

A light green silhouette of the Hawaiian Islands is positioned at the top of the page, partially overlapping the title text.

Hawaii's

**FRAUD PREVENTION
& RESOURCE GUIDE**



How to keep your money and your information safe from fraud.



LETTER FROM GOVERNOR LINDA LINGLE

Hawaii's Fraud Prevention & Resource Guide

Aloha! I'm pleased to introduce the first-ever Hawaii's Fraud Prevention & Resource Guide, designed to help residents protect themselves and their families against fraud.

Since coming into office, our Administration has taken a proactive approach to preventing fraud. The state agencies that collaborated in assembling this guide, including the Executive Office on Aging, the Department of Commerce and Consumer Affairs and the Department of the Attorney General, work tirelessly to empower residents with information and resources to fight several different types of fraud, from identity theft, to internet fraud, to tax fraud, to securities fraud, to healthcare fraud. These efforts include education awareness campaigns, counseling and enforcement.

In 2007, I signed three bills into law that help protect Hawaii's senior citizens from financial abuse and fraud. One law requires financial institutions in Hawaii to report any suspected financial abuse committed against a senior citizen. The two other laws stiffen penalties for securities fraud and violations by mortgage brokers committed against kupuna.

This guide builds on these initiatives and legislation, providing residents with helpful information that includes valuable tips on how to protect against fraud, what to do if you are a victim of fraud, a special section for our kupuna, and a directory of important contacts.

I want to thank the state agencies that worked together to develop this important book, which is one of the first comprehensive state guides in the nation with the primary purpose of helping the public fight fraud. Our goal is to ensure that our residents do not fall victim to the scams of unscrupulous individuals. We believe that the more information residents have, the better protected they will be.

Mahalo nui loa,

Linda Lingle
Governor of the State of Hawaii

This guide is provided by the State of Hawaii, Executive Office on Aging, SMP Hawaii Program, formerly known as SageWatch; Department of Commerce and Consumer Affairs, Office of the Securities Commissioner; and Department of the Attorney General, Crime Prevention and Justice Assistance Division.

Primary funding for this guide is provided by the State of Hawaii, Executive Office on Aging, SMP Hawaii Program, formerly known as SageWatch; with additional funding provided by the Department of Commerce and Consumer Affairs, Office of the Securities Commissioner.

The information provided in this guide is for general informational purposes only, and may not be applicable to every situation. The information presented here is not intended to set any standards, nor is it to be taken as, nor should it replace, legal counsel. Although some of the information contained herein is about legal issues, this guide is not and should not be treated as legal advice. Due to the ever-changing nature of the law, the public should seek timely legal advice from counsel, based on current law, prior to taking any action based upon information contained in this guide.

This Resource Guide was supported, in part by a grant from the U.S. Department of Health and Human Services, Administration on Aging. Grantees undertaking projects under government sponsorship are encouraged to express freely their findings and conclusions. Points of view or opinions do not, therefore, necessarily represent official Administration on Aging policy.

©2008 State of Hawaii, Executive Office on Aging, Department of Commerce and Consumer Affairs, and Department of the Attorney General.

For more information about reprint permission, contact the Executive Office on Aging, 808-586-0100 (phone), www4.hawaii.gov/lea (website).

May 2008

CONTENTS

INTRODUCTION	8
1 Ways We Get Scammed: Methods	10
Internet	11
Mail	12
Marketing	14
Person-to-Person	15
Phone	16
2 Ways We Get Scammed: Advance Fee Fraud	19
Charity Fraud.....	21
Construction and Home Repair Fraud	23
Inheritance Scam	26
Lottery Scam	27
Foreign Money Transfer Scam.....	29
On-Line Auction Overpayment and Fake Check	30
Rental Scam	32
Where to Get Help	34
3 Ways We Get Scammed: Financial Fraud	36
Credit Card Fraud	37
Insurance Fraud	38
Investment Fraud	40
Common Types of Investment Scams	
Ponzi.....	41
Pyramid.....	42
Loan Scams	43
Blank Documents	43

Caretakers: Family, Friends, and Professionals.....	43
Deed Forgeries	43
Foreclosure Consultants.....	43
Home Equity Loan and Predatory Lending	43
Home Repair	44
Fly-By-Night Lenders	44
Refinancing Scams	44
Reverse Mortgage Fraud.....	44
Where to Get Help	46
4 Ways We Get Scammed: Healthcare Fraud	48
The Five Main Types of Healthcare Fraud	49
Billing for Non-Covered Services.....	49
Billing for Non-Rendered Services.....	49
Offering Money or Gifts in Exchange for Medical Services..	49
Unbundling.....	49
Up-coding	49
Where to Get Help	52
5 Ways We Get Scammed: Phishing	54
Internet Phishing	55
Link Manipulation	55
Phone Phishing.....	56
Website Forgery	57
Where to Get Help	58
6 Protecting Hawaii’s Seniors (Our Kupuna)	59
Senior Fraud Squad — Be A Volunteer.....	61
Talking Story with Our Kupuna About Scams.....	62
Tips for Our Kupuna	72
Where to Get Help	73

7	Prevention Tips: How to Be a Safe Consumer	75
	Auction/On-line Purchases	76
	Computer/Internet	78
	Finances	84
	Mail	85
	Phone	86
8	If You Are a Victim: Steps to Recovery	87
	Victim Journal Log.....	88
	Where to Get Help:	
	EQUIFAX—How to Place a Fraud Alert by Phone	89
	Where to Get Help:	
	EXPERIAN—How to Place a Fraud Alert by Phone	90
	Where to Get Help:	
	TRANSUNION—How to Place a Fraud Alert by Phone	91
	How to Obtain a Free Credit Report.....	94
	Sample Letters to Help You with Recovery	95
	Credit Bureau	96
	Creditor of a New Account	
	Opened Fraudulently in Your Name	97
	Creditor of an Existing Credit or Debit Account	
	Used Fraudulently	98
	DCCA Securities Enforcement Complaint Form	99
9	Directory of Resources	103
	GLOSSARY	131



INTRODUCTION

SURF, SUN, AND SAND: TYPICAL POSTCARD IMAGES OF HAWAII.

The scenic beauty of our state is matched only by its people, known for their warmth, generosity, and aloha. However, under the surface of this picturesque scene, fraud is a threat to our state.

Sadly, many of Hawaii's citizens fall victim to consumer and financial fraud — including identity theft — every year. Victims of financial and consumer fraud are not limited to a specific ethnicity, gender, or age group.

The State of Hawaii, Executive Office on Aging, SMP Hawaii Program, formerly known as SageWatch; Department of Commerce and Consumer Affairs, Office of the Securities Commissioner; and Department of the Attorney General, Crime Prevention and Justice Assistance Division are pleased to provide you with this booklet, *Hawaii's Fraud Prevention and Resource Guide*.

This guide was developed to educate consumers about the most common methods used to fraudulently obtain their personal information and money. This guide will provide you with information on consumer and financial fraud, prevention tips to avoid becoming a victim of fraud, steps to recovery if you have been victimized, and a resource directory.

Please take the time to read this guide and protect yourself from becoming a victim of consumer and financial fraud.

Ways We Get Scammed

METHODS



THE FOLLOWING SECTION will focus on the ways we are approached by scammers in our daily lives.

There are five main ways we may be scammed. It may be one or several of these methods in combination: Internet, mail, marketing, person-to-person, or phone.



Internet

Modern technology, especially the increased use of a personal computer and access to the Internet, has its advantages and disadvantages. It can improve our quality of life, but it can also put us at risk physically and/or financially.

An identity thief can retrieve sensitive information over an unsecured transmission or by installing software on your computer that will automatically collect and transmit sensitive information, which can ruin your credit and cause havoc in your life.



HELPFUL TIPS FOR STAYING SAFE FROM INTERNET SCAMS

- Remember, what you see is not always what you get. Don't believe anything — scrutinize everything. Do your research *before* you react to the information you are viewing, whether it's from an e-mail or a website.
- Install anti-virus and anti-spyware software, and keep current with updates.
- Use a firewall. Sharing a single Internet connection involves using a router. These routers are not secured when you connect them to your computer. You will need to read the manual to learn how to prevent your information from being compromised over the Internet.
- There is no such thing as being completely safe and secure. If you are not familiar with computers, seek professional help to understand the risks before using technology you are not familiar with. If you have questions, ask a professional, such as a computer technician, to help you.



Mail

People receive and send mail on a daily basis, and our mail contains information that identity thieves want to obtain. For example, bank statements, utility bills, credit card bills, credit card offers, and blank checks contain account information that the thief could use to assume your identity or to gain access to your money. The methods identity thieves employ to steal mail are not sophisticated. Mail thieves target neighborhoods by observing the time mail is delivered, the presence or absence of residents at a particular time, and the little red flags raised on mailboxes that indicate outgoing mail.



HELPFUL TIPS FOR STAYING SAFE FROM MAIL SCAMS

- Place all outgoing mail into a secure, locked post office box.
- Install a locking mailbox for incoming mail or promptly remove incoming mail after delivery.
- If traveling, contact your local post office to hold your mail or have someone you trust retrieve your mail.
- Shred mail with your personal information.
- Monitor your monthly bills and financial statements. Contact the companies if you are missing your monthly bills or financial statements.

