Identity Theft

• Identity theft occurs when your personal information is used to commit certain crimes including theft, fraud, forgery, etc.
• It is also a crime to possess confidential personal information of another person without authorization.

Personal Information is anything that confirms your identity, but not limited to:

- •Driver's license number
- •Social Security Number
- •Bank account numbers
- •Passwords
- •Any name, number, code, etc. used to confirm who you are

Ways Criminals Get Information

Advance Fee Fraud is a scam that involves an advance payment from the victim to the scammer.

Dumpster Diving is rummaging through other people's trash to obtain personal information.

Phishing is a popular method that ID thieves use that utilizes "spam" (junk email) that tricks you into disclosing your sensitive information, such as account numbers, passwords and usernames.

Phishers send phony email messages that appear to be from a business or organization that you deal with— for example, your credit union, internet service provider, or even a government agency. The message will usually claim that your account information needs to be "updated" or "validated." The message may also contain a threat that your account will be "suspended" or "closed" should you fail to respond. It also directs you to a website that looks legitimate, complete with the company's logo. However, this website is NOT legitimate.

The purpose of this phony site is to fool you into disclosing your sensitive information so that the scam artists can steal your identity and run up bills or commit crimes using your name.

Phishing scams are growing at an alarmingly fast rate, and the frequency and sophistication of these scams are increasing dramatically. While on-line banking and e-commerce is generally very safe, you need to be VERY CAREFUL about giving out your personal financial information over the internet. Always report phishing, even if you're not a victim. Report any phishing emails to the following groups:

1) Forward the email to *reportphishing@antiphishing.com*
2) Forward the email to the FTC at *spam@uce.gov*
3) The company that is being "spoofed" (i.e. your bank or credit union)
4) When forwarding spoofed messages, always include the entire original email with its original header information intact
5) Notify Internet Fraud Complaint Center of the FBI by filing a complaint on their website: *www.ifccfbi.gov*

Shoulder Surfing is using direct observation techniques, such as looking over someone's shoulder, to obtain personal information.

Skimming is a scam where a device or person collects your credit, debit or ATM card information.

Theft of home, auto, wallet, cell phone, electronic organizers, and computers etc.

Unsecured Mailboxes allow thieves to access incoming and outgoing mail.

What Criminals Do With Your Data

- •Establish accounts and services such as loans, credit cards and retail accounts etc.
- •Obtain an official identification card.
- •Write your checks to make purchases.
- •Authorize transfers to deplete your account.
- •Make purchases with credit, ATM or debit cards.

Tips to Prevent Identity Theft

Online Purchases:

- •Designate one credit card with minimal limit for online shopping.
- •Do not go outside of the online store website to complete transactions.

Computer/Internet:

- •Use a firewall and virus protection.
- •Change passwords quarterly on your e-mail and online accounts.
- •If paying bills or shopping online, look for the Secure Sockets Layer Certificate or secure padlock on the bottom of the screen and https in the address box.
- •Destroy hard drive if discarding computer.

Finances:

- •Make sure you're receiving your monthly statements and/or bills.
- •Do not give out your financial account passwords and PIN numbers.
- •Keep track of your accounts: Check your online accounts on a regular basis. Don't leave it for as long as a month before you check each account. Also, regularly check your bank, credit card and debit card statements to ensure that all transactions are legitimate. If you see anything suspicious, contact your financial institution and all card issuers right away.

Stop Solicitations:

- Stop telemarketing solicitations
  1-888-382-1222
  www.donotcall.gov

- Stop mail and e-mail solicitations
  www.dmaconsumers.org

- Opt out of pre-approved credit card offers
  1-888-567-8688
  www.optoutprescreen.com

Obtain a free credit report to review:

- 1-877-322-8228
  www.annualcreditreport.com

If You are a Victim of Identity Theft

- Place a 90-day Fraud Alert on your credit file. Ask creditors to call you before opening any new accounts or changing existing accounts. Request copies of your credit report and review them carefully.

- **Equifax**
  1-800-525-6285
  www.equifax.com

- **Experian**
  1-888-397-3742
  www.experian.com/fraud

- **TransUnion**
  1-800-680-7289
  www.transunion.com

- Close any financial accounts that have been tampered with or established fraudulently.

- File a police report to help you with creditors who may want proof of the crime.

City and County of Honolulu	911
Maui County	(808) 244-6400
Kauai County	(808) 241-1711
Hawaii County	(808) 935-3311

- Make sure to obtain the police report number and copy of report if possible.

- File a complaint with the Federal Trade Commission and complete the **Identity Theft Complaint Form** and **Identity Theft Affidavit:**

Federal Trade Commission (FTC)
1-877-438-4338 www.ftc.gov

Mail:

- Install a locking mailbox or promptly remove incoming mail after delivery.
- Shred mail with your personal information.

