

## Identity Theft Victims: *Immediate Steps*

**FILE A REPORT WITH ALL THREE MAJOR CREDIT BUREAUS.** Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen. Ask that a "fraud alert" be placed in your file.

- Trans Union - Phone: 800-680-7289 P.O. Box 1000, Chester, PA 19016-1000.
- Experian (formerly TRW) - Phone: 888-EXPERIAN (888-397-3742) P.O. Box 9532, Allen, TX 75013.
- Equifax - Phone: 800-525-6285 P.O. Box 105069, Atlanta, GA 30348.

**FILE A POLICE REPORT.** Get a copy of the police report and retain it for your records. Credit card companies and financial institutions may require you to show a copy of this report to verify the crime. Keep the phone number of your investigator and provide it to creditors and others who require verification of your case.

**CONTACT ALL CREDITORS.** For any accounts that have been fraudulently accessed or opened, contact the billing inquiries and security departments of the appropriate creditors or financial institutions. Close these accounts. Ask that old accounts be processed as "account closed at consumer's request." Ask that lost or stolen credit card accounts be processed as "credit card lost or stolen". Carefully monitor your mail and credit card bills and report immediately any new fraudulent activity to credit grantors.

**OBTAIN A FREE COPY OF YOUR CREDIT REPORT.** As a victim of identity theft, you may obtain a free copy of your credit report. 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.

**CONTEST BILLS THAT RESULT FROM IDENTITY THEFT.** Consumer and privacy advocates suggest not paying any portion of a bill which is a result of identity theft and not filing for bankruptcy. This will involve disputing credit card charges with the card company by writing to the address for "billing error" disputes - not the bill payment address. You should follow the directions given by the credit card company for disputing charges. This information must be provided by the company.

**NOTIFY THE DEPARTMENT OF MOTOR VEHICLES OF MISUSE OF DRIVER'S LICENSE NUMBER.** You may need to change your driver's license number if someone is using yours as identification on bad checks. Call the DMV to see if another license was issued in your name.

**REPORT STOLEN CHECKS.** If you have had checks stolen or bank accounts set up fraudulently, report it to the appropriate check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses. To report fraudulent use of your checks:

- CheckRite: (800) 766-2748
- Chexsystems: (800) 428-9623
- TeleCheck: (800) 710-9898

### STOP UNSOLICITED MAILINGS

**Opt out of pre-approved credit card offers**

- [www.optoutprescreen.com](http://www.optoutprescreen.com) (888) 567-8688

**Opt out of direct marketing solicitations**

- [www.dmaconsumers.org/consumerassistance.html](http://www.dmaconsumers.org/consumerassistance.html)

**REPORT STOLEN ATM CARDS.** Get a new ATM card, account number and password. You may be liable if fraud is not reported quickly.

**FOR FRAUDULENT CHANGE OF ADDRESS, NOTIFY LOCAL POSTAL INSPECTOR.** Call the U.S. Post Office to obtain the phone number. 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. [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect)

**REPORT MISUSE OF SOCIAL SECURITY NUMBER.** 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. If you fit specific fraud victim criteria, the Social Security Administration may change your Social Security Number.

### DEPARTMENT OF THE PROSECUTING ATTORNEY

1060 Richards St.  
Honolulu, HI 96813  
Phone: 808-547-7400  
[www.honolulu.gov/prosecuting](http://www.honolulu.gov/prosecuting)



## DEPARTMENT OF THE PROSECUTING ATTORNEY



## IDENTITY THEFT

### Protecting Your Good Name



## WHAT IS IDENTITY THEFT?

Under Hawaii law, a person commits the offense of Identity Theft if he/she uses the personal information of another person with the intent to commit theft. A person commits the related offense of Unauthorized Possession of Confidential Personal Information if he/she possesses, without authorization, the confidential personal information of another. The potential penalties for these two crimes range from 5-20 years in prison.

## HOW IDENTITY THEFT OCCURS

Here are a just a few examples of how skilled identity thieves obtain access to your personal information:

**Mail Theft** – they may steal your mail, including bank and credit card statements, “pre-approved” credit card offers, new checks, tax information, and personal checks that you place in your mail box.

**Theft Of Your Personal Property** – they may steal your wallet or purse, or any personal information that they find in your car, home, or place of business.

**“Dumpster Diving”** – they may rummage through your trash, the trash of businesses, or public trash dumpsters.

**“Shoulder Surfing”** – they may look over your shoulder as you enter your PIN number at an ATM machine.

**“Skimming”** – employees at restaurants or retail establishments may “skim” or “swipe” your credit card through a small handheld electronic device known as a “skimmer”. The “skimmer” will capture your credit card number from the magnetic strip on the back of the card.

**“Phishing”** – they may send you an e-mail message that appears to be coming from a legitimate business, such as a financial institution. The e-mail will claim that there is a problem with your account and that it will be closed unless you immediately respond by providing them with your personal information.

**Data Theft** - they may access your personal or work computer, or the computer system of a business or government agency and steal your personal information.

**Once an identity thief obtains your personal information, they may use it to commit fraud or theft. For example:**

**Fake ID Card** – they may obtain identification, such as a driver’s license, issued in your name but with their picture on it.

**Forgery** – they may forge your signature on checks, credit card slips, or bank withdrawal slips.

**Bank Account** – they may open a new bank account in your name and write bad checks.

**Credit Card** – they may open a new credit card account in your name. When they use the card and don’t pay the bill, the delinquent account is reported on your credit report.

**Loan** – they may take out a loan in your name.

**Change Of Billing Address** – they may call your credit card issuer and change the billing address on your account. It may be some time before you realize that charges are being run up on your account.

**Phone Service** – they may open up a phone or wireless service plan in your name.

**Police Contacts** – they may give the police your personal information during a traffic citation or an arrest. When they fail to show up in court, a warrant for arrest is issued in your name.

## HOW CAN YOU TELL IF YOU ARE A VICTIM OF IDENTITY THEFT?

- You stop receiving bills, financial statements, or other mail.
- Your bills or financial statements contain unexplained charges or withdrawals.
- You receive a credit card for which you did not apply.
- You are denied credit for no apparent reason.
- You receive calls from debt collectors or companies about merchandise or services that you did not buy.

## PREVENTING IDENTITY THEFT

- Be careful about giving out your personal information to others unless you have a good reason to trust them.
- Never give out your personal information over the phone, through the mail, or on the Internet unless you initiated the contact and trust the person or company that you are dealing with.
- Your wallet or purse should NOT contain any of the following: passwords, PIN numbers, account numbers, your social security card, or your mother’s maiden name.
- Monitor the balances of your accounts. Look for unexplained charges or withdrawals.
- Shred “pre-approved” credit card applications, credit card receipts, bills, and other financial information that you don’t want before discarding them in the trash or recycling bin.
- Order a free copy of your credit report once a year to check for fraudulent activity or other discrepancies.
- Promptly remove mail from your mailbox after delivery. Deposit outgoing mail in post office collection boxes or at your local post office.
- Beware of mail or telephone solicitations that are disguised as promotions offering instant prizes or awards designed solely to obtain your personal information.
- If you use a computer, keep your anti-virus software updated. Do not open files or e-mail attachments from strangers. Do not click on hyperlinks or download programs from people or companies that you don’t know. Use a firewall to block unauthorized access to your computer. Beware of “phishing” scams.