To stop receiving junk mail, you may send a postcard or letter with your name, home address, and signature to:

Mail Preference Service
Direct Marketing Association
P.O. Box 643
Carmel, NY 15012-0643

Registering with Mail Preference Service places your name and address on a “do-not-mail” list.

The Better Business Bureau advises that you consider the following to reduce the amount of mail you receive:

- Putting your name into a free drawing box at trade shows or other events may generate more mail. Before dropping your name into the drawing box, ask what happens to your completed entry blank after the winner is announced.
- When completing surveys/warranty slips that are included with your purchases, your information may be sold as marketing/sales leads lists.
- Purchasing a national magazine subscription may be cheaper per issue than purchasing off the rack; however, your information may be sold to subsidize the cost of the subscription.
- Call companies directly to remove your name from their mailing lists.



Marketing

Scammers use false advertisements, misleading information or free meals or goods to attract people to visit their store or buy their products or services. These advertisements are usually seen or heard on the radio, television, print, or the Internet. It is important to know that those who make and sell products must honestly present their products, services, and prices to the consumer.



HELPFUL TIPS FOR STAYING SAFE FROM MARKETING MEDIA SCAMS

- Do your homework and research the company before getting involved. Find out if the company is legitimate.
- Do your research on the salesperson. Be certain he or she is registered or licensed to sell the product or service.
- Don't let pitches, glossy marketing materials, and free meals lure you into a scam.



Person-to-Person

Person-to-person fraud is any face-to-face interaction with a scammer who uses dishonest methods to sell fraudulent products or services. For example, scammers use their communication skills to gain trust.

A person-to-person fraud is a one-on-one meeting or a seminar that involves props, fake documents, or the inappropriate solicitation of others to endorse or invest in the scam.



HELPFUL TIPS FOR STAYING SAFE FROM PERSON-TO-PERSON SCAMMERS


- Give yourself time to research the person and the company before you invest.
- Check for license or registration:
No License,
No Deal.
- Remember —
“If it sounds too good to be true,
it probably is.”





Phone

Scammers, like identity thieves, also use the phone to solicit personal information from their victims. The target victim could be prompted by a telephone message to call a customer support number, where the scammer or an audio response unit waits to take an account number, personal identification number, password, or other valuable personal data. The scammer may also claim that the victim's financial account will be closed or other problems could occur if the victim does not respond immediately. Scammers often use pay phones, stolen cellular phone numbers, or hacked accounts.



Hello. We have an important message regarding your mortgage loan. Please make sure to call us at 800-555-5555 right away...



HELPFUL TIPS FOR STAYING SAFE FROM PHONE SCAMS

- Do not give any personal information over the phone unless you initiated the call and are certain of who you contacted.
- If you are not sure who is on the other end of the phone, say, "please send me the information and I'll get back to you."
- If the caller makes you feel uncomfortable, hang up the phone.

ONE COMMON PHONE SCAM: Sweepstakes and Other Prizes Winner

If you receive a phone call informing you that you won money, a prize, or a trip in a contest you entered, you need to be cautious. While many contests are legitimate, some are not. Prizes in legitimate contests are awarded by chance, and contestants do not have to pay a fee or buy anything to enter or increase their odds of winning.



KEEP IN MIND...

The next time you receive a phone call about being a winner in a contest, remember the following:

- Legitimate sweepstakes don't require you to pay or buy something to enter.
- Sponsors of legitimate contests identify themselves prominently; fraudulent promoters downplay their identities.
- Legitimate offers clearly disclose terms and conditions of the contest.
- If notified by mail, check the postmark on the envelope. If it was sent as bulk rate, it is unlikely that you've won a big prize.
- Do not send any check or money order by overnight delivery or courier to claim your prize.
- Don't be deceived by endorsements from a well-known celebrity that fraudulent promoters may use to elicit confidence in their offer.
- Read the material carefully and pay close attention to the fine print.
- Be skeptical when asked to attend a sales meeting to win a prize.

- By signing up for a contest at a trade show or similar event, you run the risk of having your personal information sold or shared with telemarketers.
- Beware of promoters using toll-free 800 numbers that direct you to pay-per-call 900 numbers.
- Do not give your checking, credit card, or other bank account information over the phone in response to a sweepstakes promotion.
- Call the Better Business Bureau on Oahu at (808) 536-6956 or toll-free at 1-877-222-6551 to receive a report on the company.



WARNING FLAGS! SIGNS OF A POTENTIAL FRAUD

- It sounds too good to be true.
- It is urgent. You must act now!
- You are pressured — repeated phone calls, mail, and e-mails.
- You are asked to give your bank or credit card account number or other personal information.



Ways We Get Scammed

ADVANCE FEE FRAUD

ADVANCE FEE FRAUD IS A SCAM that involves advance payment from the victim to the scammer. It is also known as a confidence trick, in which the target or victim is persuaded to send in advance small sums of money in the hope of realizing a much larger gain.



WARNING FLAGS! SIGNS OF A POTENTIAL FRAUD

- You do not know the person who has sent you the message.
- You are promised huge sums of money for little or no effort on your part.
- You are asked to provide money up front for questionable activities, a processing fee, or the cost of expediting the process.
- You are asked to provide your bank account number or other personal financial information, presumably to allow the sender to deposit money into it.
- The request contains a sense of urgency.
- The sender repeatedly requests confidentiality.
- The sender offers to send you photocopies of government certificates, banking information, or other “evidence” that their activity is legitimate (though the materials are forged).

THEMES AND VARIATIONS

Advance Fee Frauds tend to have some or all of the following characteristics: the proposals are unsolicited, emphasize the urgency and confidentiality of the deal, and require the victim to pay various government and legal fees and taxes for the promise of returns that turn out to be non-existent.

While these can all fall under Advance Fee Fraud, at times the same characteristics may amount to outright fraud.



Charity Fraud

Charity fraud is committed when a perpetrator creates a bogus fundraising operation by taking advantage of disasters, such as Hurricane Katrina, or creates a fictitious charity in order to take advantage of goodwill donations. Charity fraud may also occur when a legitimate charity represents that funds will be used for purpose “X” but the money is used for other purposes. There are many good causes, so don’t let fraud dissuade you from giving to charities. These tips will help ensure that your donations are put to good use.



HELPFUL TIPS FOR STAYING SAFE FROM CHARITY FRAUD

- Make sure you understand which organization wants your money. For example, police departments do not solicit money over the phone; police unions do. Also, some charities have names that may sound confusingly similar to another charity’s name.
- Ask how your donation will be used. Make the caller be specific. If the answer is vague, be wary. You should be satisfied that your donation will support programs you think are worthwhile.
- Ask where your donation will be used, especially if you prefer your donation to be used locally.
- Ask who you are talking to. Get the name and write it down. If called by a police union, don’t be fooled into thinking you are talking to a police officer.
- If it is important to you, ask the caller if he or she is being paid to make the call.
- If it is important to you, ask what percentage of your donation goes to

the organization. There is no certain amount that is good or bad; it is up to you to decide your level of comfort. Financial reports for charities, filed with the Attorney General's office by paid solicitors, indicate the percentage of donations that actually go to the charity. These reports are available on the Internet at www.hawaii.gov/ag/charities/quicklinks/financial_reports.

- Never agree to donate over the phone. Always ask for written information. But be careful; just because an organization sends you information doesn't mean you should automatically be comfortable with it. Read the material thoroughly. Does the organization clearly tell you what it does and precisely how it will spend your donation?
- Always donate by check, never with cash.
- Check for fund-raising reports on the charity on the Attorney General's website and with charity watchdogs such as:
 - The American Institute of Philanthropy (www.charitywatch.org)
 - Better Business Bureau's Wise Giving Alliance (www.give.org)

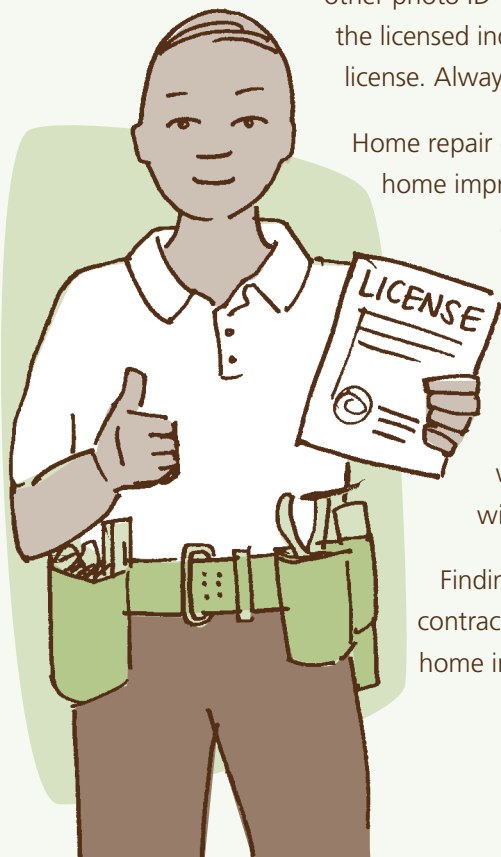


Construction and Home Repair Fraud

Construction fraud con artists lure you into doing major construction or home renovation (e.g., fix your roof, remove walls). In most cases, the scammer will take your deposit, do a portion of the job, and leave without finishing.

