To organize and support community partnerships to prevent crime and the fear of crime

4747 E. Burnside
Portland, Oregon 97215

tel 503-823-4064
fax 503-823-2909
tty 503-823-6969

This document is available at the Crime Prevention Program website:

www.portlandoregon.gov/oni/cp

office of neighborhood involvement

Identity Theft

When bad things happen to your good name

Office of Neighborhood Involvement Crime Prevention Program
Fall 2013

Identity theft is when someone uses your personal information, such as your name, Social Security Number, or your personal financial information, to commit fraud or other crimes. It can be very difficult and time-consuming to regain your good name and credit rating after being the victim of identity theft. Prevention is much easier.

How Identity Theft Occurs

HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION

- They get information from business or other institutions by stealing records or information while they're on the job, bribing an employee who has access to these records, hacking these records, or conning information out of employees.
- They may steal your mail, including bank statements, credit card offers, and new unused checks.
- They may steal your wallet or personal information from your home.

Skimming, Phishing, Pretexting, and Dumpster Diving

ID Thieves may steal your credit or debit card numbers by capturing the information in a data storage device attached to an ATM in a practice known as "skimming." They may steal personal information from you through email ("phishing") or phone ("pretexting") by posing as legitimate companies and claiming that you have a problem with your account. ID thieves will rummage through your trash in a practice known as "dumpster diving."

How to Prevent Identity Theft

ACCOUNT SECURITY

- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done in your home.
- Ask about information security procedures in your workplace or at businesses, doctor's offices, or other institutions that collect your personally identifying information. Find out how your information will be shared with anyone else.
- Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know whom you're dealing with. Before you share any personal information, confirm that you are dealing with a legitimate organization.

El Programa de la Prevención del Crimen tiene un miembro que habla español. Llame por favor al número principal 503-823-4000 si usted necesita los servicios en español.

MORE IDENTITY THEFT INFORMATION

For much more detailed identity theft prevention and resolution information visit *www.consumer.gov/idtheft* and download or view the Federal Trade Commission's June 2005 "Take Charge: Fighting Back Against Identity Theft." This information sheet is only a brief summary of the useful identity theft tips in the longer document.

- Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox.
- Tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. To opt out of receiving credit offers in the mail call 1-888-5-OPTOUT.
- Don't carry your Social Security card; leave it in a secure place.
- Give your Social Security Number (SSN) only when absolutely necessary. If someone asks for your SSN, ask: Why do you need it? How will it be used? How do you protect it from being stolen? What will happen if I don't give you my SSN?
- When ordering new checks, pick them up at the bank instead of receiving them in the mail.

COMPUTER SECURITY

- Virus protection software should be updated regularly, and patches for your operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of your computer files and passwords.
- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know.
- Use "strong" passwords- combinations of letters (upper & lower case) and numbers.
- Use a firewall program if you use a high-speed Internet connection that leaves your computer connected to the Internet 24 hours a day to stop uninvited access to your computer.
- Do not conduct financial transactions of any kind over the internet unless you are using a secure browser to encrypt or scramble sensitive information. Look for "https" instead of "http" in the location bar, and a padlock icon near the bottom of the browser window.
- Look for website privacy policies to answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties.

If Your Identity Has Been Stolen

IMMEDIATE ACTION

- Place a fraud alert on your credit reports, and review your credit reports. Fraud alerts help prevent an identity thief from opening any more accounts in your name. Contact one of the three credit bureaus:

  Equifax: 1-800-525-6285; www.equifax.com
  Experian: 1-888-397-3742; www.experian.com
  TransUnion: 1-800-680-7289; www.transunion.com
- Close the accounts you know, or believe, have been tampered with or opened fraudulently.
- File a report with your local police or the police in the community where the identity theft took place.
- File a complaint with the Federal Trade Commission. Visit *www.consumer.gov/idtheft* or call 1-877-438-4338 to register your complaint.
- Obtain a copy of "Take Charge: Fighting Back Against Identity Theft" from the Federal Trade Commission (see above for contact info) and follow their suggestions for recovery from identity theft.