If you become a Victim:

1. Place a 1 year 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 equifax.com
Experian	☎ 1-888-397-3742 experian.com/fraud
TransUnion	☎ 1-800-680-7289 transunion.com

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

3. File a report or a misc. pub. with the police department to help you with creditors who may want proof of the crime.

Hawaii Police	☎ (808) 935-3311
Honolulu Police	☎ (808) 529-3111
Kauai Police	☎ (808) 241-1711
Maui Police	☎ (808) 244-6400

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

5. File a complaint with the Federal Trade Commission (FTC) and complete the Identity Theft Complaint Form and Identity Theft Affidavit.

Federal Trade Commission	☎ 1-877-438-4338 ftc.gov

HAWAII IDENTITY THEFT RESOURCES

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

BBB Northwest - Pacific
☎ Fraud Hotline (808) 628-3950
bbb.org/hawaii/

Department of the Prosecuting Attorney - Honolulu
☎ (808) 547-7400 or toll free 1-800-531-5538
honoluluprosecutor.org

Department of the Prosecuting Attorney - Maui
☎ (808) 270-7777
mauicounty.gov/123/Prosecuting-Attorney

Office of the Prosecuting Attorney - Hawaii
☎ East Hawaii Unit: (808) 964-3306
☎ West Hawaii Unit: (808) 322-2552
hawaiicounty.gov/pa-victims-witnesses

Office of the Prosecuting Attorney - Kauai
☎ (808) 241-1888
kauai.gov/ProsecutingAttorney

STATE OF HAWAII

Department of the Attorney General
ag.hawaii.gov

Department of Commerce & Consumer Affairs
☎ (808) 586-2653
cca.hawaii.gov

Department of Health
Senior Medicare Patrol (SMP) Hawaii
☎ (808) 586-7281 or toll free 1-800-296-9422
smphawaii.org

FEDERAL

Federal Bureau of Investigation - Honolulu
☎ (808) 566-4300

United States Postal Service
☎ (808) 423-3790

United States Secret Service
☎ (808) 541-1912

Your Identity is Your Kuleana

(Responsibility)

Department of the Attorney General
Crime Prevention & Justice Assistance (CPJA) Division

ag.hawaii.gov

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:

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

How do Scammers Access Your Personal Information?

- **Dumpster diving**
- **Frauds or scams**
- **Hacking**
- **Lost wallets, cell phone, etc.**
- **Phishing**
- **Shoulder surfing**
- **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
- It can take years to rebuild good credit

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

- Authorize money transfer from your bank account
- Obtain an official identification card
- Open new credit card
- Establish a cell phone service

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 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.

Other Prevention Resources

National Do Not Call Registry
Stop telemarketing solicitations.
☎ 1-888-382-1222 💻 donotcall.gov

Direct Marketing Association
Stop mail and e-mail solicitations.
💻 www.dmaconsumers.org

Opt Out Services LLC
Opt out of pre-approved credit card offers.
☎ 1-888-597-8688 💻 optoutprescreen.com

Central Source LLC
Obtain a free credit report to review.
☎ 1-877-322-8228 💻 annualcreditreport.com