Hawaii requires contractors to be licensed with the Department of Commerce and Consumer Affairs. Call (808) 587-3222 on Oahu or use the on-line services at www.hawaii.gov/dcca/pvl to find out if a contractor is licensed and whether he or she has been named in any prior complaints.

Ask for the contractor's license number. If the contractor shows you a document with a license number on it, ask to see a driver's license or other photo ID that proves the contractor is really the licensed individual or employee named on the license. Always hire a licensed contractor!



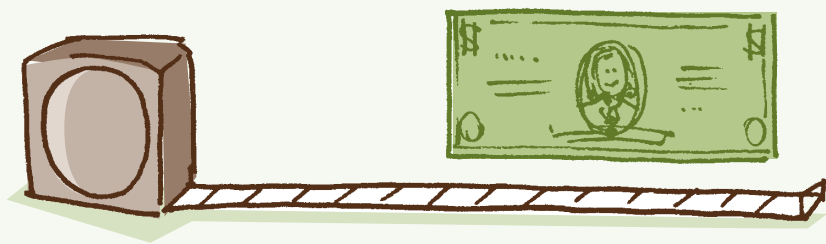
Home repair con artists have emerged in the home improvement industry, offering to do an expensive job for an unusually low price. Free inspections by these con artists often lead to recommendations for expensive and unneeded repairs. Some even offer to do the work on the spot. However, when they leave, victims may be left with a large bill and a faulty repair job.

Finding a licensed, competent, and reliable contractor is the first step to a successful home improvement project.



CHECKLIST: HOW TO CHOOSE A CONTRACTOR

- Ask friends, neighbors, and relatives for referrals. Contact trade associations or contractor associations for names of members.
- Ask the contractor for customer references who have projects that are similar to yours.
- Check with the State Consumer Resource Center for current and appropriate contractor's license and complaint history.
- Get a Better Business Bureau report on the company.
- Get at least three written estimates for the project. Make sure bids are based on identical project specifications.
- Get all guarantees, warranties, and promises in writing. Read the entire contract and make sure you understand all terms and conditions. If it's hard for you to understand the contract, ask a friend or family member to help you go through the contract with the contractor. Ask questions.
- Agree on a start and end date and have it written into the contract.
- Agree upon who will be responsible for obtaining the building permit.
- Work with your contractor on a payment schedule and include it in the written contract. We recommend that you do not pay for the entire project up front.
- Let your neighbors know that you are having work done on your home and ask them to keep an eye out for any suspicious activity.



HELPFUL TIPS: ONCE YOU'VE CHOSEN A CONTRACTOR

- Read everything before you sign.
- Include every promise and detail, start date, materials, schedule, prices, and styles in the contract.
- Oral promises are difficult to prove later; get all agreements in writing.
- Never sign a blank contract.
- You must be provided with warranty information before the purchase.
- Keep a copy of the contract so you can prove what was in the original agreement.
- Make sure you have a copy of documentation explaining how and when you have a right to cancel the agreement.
- Inspect the finished product before you pay, and never pay in cash.
- Get a written contract. Be sure to read it and be sure that you understand it before you sign it. Any contract is a legally binding agreement that describes the obligations of the signers.



Inheritance Scam

Scammers create mass mailings that describe how a fictional individual—with the same last name as the recipient—died without heirs in urban and remote parts of the world. If the recipient replies to the e-mail, the scammer will attempt to convince the recipient to send money to pay for legal fees, bribes, or other expenses. The scammer may also attempt to obtain copies of the recipient's personal information, identification cards, financial account information, and other information, which can be used to forge bank drafts, empty the recipient's bank account, obtain credit under the recipient's name, or commit identity theft.





Lottery Scam

A typical lottery scam begins with an unexpected notification through e-mail, postal mail, or fax that claims you have won a large sum of money in a lottery. The target of the scam is usually directed to keep the notice confidential and to contact a “claims agent.” After contacting the agent, the target of the scam will be asked to pay “processing fees” or “transfer charges” so that the winnings can be distributed. The victim never receives any lottery payment. Many e-mail lottery scams illegally use the names of legitimate lottery organizations.

According to the U.S. Postal Inspection Service, thousands of U.S. citizens have lost millions of dollars to fraudulent foreign lottery scams. Beware of solicitation by phone, mail, fax, or e-mail asking you to participate in a lottery in Canada, Spain or other foreign countries. Avoid soliciting companies that offer convenient purchase of lottery tickets, with promises of unbelievable odds and high winnings.



HELPFUL TIPS FOR AVOIDING LOTTERY SCAMS

- Purchasing foreign lotteries are illegal. United States law prohibits mailing payments to purchase any ticket, share, or chance in a foreign lottery.
- Most foreign lottery solicitations sent to addresses in the United States do not come from foreign government agencies or licensees. They come from fraudulent companies that seek exorbitant fees from those wishing to play.
- Those who pay the required fees never see any lottery tickets or any other evidence that lottery tickets were purchased on their behalf.
- In some cases, the soliciting company uses high-pressure telemarketing techniques to obtain credit card account numbers. Once credit card

numbers have been obtained, repeated unauthorized transactions are made on the accounts.

- Call the Better Business Bureau on Oahu at (808) 536-6956 or toll-free at 1-877-222-6551 for more information.

INTERNATIONAL LOTTO COMMISSION



----- WINNING NOTIFICATION -----

We happily announce to you the draw of the LA PRIMITIVA LOTTERY PROMOTIONS PROGRAM held on the 27th of September, 2007. Your e-mail address attached to ticket number: 564 75600545188 with Serial number 5368/02 drew the lucky numbers: 19-6-26-17-35-7, which subsequently won you the lottery.

You have therefore been approved to claim a total sum of US\$2,500,000.00 (Two million, Five Hundred Thousand United States Dollars) in cash credited to file ktu/9023118308/03. Congratulations!

Due to false practices, you are advised to keep your winning information CONFIDENTIAL until your claim is processed and your money remitted to you in whatever manner you deem fit to claim your prize.

To begin your lottery claim, please fill and fax the payment processing form with a copy of your identity (international passport, driver's license, etc.) to your agent's company, and contact your claims agent immediately for further direction on administrative requirement needed to release your funds.

GLORIA SCAMA



VICE PRESIDENT, LOTTERY BOARD



Foreign Money Transfer Scam Also Known As the Nigerian Letter Scam

A Foreign Money Transfer scam combines the threat of impersonation fraud with a variation of an Advance Fee Fraud, in which an e-mail or letter mailed from a foreign country offers the recipient the “opportunity” to share in a percentage of millions of dollars that the scammer, a self-proclaimed government official, royal, or business executive, is trying to transfer illegally out of the foreign country.

Many good people have fallen for this scam that was popularized by scams originating from Nigeria. Once they become involved, they are fearful of having illegally assisted the scammer. If this has happened to you, don’t let fear prevent you from taking steps to protect yourself once your information has been compromised.

Reply Forward Delete

From: r_okam@0000/nigeriagov.net
Subject: Request for Urgent Business Relationship

WE ARE TOP OFFICIALS OF THE FEDERAL GOVERNMENT CONTRACT REVIEW PANEL WHO ARE INTERESTED IN IMPORTATION OF GOODS INTO OUR COUNTRY WITH FUNDS WHICH ARE PRESENTLY TRAPPED IN NIGERIA. IN ORDER TO COMMENCE THIS BUSINESS WE SOLICIT YOUR ASSISTANCE TO ENABLE US TO TRANSFER INTO YOUR ACCOUNT THE SAID TRAPPED FUNDS...



HELPFUL TIPS FOR AVOIDING FOREIGN MONEY TRANSFER SCAMS

- If you get an e-mail like this, delete it. Do not reply.
- Be careful when a letter states “Confidential” or “Top Secret,” because it could be a sign of a scam.
- Do not provide your personal information.



On-Line Auction Overpayment and Fake Check

An on-line/Internet auction overpayment is a scam in which the scammer offers to buy items or a service from a legitimate website (e.g., eBay, Bidz, etc.). The scammer sends an official, certified bank check, a cashier's check, postal money orders, travelers checks, or a check drawn on a business account that has an "accidentally" or mutually agreed-upon overpayment, greater than the price of the item. To retrieve the overpayment, the scammer asks the seller to deposit the check(s) and wire the overpayment amount before the initial check is cleared. By the time the initial check is presented to the paying bank and determined to be fraudulent, you've already wired the overpayment. The check is then returned to the bank of first deposit and charged back to the seller. The seller/depositor is responsible for the full amount of the check.

On-line auction houses are go-betweens for would-be buyers and sellers. Before you bid, find out how it works. The Federal Trade Commission and the Better Business Bureau offer more information and you should verify the reputation and transaction history of auction houses with them.

