this Brief

Legislative Committee Services
State Capitol Building
Salem, Oregon 97301
(503) 986-1813

Background Brief on…

Identity Theft

Prepared by: Bill Taylor

Background

The 1999 Legislature, in enacting House Bill 3057, created the new crime in Oregon of identity theft. It did so, in response to the rapidly expanding use by criminals of other people's identity for the purposes of fraud.

A person commits a Class C felony of identity theft if the person, with the intent to deceive or to defraud, obtains, possesses, transfers, creates, utters or converts to the person's own use the personal identification of another person. Personal identification is defined broadly in statute to include almost any identification (including name, date of birth, driver's privileges, personal identification number, or photograph) of a real or imaginary person. As originally enacted in 1999, the law prohibited misuse of another's identification "with the intent to defraud." In 2001, House Bill 2918 changed the state of mind requirement to "with the intent to deceive or defraud" to clarify that the law applies to misuse of identification for pecuniary or non-pecuniary reasons.

On October 30, 1998, Congress enacted the "Identity Theft and Assumption Deterrence Act." In doing so, it made it a federal crime to transfer or use another person's identity 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.

Of the victims who reported identity theft to the Federal Trade Commission, 42 percent reported credit card fraud, 20 percent reported the identity thief obtained unauthorized utility services or telecommunications or equipment in their name, and 13 percent reported identity theft targeting their checking or savings account.

How it Happens

Identity theft takes three primary forms. The first, "true name" fraud, occurs when someone uses a consumer's personal information to open accounts in the consumer's name. The thief then uses these fraudulently obtained accounts to purchase goods and services, leaving the consumer with the bills. The consumer may find accounts in her name owing thousands of dollars if victimized in this manner. A second form of identity theft is "account takeover" fraud. This is when a criminal gains access to

existing accounts and makes fraudulent charges on the victim's checking, savings, or credit accounts. The third type of identity theft occurs when a criminal provides a victim's personal information to law enforcement when the criminal gets arrested. Unless discovered and corrected by law enforcement, a victim can have an outstanding warrant or criminal record attached to their name without even realizing it until a background check uncovers the deception.

Criminals use several techniques to gain access to a person's identity. Some may steal mail from a business or residence, usually stealing outgoing checks. The thief then may attempt to forge new checks using the victim's name or account number, or merely attempt to cash the checks the victim wrote for an intended payee. Another "low tech" means of gaining access to identification that is being used by criminals is known as "dumpster diving." These are usually late-night expeditions into trash cans or dumpsters to obtain checks, copies of credit card statements, or credit card applications.

The information age has allowed those with the ability to use the internet and computers to obtain and utilize personal information. Check-writing software allows a person with the use of a computer, security paper, and a laser printer to create high-quality, forged checks if the criminal can obtain the account number or other information of a victim. On the internet, some unsuspecting victims fall prey to unsolicited emails, known as "spam," that promise some benefit if the victim enters his or her identifying data. Finally, some computer "hackers" have been able to glean large amounts of personal data from bank or government data banks. Such crimes violate Oregon's forgery laws and Oregon's computer crime statute in addition to constituting identity theft.

Sentencing

The presumptive sentence for a first conviction of identity theft is an 18-month probation sentence, which usually includes a short jail sentence, work release, and an order to pay restitution. However, identity theft is subject to the Repeat Property Offender statute, codified as ORS 137.717. If a person is convicted of misusing several people's identities in one indictment, each subsequent count after the first is considered to have occurred after that first conviction. Consequently, an identity thief may be considered a repeat property offender for stealing several people's identity during one criminal episode. The presumptive sentence for a conviction of identity theft as a repeat property offender is 13 months.

Limitations on Application of Oregon's Identity Theft Law

This law does not apply to:

- A person under 21 who uses a false ID to buy alcohol
- A person under 18 who uses a false ID to buy tobacco
- Any underage person who uses a false ID to enter a bar or other place with an age restriction

2004 Legislation

- Includes Identity Theft in crimes identified as RICO predicates.[1]
- Creates the crime of unlawful possession of a personal identification device and classifies it as a Class C felony. A person commits the crime if the person, with the intent to commit a crime, possesses a device that is used to manufacture or print: (a) A driver license or permit; (b) An employee identification card; or (c) A credit or debit card.[2]
- Expands the crime of unlawful factoring of credit card transactions to debit and other such cards. Enhances the penalty for second and subsequent such convictions.[3]
- Increases the penalty for unlawful production of identification cards, licenses, permits, forms or camera cards from a Class A misdemeanor to a Class C felony.[4]

Information for Victims

The Federal Trade Commission recommends victims take the following action immediately if they find they have been a victim of identity theft:

- Contact the fraud departments of each of the three major credit bureaus, and tell them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name. The three credit bureaus are:

[1] HB 2119
[2] HB 3296
[3] HB 3317
[4] HB 3318

Equifax, 1-800-525-6285 or www.equifax.com;
Experian, 1-888-Experian or www.experian.com; and
Trans Union, 1-800-680-7289 or www.tuc.com

- Contact the creditors for any accounts that have been tampered with or opened fraudulently, ask to speak to the fraud department, and then follow up in writing with a letter explaining your accounts have been compromised
- File a report with your local police department or the police in the locations where the identity theft took place

Staff and Agency Contacts:

Federal Trade Commission ID Theft Hotline
1-877-ID THEFT
http://www.consumer.gov/idtheft/

Bill Taylor Judiciary Counsel
503-986-1694