



If You are a Victim of Identity Theft:

1. 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
2. Close any financial accounts that have been tampered with or established fraudulently.
3. File a police report or a misc. pub. 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
4. Make sure to obtain the police report number and copy of report if possible.
5. 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



Hawaii Identity Theft Resources:

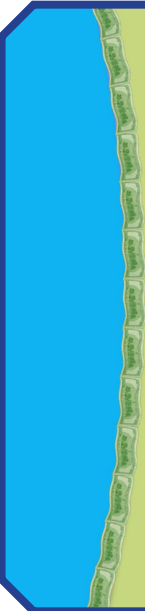
- ◆ **AARP - Hawaii**
toll free 1-866-295-7282
- ◆ **Better Business Bureau - Honolulu**
(808) 536-8609
www.hawaii.bbb.org
- ◆ **City & County of Honolulu**
Department of the Prosecuting Attorney
(808) 547-7400 or toll free 1-800-531-5538
www.honolulu.gov/prosecuting
- ◆ **Federal Bureau of Investigation - Honolulu**
(808) 566-4300
www.honolulu.fbi.gov
- ◆ **State of Hawaii:**
 - ◆ **Department of the Attorney General**
Hawaii Internet & Technology Crimes Unit
(808) 974-4000 ext. 741111 Hawaii
(808) 274-3141 ext. 741111 Kauai
(808) 984-2400 ext. 741111 Maui
1-800-468-4644 ext. 741111 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



YOUR IDENTITY IS YOUR KULEANA



Department of the Attorney General
Crime Prevention & Justice Assistance (CPJA) Division
Hawaii Internet & Technology Crimes (HITeC) Unit



What is 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 other name, number, code, etc. used to confirm who you are.

How is Personal Information Obtained?

- ◆ Frauds or scams.
- ◆ Phishing.
- ◆ Shoulder surfing.
- ◆ Hacking.
- ◆ Lost wallets, palm pilots, etc.
- ◆ Dumpster diving, skimming, unsecured mailbox, bribery, home or auto theft, etc.

Here are a few ways of how your personal information is obtained:

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 asking customers to update personal or sensitive information by impersonating businesses such as banks, credit card companies, online retail stores, government agencies, etc. by e-mail, mail or phone calls.

Shoulder Surfing:

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



What Happens if You Respond to a Scam?

- ◆ Monetary loss.
- ◆ Physical harm or death.
- ◆ Unable to purchase a car, home or obtain any type of credit.
- ◆ It can take years to re-gain good credit.

Here are a few ways of how your personal information is misused:

- ◆ Open new credit card.
- ◆ Establish phone or wireless service.
- ◆ Authorize electronic transfers to drain your bank account.
- ◆ Obtain an official identification card.

Prevent Identity Theft

Auction/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 to protect data.

- ◆ Change your 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/bills.
- ◆ Do not give out your financial account passwords and PIN numbers.

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 to you. Instead, call the number listed in the telephone book.

Others:

- ◆ Stop telemarketing solicitations.
1-888-382-1222
www.donotcall.gov
- ◆ Stop mail and e-mail solicitations.
www.dmaconsumers.org
(Click on Customer Assistance.)
- ◆ 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