EXAMPLES OF ON-LINE AUCTION SCAMS

On-line auction scams involve the appeal of high-value goods that the seller advertises at low cost. The text of the ad instructs buyers to contact the seller directly, outside of the website, at a Yahoo or Hotmail type of account. When contact is made, the seller provides a story about his problems receiving payment via third party payment service, such as money orders. The allure is that the product is priced well below market value and is a great bargain, for example, a \$1,000 item may be advertised for \$500. If the money is sent, it is gone forever and no product is delivered.



HELPFUL TIPS FOR SAFE ON-LINE AUCTIONING

- Always inform your bank that the check is from someone you do not know before you deposit it to your account.
- Never wire money from overpaid checks.
- Do not send merchandise until you are certain the check has cleared. This may take months and problems may arise after your bank has credited the funds.
- Do not wire money to anyone unless you know exactly where the money is going.
- Avoid doing business with anyone who wants to operate outside of a monitored website.
- Check history, seller and buyer ratings before making a purchase.
- Identify the seller and check their reputation with the Better Business Bureau.
- Check the seller's reputation and transaction history.
- Avoid impulse bids and purchases. Do your homework. Know what you're bidding on, its value, and all terms and conditions of the sale.
- Ask about the seller's return policy. Who pays for shipping and handling, or costs on a returned item?
- Evaluate the different payment options such as credit card, escrow services, or C.O.D.
- Be cautious if the seller insists on payment by check or money order.
- Ask the seller about servicing the product after the purchase.



Rental Scam

There are three general types of rental scams — fake landlord, fake tenant, and fake vacation rentals.

FAKE LANDLORD

A scammer advertising a high-standard rental for a low cost victimizes a prospective tenant looking for an accommodation. The victim is required to pay a deposit, but the scammer disappears once he has received it, leaving the victim without a rental and the money deposited.

FAKE TENANT

The victim, an innocent landlord, is looking to find a tenant for an accommodation, and the scammer poses as an interested party looking to occupy a vacancy.

In one scenario, the scammer will send the landlord a check with an overpayment asking the victim to forward the extra money back to them via money order or wire transfer, before the initial check has cleared.

In a second scenario, the scammer will send the landlord a check for the deposit. The scammer will then contact the landlord with a story of a death in the family or other crisis and ask them to wire the deposit back to them as soon as possible, before the initial check has cleared.

The scam is that the initial check will never clear and you've just spent that money by wiring it. You've paid out the amount of the wire and you're not going to get any payment back.

FAKE VACATION RENTAL

In this scam, the victim is usually a non-resident who is planning to vacation in Hawaii. Typically, they will be checking postings on various websites listing vacation rentals. The properties offer idyllic beach front settings, seclusion, and easy access to sundries, grocery, and visitor attractions. The “hook” is the cost of the rental, which is low and very enticing. Of course, a security deposit is required and must be paid in advance.

When our vacationing visitor arrives, they soon discover that they have been duped. Their island retreat did exist, but was inhabited by its residents, who have no intention of renting their home nor have they authorized anyone to make such an offer.

The visitor has not only lost the money but now needs to find lodgings for his family.



HELPFUL TIPS FOR AVOIDING RENTAL SCAMS

- Always inform your bank that the check is from someone you do not know before you deposit it to your account.
- Never wire money.
- Do not refund deposits until you are certain the check has cleared.



Where to Get Help

If you or someone you know has been a victim of any of these Advance Fee Frauds, call:

BETTER BUSINESS BUREAU OF HAWAII

1132 Bishop Street, Suite 615, Honolulu, HI 96813

OAHU: (808) 536-6956 **TOLL-FREE:** 1-877-222-6551

WEBSITE: www.hawaii.bbb.org

DEPARTMENT OF COMMERCE & CONSUMER AFFAIRS (DCCA)

King Kalakaua Building, 335 Merchant Street, Honolulu, HI 96813

www.hawaii.gov/dcca

Consumer Resource Center

OAHU: (808) 587-3222 **TOLL-FREE:** 1-800-394-1902

Monday-Friday, 7:45 a.m. to 4:30 p.m. Call for license verification and complaint history of professionals or businesses, information on identity theft, and other general consumer information.

Landlord-Tenant Information Line

OAHU: (808) 586-2634

Volunteers available from Monday-Friday,
8:00 a.m. to 12:00 p.m., except state holidays.

For neighbor island toll-free numbers, see list on page 117.

Office of Consumer Protection

235 S. Beretania Street, Room 801, Honolulu, HI 96813

OAHU: (808) 586-2630 **FAX:** (808) 586-2640

For neighbor island toll-free numbers, see list on page 116.

POLICE DEPARTMENTS BY COUNTY

Hawaii County Police Department

349 Kapiolani Street, Hilo, HI 96720

HAWAII: (808) 935-3311 or 911

WEBSITE: www.hawaiipolice.com

Honolulu Police Department

801 S. Beretania Street, Honolulu, HI 96813

OAHU: (808) 529-3115 or 911

WEBSITE: www.honolulupd.org

Kauai Police Department

3990 Kaana Street, Suite 200, Lihue, HI 96766-1268

KAUAI: (808) 241-1711 or 911

WEBSITE: www.kauai.gov/Police

Maui Police Department

55 Mahalani Street, Wailuku, HI 96793

MAUI: (808) 244-6400 or 911

WEBSITE: www.co.maui.hi.us/departments/Police



NATIONALLY, BILLIONS OF DOLLARS and millions of consumers are victims of financial fraud.

In 2007, according to the Federal Trade Commission, Hawaii ranked 10th in the nation in the number of fraud complaints relative to the size of our population.

Don't be a statistic. Protect yourself from financial fraud.

The following are the many types of financial fraud and ways that you can prevent yourself from becoming victimized.



Credit Card Fraud

Credit card fraud can take two forms:

- 1) The perpetrator charges items, usually via on-line purchases, to another person's credit card account.
- 2) The seller is tricked into releasing merchandise or services to the scammer, believing that a credit card account will provide payment for goods or services. The seller later learns that the amount due will not be paid, or the payment received will be reclaimed by the credit card's issuing bank.



HELPFUL TIPS FOR AVOIDING CREDIT CARD FRAUD

- Sign your cards as soon as they arrive.
- Carry your cards separately from your wallet and keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep an eye on your card during any transaction.
- Save receipts to compare with billing statements. Destroy all receipts containing your account information once verified with your monthly statements.
- Open bills promptly and reconcile accounts monthly. Report any questionable charges promptly and in writing to the card company.
- Notify card companies in advance of a change in address.



Insurance Fraud

Dishonest insurance agents may create additional sales by asking you to purchase additional lines of insurance (automobile, homeowner's, life) with them in order to secure coverage. For example, you wish to buy a homeowner's insurance policy but the agent tells you he or she can't write your homeowner's insurance unless you let them write insurance on your car or you buy a life insurance policy from them. This practice is known as "conditional sales" or "bundling" and is illegal.

When moving retirement funds from one tax deferred plan (401ks, IRAs, etc.) to another, be alert to what products your new tax deferred plan will be funded with. Many brokers, dealers, and investment advisers are also licensed insurance agents. If they are placing your funds into an annuity or other insurance product, ask them to explain their action, cost, benefits, and drawbacks of the insurance product. Many insurance products pay a much higher commission rate than traditional mutual funds so you may be

steered to them by a broker, dealer, or financial adviser that has his or her best interest at heart rather than yours.

When a Certificate of Deposit (CD) matures, a customer service representative from the bank may suggest that you meet with a financial adviser to look into alternative ways to increase the interest you are receiving or will receive on a CD. Many consumers are encouraged to place their money into an annuity instead



of renewing their CDs. Be aware that the penalties for early withdrawals from an annuity are much higher than a CD. Also, the Federal Deposit Insurance Corporation (FDIC) does not cover annuities and life insurance products.

Insurance is an important product for the protection of our assets and quality of life. Except for a small minority, insurance agents in Hawaii are professional, ethical, and focused on taking care of your insurance needs. When involved

in any kind of financial transaction, it is always a good idea to take your time and seek out a second opinion.

No good deal will be gone tomorrow. Always ask for an explanation and copy of any documents you sign. Please direct any questions or concerns you have about insurance or insurance agents to the DCCA Insurance Division's Investigations Branch on Oahu at (808) 586-2790.





Investment Fraud

Investment fraud may include securities, commodities, Ponzi schemes, pyramid schemes, and other investments where financial advisers or salespeople persuade victims to make investments based on misleading or dishonest information. Often, the appeals of these frauds include the promise of large returns on your investment, higher-than-market interest on your capital, and a low or no-risk guarantee. It is important to remember that all investments have risk — higher returns usually involve higher risk and a greater chance of losing investors' money.

Investment scammers use high-pressure sales techniques and make their scam look legitimate. For example, some scammers may rent an office space and may have a receptionist, investment counselors, and brochures.

