Background Brief on …

# Identity Theft

June 2010

## Inside this Brief

- **How it Happens**
- **Sentencing**
- **Information for Victims**
- **Staff and Agency Contacts**

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

The crime of identity theft was created in Oregon by the 1999 Legislative Assembly in response to increasing abuse of people's personal identifying information by criminals.

A person commits the Class C felony of identity theft if the person, with the intent to deceive or defraud, obtains, possesses, transfers, creates, utters, or converts to the person's own use the personal identification of another person (ORS 165.800). "Personal identification" is broadly defined to include almost any identification (**ID**), including one's name, date of birth, driver's privileges, personal identification number, or a photograph of a real or imaginary person (ORS 165.800(4)(b)).

The law applies to misuse of identification for pecuniary or non-pecuniary reasons; however, it 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; or,
- Any underage person who uses a false ID to enter a bar or other place with an age restriction

The 2003 Legislative Assembly addressed the problem of identity theft again by:

- Creating the Class C felony of unlawful possession of a personal identification device (ORS 165.810);
- Creating the Class C felony of unlawful possession of fictitious identification (ORS 165.813);
- Expanding the crime of unlawful factoring of credit card transactions to debit and other cards, and enhancing the penalty for second and subsequent such convictions; and,
- Increasing the penalty for unlawful production of identification cards, licenses, permits, forms, or camera cards from a Class A misdemeanor to a Class C felony.

On October 30, 1998, Congress enacted the "Identity Theft and Assumption Deterrence Act" (18 USC 1028) making it a federal crime to transfer or use another person's identity with the intent to commit, or aid or abet, any unlawful activity constituting a violation of any applicable state, local, or federal law.

Of the victims who reported identity theft to the Federal Trade Commission at the time, 42 percent reported credit card fraud, 20 percent reported that utility services or tele-communications or equipment were obtained in their name, and 13 percent reported that their checking or savings account had been targeted.

## How it Happens

Identity theft takes three primary forms. The first, sometimes referred to as "true name fraud," occurs when someone uses a victim's personal information to open accounts in the victim's name. Goods and services are then obtained using the unauthorized accounts and the victim is stuck with the bill.

A second form of identity theft is "account takeover fraud." This occurs when a criminal gains access to a consumer's existing checking, savings, or credit accounts and incurs unauthorized charges.

The third type of identity theft occurs when a criminal is arrested and they provide another person's identifying information to law enforcement. Unless discovered and corrected, a victim can accumulate outstanding warrants and have a criminal record associated with their identity, entirely unknown to them until a background check reveals the deception.

Criminals use several techniques to gain access to a victim's personal identifying information. Some steal mail from businesses or homes, including outgoing checks. A thief can then attempt to cash those checks, and also forge new checks using the victim's name and account number. Another "low tech" means of obtaining identifying information is known as "dumpster diving." These are usually late-night expeditions into trash cans or dumpsters to obtain discarded checks, banks statements, credit card statements, or credit card applications or offers; anything discarded by a consumer that could contain personal identifiers and account information.

The information age has allowed criminals with access to computers and the internet to obtain and exploit other people's personal information in entirely new ways. Some unsuspecting victims fall prey to unsolicited emails, or "spam," that promise a benefit if they provide their identifying and account information. Check-writing software that allows anyone with a computer, security paper, and a laser printer to create high-quality checks, is susceptible to abuse by criminals in furtherance of fraud. Personal information is now also primarily gathered and stored in electronic form which can be vulnerable to "hacking."

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 for identity theft is an 18-month probationary period that usually includes a short jail sentence, work release, and an order to pay restitution. Identity theft, however, is subject to the Repeat Property Offender statute (ORS 137.717). If a defendant is charged and convicted of several separate counts for using several different victim's identities during a single criminal episode, each such conviction counts in succession, so the thief may be considered a repeat property offender for sentencing purposes.

The presumptive sentence for a conviction of identity theft as a repeat property offender is 24 months of incarceration. The 24-month sentence applies to crimes committed after January 1, 2009; however, as a result of severe budget shortfalls and the need to reduce prison costs, those sentenced between February 15, 2010, and January 1, 2012, will receive a 13-month sentence.

Senate Bill 447 (2007) added "deceased" to the definition of a person under the statute and

added trust company account information to the definition of personal identification.

## Information for Victims

The Federal Trade Commission recommends the following immediate action upon discovery of identity theft by the victim:

- Contact the fraud departments of each of the three major credit reporting agencies 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 major credit reporting agencies are:
    - Equifax - 800-525-6285
    - Experian - 888-397-3742
    - Trans Union - 800-680-7289
- Contact creditors for any accounts that have been tampered with or opened fraudulently, ask to speak to the fraud department. Follow up in writing with a letter explaining that your identity has 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
877-438-4338

Bill Taylor
Judiciary Committee Counsel
Legislative Committee Services
503-986-1694