Thurston County Sheriff's Office

"Creating a Safer Community Together."

Identity Theft Information and Resources

How to Protect Yourself

- Get a locking mailbox. None of us would leave our personal belongings out on the street, so why do we leave our personal information in an unsecured box?
- Password-protect your credit accounts with something other than your mother's maiden name.
- Before revealing personal identifying information, find out how it will be used and if it will be shared. Ask if you have a choice about the use of your information.
- Pay attention to your billing cycles. Follow up with creditors if bills do not arrive on time. Give your Social Security number only when absolutely necessary. Ask to use other types of identifiers when possible.
- Minimize the identification information and the number of cards you carry.
- Order a copy of your credit report from the three credit reporting agencies (listed below) every year. Make sure it's accurate and includes only those activities you have authorized. Federal law requires these agencies provide you with a free copy of your report annually, upon request. To obtain a free copy of your credit report, go to https://www.annualcreditreport.com.

A Word on Passwords

Whether you are on the Internet or an online banking program, you are often required to use a password. The worst passwords to use are the ones that come to mind first - name, street addresses, etc. The best passwords mix numbers with upper and lowercase letters. A password that is not found in the dictionary is even better. There are programs that will try every word in the dictionary in an effort to crack your security. Do not be a "Joe"-someone who uses their name as their password.

The weakest link in a security system is the human element. The fewer people who have access to your codes and passwords the better. Avoid breaks in your security by:

- Changing your password regularly.
- Memorizing your password. If you have several, set up a system for remembering them. If you do write down the password, keep it at home or hidden at work. Don't write your password on a post-it note and stick it on your monitor or hard drive.
- Set up a special account or set aside a different computer at work for temporary employees and other unauthorized users.
- If you have the option of letting your computer or a Web site remember a password for you, don't use it. Anyone who uses your machine will have automatic access to information that is password protected.
- Do not send confidential, financial, or personal information on your email system.

Shopping in Cyberspace

Ordering merchandise from the Internet is the trend of the future. You can prevent problems before they occur by:

- Doing business with companies you know and trust. If you have not heard of the company before, research it or ask for a paper catalog before you decide to order electronically. Check with your state consumer protection agency on whether the company is licensed or registered. Fraudulent companies can appear and disappear very quickly in cyberspace.
- Understanding the offer. Look carefully at the products or services the company is offering.

Be sure you know what is being sold, the quality being specified, the total price, the delivery date, the return and cancellation policy, and all the terms of any guarantee.

- Using a secure browser that will encrypt or scramble purchase information. If there is no encryption software, consider calling the company's 800 number, faxing your order, or paying with a check.
- Never giving a bank account or credit card number or other personal information to anyone you do not know or haven't checked out. And do not provide information that is not necessary to make a purchase. Even with partial information, con artists can make unauthorized charges or take money from your account. If you have a choice between using your credit card and mailing a check or money order, use a credit card. You can always dispute fraudulent credit card charges, but you cannot get "cash" back.

Using ATMs, Long Distance Phone Services, and Credit Cards

Protection: Your Personal Identification Number (PIN)

The PIN is one method used by banks and phone companies to protect your account from unauthorized access. A PIN is a confidential code issued to the cardholder to permit access to that account. Your PIN should be memorized, secured and not given to anyone, not even family members or bank employees. The fewer people who have access to your PIN, the better. Never write your PIN on ATM or long distance calling cards. Don't write your PIN on a piece of paper and place it in your wallet. If your wallet and card are lost or stolen, someone will have everything they need to remove funds from your account, make unauthorized debit purchases, or run up your long distance phone bill.

Protect Your Privacy and the Privacy of Others

Be aware of others waiting behind you. Position yourself in front of the ATM keyboard or phone to prevent anyone from observing your PIN. Be courteous while waiting at an ATM or pay phone by keeping a polite distance from the person ahead of you. Allow the current user to finish before approaching the machine or phone.

Safety Tips When Using/Choosing An ATM

- Be aware of your surroundings, especially between dusk and dawn. If you notice anything suspicious (a security light out, someone loitering nearby), consider returning at a later time or using an ATM in a more populated location.
- If using the ATM at night, take someone with you.
- Park in a well-lit area, as close as possible to the ATM.
- At a drive-through ATM, be sure the doors are locked and the passenger windows are rolled up.
- Shield the keypad when entering your PIN to keep it from being observed.
- Avoid being too regular in your ATM use; do not repeatedly visit the same machine at the same time, the same day of the week.
- An ATM card should be treated as though it were cash. Avoid providing card and account information to anyone over the phone.
- When making a cash withdrawal at an ATM, immediately remove the cash as soon as the machine releases it. Put the cash in your pocket and wait until you are in a secure location before counting it. Never use an ATM in an isolated area or where people are loitering.
- Be sure to match your ATM receipts against your monthly statement. Dishonest people can use your receipt to get your account number. Never leave the receipt at the site.

Crime can be random - take steps to limit your chances of becoming a victim. Being aware of the threat of crime and alert to what you can do to prevent it will help make your electronic transactions safe and private.

Protect Your Credit Cards

- Only give your credit card account number to make a purchase or reservation you have initiated.
- Never give credit card information over a cellular phone.
- Never give your credit card to someone else to use on your behalf.
- Check to see if your credit card company offers the option to add your picture to your bank or credit card. This is a great deterrent to crooks who want to use your card.
- Watch your credit card after giving it to store clerks to protect against extra imprints being made.
- Destroy any carbons. Do not discard into the trashcan at the purchase counter. Keep charge slips in a safe place.
- Protect your purse or wallet, especially when traveling or in crowded situations.
- Save all receipts, and compare them to your monthly statement. Report any discrepancies immediately.
- Keep a master list in a secure place with all account numbers and phone numbers for reporting stolen or lost cards.