In Hawaii, all broker-dealers, sales agents, investment advisers, and their representatives must be registered with the Office of the Securities Commissioner (DCCA-OSC) on Oahu at (808) 587-2267. Contact the DCCA-OSC to verify the registration and clean history of any firm or individual attempting to sell investments. Always investigate before you invest, and never invest with unlicensed individuals or firms.

FAILURE TO DISCLOSE AND MISLEADING INFORMATION

Sometimes, investment fraud is done by omitting important information or misleading the consumer. For example, an investment adviser and a broker dealer must inform you accurately of material aspects of any investment they advise or recommend you to buy including fees, commissions, lock-up periods, and risk. If they mislead you to think a product like an annuity is FDIC insured but it is not, that is a securities violation.

They also have to assess the suitability of recommending something to you knowing your circumstances. If they don't properly disclose or they mislead you regarding the investment, that is a securities violation in Hawaii.



HELPFUL TIPS FOR AVOIDING INVESTMENT FRAUD

- Always understand the investment before investing. If you don't understand, don't buy.
- Ask questions, find out about commissions, fees and lock-up periods.
- Don't sign blank documents.
- If it sounds too good to be true, it is.
- You should always keep in mind whether an investment is suitable for your goals and needs.
- Check with the DCCA-OSC to see if the investment adviser, salespersons, the company, and the investment are properly registered.

PONZI SCHEMES

Ponzi schemes are named for the swindler Charles Ponzi, who took investors for millions in the early 1900's by promising 40% returns. The premise is simple: pay early investors with money taken from later investors. There is no real underlying business. The Ponzi scheme is based on the idea of "taking from Peter to pay Paul."

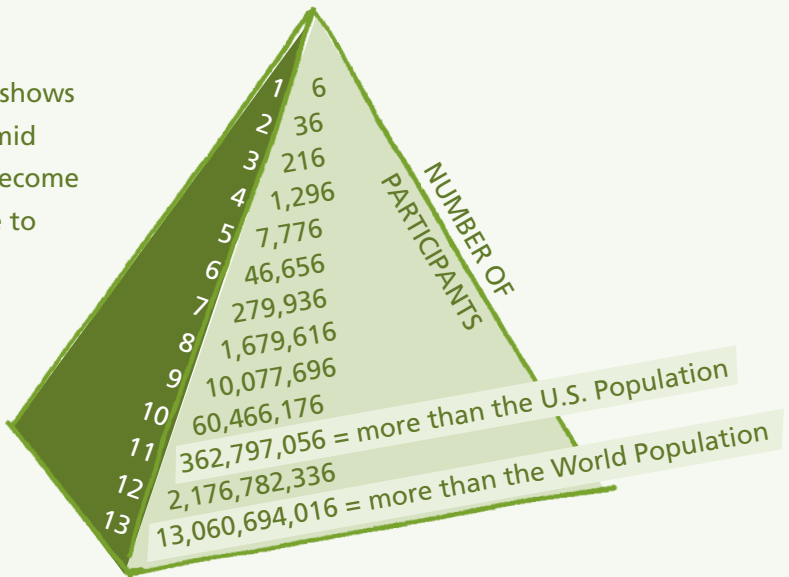
A victim may be told that he or she is making an investment with a high return. But the reality is the scammers take the victim's money and use it to pay out interest or dividends due on the principal money of earlier investors who signed up for the program. After passing a fraction of the money between victims, the scammers take the rest and leave town.

PYRAMID SCHEMES

Pyramid schemes are illegal money-making ventures that engage individuals, businesses, or small groups. A typical pyramid scheme involves a few individuals at the top who recruit participants who will, in turn, recruit more participants to offer something of value (usually money, but in some cases time) to the organization. Recruits are promised large sums of money if they successfully bring in others who will pay money to join the pyramid. For help with securities fraud, call the DCCA Office of the Securities Commissioner at (808) 586-2267.

Pyramid schemes may be disguised as games, chain letters, buying clubs, motivational companies, mail order operations, or investment organizations. Although some pyramid schemes call themselves multi-level marketing operations, not all multi-level marketing companies are pyramids. When the emphasis is on recruiting new members rather than selling something of value, the organization is probably an illegal pyramid scheme.

This chart shows
how pyramid
schemes become
impossible to
sustain:



Source: U.S. Securities and Exchange Commission, Office of Investor Education and Advocacy.



Loan Scams

Blank Documents: In this simple type of fraud, the homeowner is tricked into signing a lien document or deed transfer that has been disguised as other paperwork.

Caretakers: Family, Friends, and Professionals: Seemingly trustworthy people befriend senior homeowners, gain their trust, and have them sign over their homes or set up home equity loans that allow the “friend” to unjustly access the homeowner’s equity.

Deed Forgeries: Scam artists forge the homeowner’s signature on a blank “grant deed” in order to transfer ownership of property. With the phony deed, the scam artist can borrow against the equity in the home.

Foreclosure Consultants: Disreputable consultants may take a large fee to save a house from foreclosure and then disappear in this type of fraud. Alternatively, the consultant may convince the homeowner to sign over the deed to the property and then proceed to evict the homeowner.

Home Equity Loan and Predatory Lending: In most cases, someone who lends money secured by a borrower’s home can legally seize the home if the borrower does not make payments on time. Because of this, dishonest individuals have found ways to lure homeowners with high-rate, high-fee home loans that are impossible to repay. This is called home equity loan fraud.

In one common approach, a swindler might arrive at a victim’s door uninvited, offering to do repairs and help finance them. The swindler may talk victims into taking out a home equity loan that they cannot afford to repay and then legally obtain ownership of their house.

For example, a woman on a fixed income was persuaded to sign a loan contract that required more than \$3,000 per month in payments, although her fixed monthly income was only \$900. The lender foreclosed on the woman's home and evicted her.

Home Repair: Con artists may act as if they offer door-to-door home improvement and may recommend unneeded repairs. They further help you to arrange "easy financing" loans secured against the home that require high interest rates to cover the costs. These loans often require such a high monthly payment that failure to pay and foreclosure are almost inevitable.

Fly-By-Night Lenders: Dishonest lenders set up offices in low-income and often minority neighborhoods and convince homeowners to sign loan documents secured by their homes. Then the lenders disappear with the money, possibly reselling the loan to another lender who then forecloses on the home.

Refinancing Scams: Homeowners who fall victim to these scams are solicited to refinance their homes using a loan product they cannot afford to repay, leading to defaults and foreclosures while the disreputable brokers collect commissions and initial fees. Many homeowners who are targeted in these scams are elderly, have low incomes and/or credit problems. This illegal practice is also known as predatory lending.

Reverse Mortgage Fraud: Reverse mortgages allow older homeowners to convert part of the equity in their homes into cash, without having to sell their homes or take on additional monthly bills. Reverse mortgages can seem very attractive but can be a way to lure seniors into contracts they don't understand. Reverse mortgages can reduce inheritance amounts and give the lender the remaining value of the house. These loans may also lead to other types of fraud.



HELPFUL TIPS FOR AVOIDING LOAN SCAMS

- Never let anyone rush you into signing for a loan secured by your home. Always insist on a few days to think about it.
- Don't let family members or friends talk you into taking out or co-signing a loan on your home for their own purposes. Look for other ways to help them out of financial difficulties, such as recommending debt counseling.
- Shop around. Before you decide on a loan, meet with several different lenders, including large banks, small community institutions, and credit unions.
- Review the contract with someone you trust and have a lawyer review the document. Many local bar associations, senior organizations, and local colleges provide low-cost legal aid, which is well worth the money when something as valuable as your house is at stake.
- Never sign any document that contains blank lines that could be filled in after you sign, and insist on obtaining a photocopy of any document you sign for your records.
- Make sure you understand everything in the contract. Find out all the costs of the loan, including the APR (annual percentage rate), fees, points, and closing (or settlement) costs — including the lender's title insurance and appraisal fees.
- Be extremely cautious about using a contractor recommended by a lender, and vice versa. When choosing a contractor, get personal references and research them, then contact the appropriate government-licensing agency to verify that the contractor is licensed.
- If you negotiated in a language other than English with a loan broker or personal finance company, ask if a translation of the contract is available for you to review and keep for your records.



Where to Get Help

If you or someone you know has been a victim of Financial Fraud, contact:

BETTER BUSINESS BUREAU OF HAWAII

1132 Bishop Street, Suite 615, Honolulu, HI 96813

OAHU: (808) 536-6956 **TOLL-FREE:** 1-877-222-6551

WEBSITE: www.hawaii.bbb.org

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)

Business Registration Division (BREG)

Office of the Securities Commissioner (OSC)

335 Merchant Street, Suite 203, Honolulu, HI 96813

Consumer Resource Center:

OAHU: (808) 587-3222

TOLL-FREE: 1-800-394-1902

Monday-Friday, 7:45 a.m. to 4:30 p.m. Call for license verification and complaint history of professionals or businesses, information on identity theft, and other general consumer information.

Insurance Fraud Unit Hotline:

OAHU: (808) 587-7416

File insurance fraud complaints.

Monday-Friday, 7:45 a.m. to 4:30 p.m.

For neighbor island toll-free numbers, see list on page 120.

