LPRO: Legislative Policy and Research Office

IDENTITY THEFT

BACKGROUND BRIEF

In 2014 alone, approximately seven percent of the U.S. population over the age of 16 were victims of identity theft.[1] The leading form of identity theft comes through misuse of an existing credit card or bank account, while a small percent of victims experience theft from creation of a new account. Nearly one-fifth of victims have been victimized multiple times. In the vast majority of cases (92 percent), the victim does not know the identity of the offender.

In Oregon, 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.

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

CONTENTS

In 2003, the legislature expanded the criminal statutes related to identity theft by:

- Creating a Class C felony for the unlawful possession of a personal identification device. 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 driver's license or permit, an employee identification card or a credit or debit card.
- Creating a Class C felony for the unlawful possession of fictitious identification. A person commits the crime if the person possesses a personal identification card containing identification information for a fictitious person with the intent to use the personal identification card to commit a crime.
- Expanding the crime of unlawful factoring of credit card transactions to debit and other such cards and enhances the penalty

[1] Bureau of Justice Statistics bulletin, September 2015.http://www.bjs.gov/content/pub/pdf/vit14.pdf.

for second and subsequent such convictions.
- 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.

OREGON CONSUMER IDENTITY THEFT PROTECTION ACT

Oregon also has a cause of action within its civil statutes for addressing data breaches and identity theft. The Oregon Consumer Identity Theft Protection Act **(OCITPA)** was created in 2007 and updated in 2015. The OCITPA requires any person or company that maintains sensitive information of a consumer, including name, address, social security number, state identification number, financial account information, health information or biological data, to inform the consumer of the breach as soon as possible after the breach is discovered. Notice of the breach is required to be sent to the Attorney General when the breach involves 250 or more consumers. Failure to notify is an Unlawful Trade Practice **(UTP)** and has civil remedies. Additionally, OCITPA requires companies to develop reasonable safeguards for protecting consumer's data.

HOW IDENTITY THEFT 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 his or her name owing thousands of dollars if victimized in this manner.

A second form of identity theft is *account takeover fraud*. This occurs when someone 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 someone provides a victim's personal information to law enforcement when the person 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 databases. Such crimes violate Oregon's forgery laws and Oregon's computer crime statute in addition to constituting identity theft.

PREVENTING IDENTITY THEFT

Several trustworthy resources are available for consumers to proactively find assistance in preventing and recovering from identity theft. There are scams set up to "assist" consumers with recovering or preventing theft while actually re-victimizing individuals. Best practices recommended by the Federal Trade Commission **(FTC)** can be found at www.identitytheft.gov and include:

- Use of credit monitoring services;
- Regularly reviewing bank accounts;
- Signing up for free credit reports to monitor for any new unauthorized accounts or charges; and
- Placing a credit freeze on your or your child's banking accounts.[2]

INFORMATION FOR VICTIMS

The FTC 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:
  - Equifax - 800-525-6285
  - Experian - 888-397-3742
  - TransUnion - 800-680-7289
- 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; and
- File a report with your local police department or the police in the locations where the identity theft took place.

STAFF CONTACT

Channa Newell
Legislative Policy and Research Office
503-986-1525
channa.newell@state.or.us

Please note that the Legislative Policy and Research Office provides centralized, nonpartisan research and issue analysis for Oregon's legislative branch. The Legislative Policy and Research Office does not provide legal advice. Background Briefs contain general information that is current as of the date of publication. Subsequent action by the legislative, executive or judicial branches may affect accuracy.

[2] http://consumersunion.org/pdf/security/securityOR.pdf.