Lost or Stolen Credit / Bank Cards

Always report lost or stolen cards to the issuing company immediately. This limits any unauthorized use of your card and permits the company to begin the process of issuing a new card.

What To Do If It Happens To You:

In your contacts with the authorities and financial institutions, keep a log of all conversations, including dates, names, and phone numbers. Note the time spent and any expenses incurred, in case you are able to request restitution in a later judgment or conviction against the thief. Confirm conversations in writing. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents.

1. ***Credit Bureaus***: Immediately call the fraud units of the three credit reporting companies: Experian (formerly TRW), Equifax and Trans Union [links below]. Report the theft of your credit cards or numbers and request a credit report (free to identity theft victims). Ask that your file be flagged with a fraud alert. Add a victim's statement to your report. ("My ID has been used to apply for credit fraudulently. Contact me at [your phone number] to verify all applications.") Ask how long the fraud alert is posted on your file and how you can extend it if necessary.
   Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Request another copy of your credit report every few months so you can monitor any new fraudulent activity.

   Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months (two years for employers) in order to alert them to the disputed and erroneous information.

2. ***Creditors***: Immediately contact all creditors with whom your name has been used fraudulently, both by phone and in writing. You may be asked to fill out fraud affidavits. (New law requires these to be notarized at your own expense.) Ask that your account be password protected with something other than your mother's maiden name and social security number. Obtain replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen," because it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

3. ***Law Enforcement***: Report the crime to your local police or sheriff's department. You may also need to make a report to the police department(s) where the crime(s) occurred. Give them as much documented evidence as possible. Make sure the police report lists the fraudulent accounts. Obtain a copy of the report. Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime. It is a violation of federal law (18 USC 1028) and the laws of many states to assume someone's identity for fraudulent purposes. Some police departments don't write reports on such crimes, so be persistent! Also, report to the Federal Trade Commission.

4. ***Stolen Checks***: If you have had checks stolen or bank accounts set up fraudulently, report it to the appropriate check verification companies. Authorize a "stop payment" on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not your mother's maiden name). If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses.

5. ***ATM Cards***: If your ATM or debit card has been stolen or compromised, report it immediately. Obtain a new card, account number and password. Do not use your old password. When creating a password, don't use common numbers such as the last four digits of your SSN or your birthdate. Monitor your account statement. You may be liable if fraud is not reported quickly.

6. ***Fraudulent Change of Address***: Notify the local Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit fraud. (Call the U.S. Post Office at 800.275.8777 to obtain the correct phone number for your particular area. Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier.

7. ***Secret Service Jurisdiction***: The Secret Service has jurisdiction over financial fraud, but it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks, as well as the police investigator, to notify the particular Secret Service agent they work with.

8. ***Social Security Number (SSN) Misuse***: Call the Social Security Administration to report fraudulent use of your SSN. As a last resort, you might want to try to change your number, although we don't recommend it except for the most serious cases. The SSA will only change the number if you fit their fraud victim criteria. Also, order a copy of your Personal Earnings and Benefits Statement and check it for accuracy. The thief might be using your SSN for employment purposes.

9. ***Passports***: Whether you have a passport or not, advise the passport office to alert them to anyone ordering a passport fraudulently - www.travel.state.gov/passport_services.html.

10. ***Phone Service***: If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password which must be used any time the account is charged.

Credit Reporting Bureaus

Equifax: P.O. Box 105069, Atlanta, GA 30348
Report Fraud: Call (800) 525-6285 and write to address listed above.
Order Credit Report: (800) 685-1111

Experian (formerly TRW): P.O. Box 9532, Allen, TX 75013
Report Fraud: Call (888) EXPERIAN, (888) 397-3742 and write to address above.
Fax: (800) 301-7196
Order Credit Report: (888) EXPERIAN

Trans Union: P.O. Box 6790, Fullerton, CA 92834
Report Fraud: (800) 680-7289 and write to address above.
Order Credit Report: (800) 888-4213

To opt out of pre-approved offers of credit for all three bureaus, call (888) 5OPTOUT. You may choose a two-year opt-out period or permanent opt-out status. Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit, if you receive welfare benefits, or if you are unemployed.

Social Security Administration

Report Fraud: (800) 269-0271. Order Earnings and Benefits Statement: (800) 772-1213

To remove your name from mail and phone lists:

Direct Marketing Association, Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735

Telephone Preference Service, P.O. Box 9014, Farmingdale, NY 11735

To report fraudulent use of your checks contact the specific check guarantee-verification company named by the merchant:

- CheckRite: (800) 766-2748
- Chexsystems: (800) 428-9623
- CrossCheck: (800) 843-0760
- Equifax: (800) 437-5120
- International Check Services: (800) 526-5380
- SCAN: (800) 262-7771
- TeleCheck: (800) 710-9898

Other Useful Resources:

Federal Trade Commission (FTC): You may receive help from and file your case with the FTC Consumer Response Center, (877) IDTHEFT. Be sure to provide your police report number if you have one.

Privacy Rights Clearinghouse (PRC):
Email: prc@privacyrights.org;
web address: www.privacyrights.org. Its web site contains many publications on identity theft.