Securities Fraud Hotline:

OAHU: (808) 587-2267

TOLL-FREE: 1-877-447-2267

Report investment fraud or securities law violations.

Monday-Friday, 7:45 a.m. to 4:30 p.m.

WEBSITE: www.investing.hawaii.gov

POLICE DEPARTMENTS BY COUNTY

Hawaii County Police Department

349 Kapiolani Street, Hilo, HI 96720

HAWAII: (808) 935-3311 or 911

WEBSITE: www.hawaiiipolice.com

Honolulu Police Department

801 S. Beretania Street, Honolulu, HI 96813

OAHU: (808) 529-3115 or 911

WEBSITE: www.honolulupd.org

Kauai Police Department

3990 Kaana Street, Suite 200, Lihue, HI 96766-1268

KAUAI: (808) 241-1711 or 911

WEBSITE: www.kauai.gov/Police

Maui Police Department

55 Mahalani Street, Wailuku, HI 96793

MAUI: (808) 244-6400 or 911

WEBSITE: www.co.maui.hi.us/departments/Police

Ways We Get Scammed

HEALTHCARE FRAUD



HEALTHCARE PROVIDERS (e.g., doctors, hospitals, clinics, medical equipment providers) commit fraud when they bill for services not rendered, double bill, and/or overcharge. Alternately, healthcare frauds bill members or the government for reimbursement they should not receive. It is important to remember that most healthcare providers run honest practices. It takes only a small percentage of dishonest providers to commit fraud and cheat our healthcare systems out of billions of dollars.



The Five Main Types of Healthcare Fraud

1. **Billing for Non-Covered Services:** For example, billing cosmetic surgery as if it were medically necessary, or billing athletic shoes as orthopedic devices in order for the provider to receive payment.
2. **Billing for Non-Rendered Services:** Providers bill for services and/or equipment that is never received.
3. **Offering Money or Gifts in Exchange for Medical Services:** Be cautious of providers who offer money or gifts in exchange for your Medicare number; consistently agree to waive your co-payments; or offer free medical supplies and/or services. Sometimes these actions may be intended to keep you coming back for services that are unnecessary, but which allow the provider to bill Medicare for payment. Patients may be more inclined to return to a provider if they know that they will not have to pay any out-of-pocket costs, or if they expect to receive gifts; in reality, these patients are helping their providers to defraud the Medicare system.
4. **Unbundling:** Services that should be billed as one unit or panel are instead billed separately, at a higher cost. In other words, unbundling is selling “pieces” to receive a higher profit instead of selling the “whole” as a package, for a lower price.
5. **Up-coding:** Billing something basic, such as a routine examination, as something more costly, such as surgery. Up-coding also refers to billing for medical equipment or devices and providing an inferior product.



KEEP IN MIND

- **Your Medicare number is your Social Security number.** You may be more willing to give out your medical card or Medicare number thinking that it is a random number assigned to you by your insurance company, but in reality, that number is often your Social Security number. In the wrong hands, your Social Security number can be used for much more than healthcare fraud. It can lead to identity theft, financial fraud, and more.
- **Frauds targeting the Medicare Prescription Drug Program thrive on confusion and panic.** Medicare is not the easiest program to understand and may leave you confused. When faced with deadlines to choose a plan, you may become nervous. Fraudsters will use your confusion to mislead you to join a plan that may not be right for you or cause you to lose health benefits you may not be able to get back.
- **The consequences of Medicare fraud.** The money that has been lost due to fraud, waste, and abuse could have been used to provide more services to members, increase reimbursement rates for providers, or to reduce premiums and co-payments for members.
- **Future generations of Medicare members.** In order to ensure that your children, grandchildren, and their children receive the benefits to which they are entitled, everyone must work to protect their hard-earned dollars from fraud, waste, and abuse.



CHECKLIST: PREVENT MEDICARE FRAUD & ABUSE

- Keep a record of your doctor visits and/or hospital stays.

*Do you remember the last time you
went to the doctor and why?*

- Review your Medicare summary notice.

*Do you see anything that doesn't belong?
Is there something that doesn't look right to you?*

- Ask questions! You have a right to know about your healthcare.

*Do I need this test?
Does Medicare cover this test?*

- Find a doctor who you can talk to about your healthcare. Don't feel that you are trapped or obligated to stay with the same doctor. You have choices! Choose a provider that you trust.

- Protect your Medicare number! Treat it as you would any other important personal information.

- Don't be fooled! Don't accept money or gifts in exchange for your Medicare number.

- Be akamai, be smart! Educate yourself about Medicare.

Contact **SMP HAWAII** if you have questions or concerns regarding Medicare fraud, waste, or abuse.

OAHU: (808) 586-7281

TOLL-FREE: 1-800-296-9422



Where to Get Help

If you or someone you know has been a victim of Healthcare Fraud, contact:

BETTER BUSINESS BUREAU OF HAWAII

1132 Bishop Street, Suite 615, Honolulu, HI 96813

OAHU: (808) 536-6956

TOLL-FREE: 1-877-222-6551

WEBSITE: www.hawaii.bbb.org

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)

Business Registration Division (BREG)

Office of the Securities Commissioner (OSC)

335 Merchant Street, Suite 203, Honolulu, HI 96813

Consumer Resource Center:

OAHU: (808) 587-3222

TOLL-FREE: 1-800-394-1902

Monday-Friday, 7:45 a.m. to 4:30 p.m. Call for license verification and complaint history of professionals or businesses, information on identity theft, and other general consumer information.

Securities Fraud Hotline:

OAHU: (808) 587-2267

TOLL-FREE: 1-877-447-2267

Report Investment fraud or securities law violations.

Monday-Friday, 7:45 a.m. to 4:30 p.m.

WEBSITE: www.investing.hawaii.gov

EXECUTIVE OFFICE ON AGING

No. 1 Capitol District, 250 S. Hotel Street, Suite 406, Honolulu, HI, 96813.

OAHU: (808) 586-0100

E-MAIL: eoah@doh.hawaii.gov

WEBSITE: www4.hawaii.gov/eoa

POLICE DEPARTMENTS BY COUNTY

Hawaii County Police Department

349 Kapiolani Street, Hilo, HI 96720

HAWAII: (808) 935-3311 or 911

WEBSITE: www.hawaiipolice.com

Honolulu Police Department

801 S. Beretania Street, Honolulu, HI 96813

OAHU: (808) 529-3115 or 911

WEBSITE: www.honolulu.gov/police

Kauai Police Department

3990 Kaana Street, Suite 200, Lihue, HI 96766-1268

KAUAI: (808) 241-1711 or 911

WEBSITE: www.kauai.gov/Police

Maui Police Department

55 Mahalani Street, Wailuku, HI 96793

MAUI: (808) 244-6400 or 911

WEBSITE: www.co.maui.hi.us/departments/Police



phishing \‘fish-ing\: the act of falsely claiming to represent an established, legitimate company in an attempt to scam its customers into surrendering private information that will be used for identity theft. The victim is directed to update or provide personal information, such as passwords and credit card, Social Security, or bank account numbers already possessed by the legitimate organization.

However, the request comes from a bogus company set up only to steal users’ information.



Internet Phishing

Identity thieves may obtain sensitive information via Internet phishing. Internet phishing is the act of sending an e-mail that falsely claims to originate from an established, legitimate company in an attempt to scam the user into surrendering sensitive information that will be used for identity theft. The e-mail or pop-up instructs users to visit a website directing them to update personal information — such as passwords and credit card, Social Security, or bank account numbers — already in possession by the legitimate organization. However, the website is bogus, set up only to steal users' information.

LINK MANIPULATION

Most methods of phishing use some form of technical deception designed to make a link in an e-mail appear legitimate, as if it belongs to a legitimate organization. Deliberately misspelled uniform resource locators (URL) or misleading sub-domains are tricks frequently used by phishers. Another trick is to make the anchor text for a link appear to be a valid URL when the link actually connects to the phisher's website.

Reply Forward Delete

From: george@bankpretenders.com
Subject: Your Bank: Updating our Files

Aloha Kimo! We are updating our records and need you to visit our website at <http://www.19420.8490/yourbank.com> and verify your account information.

Please do not delay! If we do not receive verification within 5 days, your account will be deactivated.

Thank you for your time,

George A. Fisher
Customer Service Representative, Your Bank

EXAMPLE



Phone Phishing

Whereas standard phishing scams use e-mail to direct potential victims to phony web pages to steal their identities, telephone phishing scams prompt victims by voice message to call a customer support number. On the other end of the phone line, the scammer or an audio response unit waits to take the victims' account numbers, personal identification numbers, passwords, or other valuable personal data. The scammer on the other end of the phone line might claim that victims' accounts will be closed or other problems will occur if they fail to respond. Scammers often use pay phones, stolen cellular phone numbers, or hacked telephone account numbers to commit these crimes.

CALLER:

Hi I'm calling from [Your Bank] and we're just updating our records today. Could you please confirm the following information?

YOUR REPLY:

Sorry, I won't give out my information to a solicitor over the phone. I'll check with my own account representative.