Phone:

- Do not give out your personal information on the phone unless you initiated the contact.
- Ask questions and tell the caller you'll call them back. Don't call the number that was provided, call the number listed in the telephone book.

Credit Reports

What is a Credit Report? Companies that have granted you credit or loaned you money—such as banks or credit card companies—supply information about your accounts on a regular basis to credit reporting agencies (Experian, TransUnion and Equifax). This information is compiled into a credit report.

Your credit report may also contain information about you from public records, such as overdue property taxes or bankruptcies. Some states allow information about overdue child support payments to be included.

Why should you review your consumer credit report?

Your credit report is an important personal financial planning tool. It is the one, easy-to-read summary of your credit accounts and total indebtedness—both existing and potential. It can help you budget and plan for the future.

If you use credit, it's a good idea to review your credit report at least once a year. This is especially important when you're getting ready to buy an expensive item such as a car or new home. Taking the time to ensure your credit report is accurate and complete could prevent your loan approval from being delayed.

How might errors appear on your credit report?

- Typographical errors causing an incorrect letter or number to appear in the consumer's identifying information on the credit file.
- Variances in a credit report by obtaining credit under different names (Robert and Bob, Margaret and Peg, or J. Michael and James Michael); providing an inaccurate Social Security Number when applying for credit; or omitting the "Senior" or "Junior" when father and son share the same name.
- Payment experience is reported to Experian incorrectly. That can occur when a payment is applied to the wrong account.
- Errors in the credit reporting company's computerized processes.

How can you correct errors on your credit report?

Regardless of how errors are made, federal law allows consumers to dispute inaccuracies and correct their credit files, and that is always a good idea.

No one can remove accurate information. Accurate data helps consumers obtain credit and helps lenders make low-risk loans to more people.

Once you have received your credit report, there is no fee to dispute the information. Simply follow the instructions provided with your personal credit report.

How much does a credit report cost? Depending on the state you live in, the cost for a credit report can range from $3-$10.

What can I do if I am a victim of credit fraud? If you notice unauthorized charges on your credit accounts, contact the lenders as soon as you can. Notify them that your accounts are being used by someone else. To check if your credit has been damaged, contact each of the three largest credit bureaus and get copies of your credit reports. They should be free if you are a fraud victim. If you find unauthorized accounts, call the fraud department of each credit reporting bureau and ask how to place a "security alert" on your file.

The credit bureaus usually require a written request including your full name, current mailing address, Social Security number, date of birth and any previous addresses for the past two to five years. In most cases, the credit reporting bureaus will ask that you get a police report detailing the criminal activity. Call the non-emergency number for your local police department and explain your situation. According to many victims of identity theft, some police departments are not always helpful with this type of request. However, as the crimes of credit card fraud and identity theft become more well known, police departments are becoming more responsive in helping you prove you are a victim.

How do you request a "fraud alert" be placed on your file? You have the right to ask that nationwide consumer credit reporting companies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer credit reporting companies. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a consumer credit reporting company will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency. For more detailed information about the identity theft report, visit www.consumer.gov/idtheft.

Hawaii Identity Theft Resources:

AARP - Hawaii
toll free 1-866-295-7282

Better Business Bureau - Honolulu
(808) 536-8609 www.hawaii.bbb.org

City & County of Honolulu
Department of the Prosecuting Attorney
(808) 547-7400 or toll free 1-800-531-5538
www.honolulu.gov/prosecuting

Federal Bureau of Investigation - Honolulu
(808) 566-4300 honolulu.fbi.gov

State of Hawaii

- **Department of the Attorney General**
  Hawaii Internet & Technology Crimes Unit
  (808) 974-4000 ext. 74111 Hawaii
  (808) 274-3141 ext. 74111 Kauai
  (808) 984-2400 ext. 74111 Maui
  1-800-468-4644 ext. 74111 Molokai & Lanai
  (808) 587-4111 Oahu
  www.hitechcrimes.com

- **Department of Commerce & Consumer Affairs**
  (808) 974-4000 ext. 62653 Hawaii
  (808) 274-3141 ext. 62653 Kauai
  (808) 984-2400 ext. 62653 Maui
  1-800-468-4644 ext. 62653 Molokai & Lanai
  (808) 586-2653 Oahu
  www.hawaii.gov/dcca

- **Department of Health**
  Sage Watch
  (808) 586-7281 or toll free 1-800-296-9422
  www4.hawaii.gov/eoa/programs/sagewatch

United States Postal Service (808) 423-3790
United States Secret Service (808) 541-1912