Website Forgery

A legitimate website is “hijacked” and hosted on a computer which has been previously taken over by a hacker or phisher. Visitors are directed to the “hijacked” website by phishing e-mails and are asked to update their personal information.



HELPFUL TIPS FOR PROTECTING YOURSELF FROM FORGERY

- Review your statements. Call your financial institution immediately if you see any unusual transactions in your account.
- Don't give away personal information to unsolicited callers or via an Internet request.
- If an offer sounds too good to be true, it is probably a scam!



Where to Get Help

If you or someone you know has been a victim of phishing, contact your local police department or the Better Business Bureau. You can also contact the relevant source, such as your bank, credit union, mortgage lender, insurance agent, investment adviser, etc.

BETTER BUSINESS BUREAU OF HAWAII

1132 Bishop Street, Suite 615, Honolulu, HI 96813

OAHU: (808) 536-6956

TOLL-FREE: 1-877-222-6551

WEBSITE: www.hawaii.bbb.org

POLICE DEPARTMENTS BY COUNTY

Hawaii County Police Department

349 Kapiolani Street, Hilo, HI 96720

HAWAII: (808) 935-3311 or 911

WEBSITE: www.hawaiipolice.com

Honolulu Police Department

801 S. Beretania Street, Honolulu, HI 96813

OAHU: (808) 529-3115 or 911

WEBSITE: www.honolulupd.org

Kauai Police Department

3990 Kaana Street, Suite 200, Lihue, HI 96766-1268

KAUAI: (808) 241-1711 or 911

WEBSITE: www.kauai.gov/Police

Maui Police Department

55 Mahalani Street, Wailuku, HI 96793

MAUI: (808) 244-6400 or 911

WEBSITE: www.co.maui.hi.us/departments/Police



Special Senior Section

PROTECTING HAWAII'S SENIORS

OUR KUPUNA

BOTH NATIONAL AND LOCAL NEWS ACCOUNTS report the rising incidence of elderly citizens being victimized by a variety of consumer and financial fraud. Some of the most common scams include identity theft, investment fraud, and healthcare fraud.

Fighting the fraud and abuse of elders presents unique challenges in Hawaii. Statistics indicate that our aging population is growing significantly faster than the national average.

A NOTE ABOUT HAWAII'S ELDERLY

The cultural and ethnic diversity that represents our senior population is unlike that of any other state in the nation. Chinese, Filipino, Japanese, Korean, and other Asian ethnicities make up the majority of the population over 60 years old in Hawaii. The State of Hawaii also has the unique distinction of having the largest and highest percentage of Native Hawaiians and other Pacific Islander populations in the nation.

Due in part to the ethnic make-up of our senior population, there exists a common thread of local etiquette and courtesy. Listed below are some characteristics and barriers that can make Hawaii's elderly susceptible to fraud:

- Seniors were raised in a culture and generation in which strangers were embraced, welcomed, and trusted.
- Cultural protocols dictate that people in authority (or with the appearance of authority) should not be questioned.
- The elderly are hesitant to report that they have been victims of fraud for fear that loved ones will take away their independence.
- They were taught never to "make waves" or "ruffle feathers."



Senior Fraud Squad — Be A Volunteer

The Senior Fraud Squad serves as an educational resource for the community. Volunteers are trained by representatives of partnering agencies in their respective areas of expertise. Senior Fraud Squad members go out into the community and train peers to detect and report incidences of fraud, theft, and abuse. The Senior Fraud Squad encourages seniors to become self-advocates, protecting themselves, their families, and communities from financial, consumer, and healthcare fraud.

For more information about the program or volunteer opportunities, contact the **State of Hawaii, Executive Office on Aging, SMP Hawaii Program** on Oahu at (808) 586-7281 or neighbor islands call toll-free 1-800-296-9422.



Talking Story with Our Kupuna (Seniors) about Scams

In comparison to younger generations, seniors tend to have more financial assets and better lines of credit. The following section represents fraud scenarios and preventative tips every kupuna, family member, and caregiver should know.



Tutu, Protect Your Money!

Tutu got a phone call from a long-lost niece, Julie, who moved back to Hawaii and said she was an investment adviser with XXX Firm. After several calls and visits with food for Tutu, Julie said she had a “once in a lifetime” investment deal for Tutu. The return on investment would allow Tutu to help her grandchildren go to private school or even college. All Julie needed was Tutu’s personal information in order to set up an investment account for Tutu. Tutu gave Julie her personal information and authorized a \$20,000 withdrawal so Julie could set up an account to manage. A month later, Tutu became ill and her family came to help take care of her. They discovered that \$20,000 was missing from her account, the “so called” niece was not a registered investment adviser, and the \$20,000 was gone — along with Julie.



WARNING FLAGS! SIGNS OF A POTENTIAL FRAUD

- A stranger contacts you.
- You are offered a “great” deal.
- You must act right away.
- You are asked to give your personal information, such as your Social Security number and bank account information.
- You are asked to write a check to the individual or provide cash.
- When you are contacted under these circumstances, the best thing to do is to just say “NO.”

Grandma, That's a Bad Investment!

Grandma was 80 years old and was introduced to an investment opportunity to purchase a variable annuity for \$50,000. She didn't know much about variable annuities, but John, the investment adviser and salesperson, was so nice she just couldn't say no. John reassured Grandma that he would take care of everything and that Grandma didn't need to worry about anything. Grandma trusted him. Weeks later, Grandma still hadn't received any paperwork or statements. She called John but got no answer. One afternoon while Grandma was watching television, she saw John being arrested for investment fraud. By the time she checked, part of the money was locked in an investment she didn't understand and required a large penalty for withdrawal. The rest of the money was gone. John was not registered to sell securities in Hawaii.



CHECKLIST: PROTECT YOUR INVESTMENTS

- Verify that your investment adviser is registered with the Office of the Securities Commissioner at 1-877-447-2267.
- Understand it before you buy it. Never be embarrassed to ask questions.
- Request a copy of the final signed document before handing over any money.
- Keep an eye on the activity in your account and request regular statements.
- Keep all of your records relating to your investments and instructions, including notes of conversations you have with brokers, salespeople, financial advisers, and the like.

If you think you are or have been in a similar situation as Grandma, call the **Office of the Securities Commissioner** today to report investment fraud:

OAHU: (808) 586-2267

TOLL-FREE: 1-877-447-2267

WEBSITE: www.investing.hawaii.gov



Grandpa, Protect Your Medicare Number!

Grandpa gets a call from a man named Samuel Powers, who introduces himself as a representative of Company Rx Part D Plan. Mr. Powers states that his company has been contracted by Medicare to ensure that all senior citizens who do not currently have drug coverage sign up with his company's plan immediately, before all benefits are lost. Mr. Powers goes on to tell Grandpa that his plan carries full benefits without high premiums or co-payments. All Grandpa needs to do is provide Mr. Powers with his Medicare number and he will be automatically enrolled into the drug plan.



KEEP IN MIND

- Grandpa should call SMP Hawaii to find out if Company Rx Part D Plan is a Medicare-approved plan.
- Your Medicare number is personal information and you should never reveal your Medicare number to anyone you don't know or trust.
- Beware of some insurance agents who may try inappropriately to scare you or pressure you into joining a plan. Tell the insurance agent you need time to think about it and you will call them back. Then contact the DCCA-Insurance Division at (808) 586-2790 to check if they have a current license or report any concerns about the agent's actions.

Uncle, That Scooter's Not Free!

Uncle was waiting at the bus stop when his friend, Joe, rolled up in his new chromed-out MX3000 Power Scooter. Uncle asked, "How'd you get that?"

Joe replied, "I saw a commercial on TV from a company called Scooters 4 U, saying I can get a free power scooter and diabetic supplies paid for by Medicare."

Uncle said, "I didn't know you have diabetes!"

Joe, without hesitation, replied, "I don't. But it was free! All I had to do was give them my Medicare number." As Uncle's bus pulled up, Joe gave him the number to call: 1-800-RIP-U-OFF.



KEEP IN MIND

- Medicare will NEVER give out free medical supplies, including power scooters.
- Medicare will only pay for medical supplies if they are medically necessary.
- Only after YOUR physician's approval will Medicare pay for medical supplies.
- Never give out your Medicare number to unfamiliar companies or individuals because it is your Social Security number.
- If something seems too good to be true, it probably is.

If you believe that you, or someone you know, is a victim of healthcare fraud, contact **SMP Hawaii** on Oahu at (808) 586-7281 or neighbor islands call toll-free at 1-800-296-9422.

Aunty Kanani, Protect Your Mail!

Aunty Kanani received a call from a debt collector who demanded payment on a six-month overdue account for a credit card she never had. Auwe! What happened? Last year, mail from a new credit card company was sent to Aunty Kanani. Aunty didn't know this, but the mail from the new credit card company was stolen from Aunty's mail box and used by a perpetrator to make charges using Aunty Kanani's good credit history and her name.



CHECKLIST: WHAT CAN AUNTY KANANI DO?

- Notify credit bureaus and establish fraud alerts. Immediately report the situation to the fraud department of one of the three credit reporting companies:

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

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

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

- Monitor your credit reports. The federal FACTA law enables you to receive one free credit report per year from each of the three credit bureaus. Call 1-877-322-8228 for your free credit report.
- Call the police: 911. Report the crime to your local police right away. Get a copy of the report and/or report number.
- Place a security freeze. Hawaii and certain other states have a law that enables you to place a "security freeze" on your credit report. This is stronger than a fraud alert because it prevents anyone from accessing your credit file for any reason unless you instruct the credit bureaus to unfreeze your report.

- Inform the Federal Trade Commission (FTC). Report the crime to the FTC. Include your police report number. Although the FTC does not investigate identity theft cases, they share such information with investigators nationwide who are fighting identity theft. FTC's ID Theft Hotline: 1-877-438-4338 or www.consumer.gov/idtheft.
- Contact the creditors immediately by phone and in writing. Ask the credit grantors in writing to furnish you and the police with copies of the documentation, such as the fraudulent application and transaction records.
- Work with the debt collectors. If debt collectors try to get you to pay the unpaid bills on fraudulent accounts, ask for the name of the collection company, the name of the person contacting you, phone number, and address. Tell the collector that you are a victim of fraud and are not responsible for the account. Ask for the number and dates of the charges. Ask that they confirm in writing that you do not owe the debt and that the account has been closed.



HELPFUL TIPS FOR AUNTY KANANI

- Install a locking mailbox for incoming mail or promptly remove incoming mail after delivery.
- If traveling, contact the local post office to hold your mail or have someone you trust retrieve your mail.
- Place all outgoing mail in a secure, locked post office box.



Preventing Caregiver Exploitation

Older adults are living longer than ever. This longevity is unfortunately increasing the incidence of caregiver financial exploitation. Most cases of caregiver financial exploitation involve family members or trusted associates. It can include: taking money or property; forging an older person's signature; and getting an older person to sign a deed or will through deception or coercion.



HELPFUL TIPS FOR MANAGING YOUR FINANCIAL AFFAIRS

- Use direct deposit for Social Security checks and retirement benefits.
- Keep debit/credit cards, checkbooks and other valuables hidden if you have regular visitors to your home or apartment.
- Review your financial statements every month — especially if someone is paying your bills and managing your accounts.
- Choose your Power of Attorney with care and set up a system of checks and balances so no one person has complete control.
- Be careful about letting family, friends or tenants live in your house.
- Treat home care workers like employees, not friends.
- Maintain contact with family, friends, and neighbors. The more active you are, the less likely you are to be exploited.

To avoid being a victim to aides who take advantage of older adults in the home, we suggest conducting an attendant background check.



HOW TO CONDUCT A BACKGROUND CHECK

- Ask for three references and call them. At least two should be from former employers.
- Talk with informal sources. Contact the “friend of a friend” who suggested the person.
- Ask to see photo identification such as a valid driver’s license, passport, state ID card, green card, military ID card, immigration card, alien registration card, or a valid out-of state driver’s license. Keep a record of the ID number.
- If transportation will be provided, get proof of a clean driving record by calling the State District Court that serves your island. Verify their license, insurance, and car dependability. Ask for a test drive.
- If the person claims to be a licensed nurse or other professional, confirm with the licensing agency.
- Ask the aide to sign (1) a waiver of confidentiality allowing you to view their personal history information, and (2) a waiver allowing you to run a credit check. If the prospective aide is not willing to sign a waiver, they are probably not a suitable candidate.



Tips For Our Kupuna (Seniors)

K

Keep your personal information and passwords/PIN numbers safe. Protect your privacy and stop to think before you give out your personal information. Use a locked mailbox for incoming mail and place your outgoing mail in a designated postal box.

U

Use common sense for your personal finances and keep yourself informed about scams and schemes. “If it seems too good to be true, it probably is.”

P

Protect your money and assets. Promptly and carefully check your financial statements for unauthorized activities in your accounts.

U

Use the state regulatory agencies to verify if the person or product is properly registered or licensed with the right authorities. “No license, no sales.” Check the background and proper registration of the professionals handling your money or assets.

N

Never be embarrassed or ashamed to report fraud to the authorities.

A

Always do your homework, ask for help, and take your time. Make sure you understand exactly what you are investing in and/or signing. Request written information before parting with your money. “No paperwork, no deal.” Stop if you do not understand.



Where to Get Help

Seniors, if you need help or have questions, call us. Don't be a victim of fraud, schemes, and scams! We can help you or refer you to assistance:

BETTER BUSINESS BUREAU OF HAWAII

1132 Bishop Street, Suite 615, Honolulu, HI 96813

OAHU: (808) 536-6956

TOLL-FREE: 1-877-222-6551

SENIOR SCAM HOTLINE: (808) 628-3950

The Better Business Bureau of Hawaii Foundation established a Senior Scam Hotline to help protect seniors from being victimized by fraudulent offers and other scams.

Seniors may call with questions about the legitimacy of offers and propositions made to them and can call anonymously on Oahu at (808) 536-8609 Monday to Friday from 9:00 a.m. to 3:00 p.m. for free information and advice. The Better Business Bureau wants individuals and families to know their lives and problems are meaningful, and that someone understands and can help them make informed choices.

DEPARTMENT OF THE ATTORNEY GENERAL

Criminal Justice Division

Medicaid Fraud Control Unit (MFCU)

333 Queen Street, 10th Floor, Honolulu, HI 96813

PHONE: (808) 586-1058

FAX: (808) 586-1077

Investigates allegations of provider fraud committed against the State Medicaid program, and patient abuse and neglect allegations against licensed and non-licensed care providers. Prosecutes confirmed allegations both criminally and civilly.

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)
Business Registration Division (BREG)
Office of the Securities Commissioner (OSC)

335 Merchant Street, Suite 203, Honolulu, HI 96813

SECURITIES FRAUD HOTLINE: (808) 587-2267

TOLL-FREE: 1-877-447-2267

If seniors have any questions or concerns on investment fraud, contact the DCCA Office of the Securities Commissioner Scam line.

EXECUTIVE OFFICE ON AGING

No. 1 Capitol District, 250 S. Hotel Street, Suite 406, Honolulu, HI 96813

PHONE: (808) 586-0100 **FAX:** (808) 586-0185

E-MAIL: ea@doh.hawaii.gov **WEBSITE:** www4.hawaii.gov/ea/

SMP Hawaii Program (Formerly SageWatch)

PHONE: (808) 586-7281

TOLL FREE: 1-800-296-9422

For questions or concerns regarding Medicare fraud, waste, or abuse.

Sage PLUS Program

PHONE: (808) 586-7299

TOLL FREE: 1-888-875-9229

TTY: (866) 810-4379

For questions about Medicare benefits, Medicare Advantage Program, Medicare Part D, and health plans.



PREVENTION TIPS



Helpful Tips to Protect Yourself from Being a Victim of Fraud

- Keep your Social Security card, passport, and other important documents in a secure place.
- Do not carry confidential personal information cards and/or documents, such as Social Security card or Medicare card, in your wallet.
- Always use passwords for financial accounts.
- Do not write down or use common passwords.



Auction / On-Line Purchase Tips

On-line auction houses are go-betweens for would-be buyers and sellers. Before you bid, find out how it works. The Federal Trade Commission, Better Business Bureau, and other agencies offer the following information:

- Identify the seller and check on their reputation with the Better Business Bureau.
- Check with the auction house on the seller's reputation and transaction history.
- Avoid impulse bids and purchases. Do your homework. Be sure you know what you're bidding on, its value, and all terms and conditions of the sale.
- Ask about the seller's return policy. Ask who pays for shipping and handling and costs on a returned item.
- Evaluate the different payment options such as credit card, escrow services, or C.O.D.
- Be cautious if the seller insists on payment by check or money order.
- Ask the seller about servicing the product after the purchase.
- Know which websites you are purchasing from.
- Designate one credit card with a minimal limit for on-line shopping.
- Use a secure third-party on-line payment service, which is indicated with the "https" in the address box and "Secure Sockets Layer (SSL) Certificate" to guarantee your purchase.
- Read the website privacy policy to learn how your information will be used and protected.
- Look for the stamp of approval of the Better Business Bureau or TRUSTe.

- Do not accept advance-fee payments or second chance offers.
- Do not go outside of the on-line store website to complete transactions.
- If you are unsure if a website is fraudulent or valid, go to www.ftc.gov and perform a web search on the company.
- Be wary of unreasonably low bargain prices or unusually attractive promises.





Computer / Internet Tips

- Shred documents with personal information.
- Do not give out your personal information over the Internet unless you initiated the contact and know who you are dealing with.
- Change your e-mail and on-line account passwords regularly.
- Do not give out your passwords to anyone.
- Use a firewall and virus protection software to protect data.
- If paying bills or shopping on-line, look for the “Secure Sockets Layer (SSL) Certificate” or secure padlock on the bottom of the screen and “https” in the address box.
- Run a “wiping” program to delete all data if donating your computer.
- When discarding your computer, destroy the hard drive.



Tips and Recommendations for Computer Security

- Keep your computer's operating system updated.
- Keep your software programs updated.
- Back up your data and files. You can store your data and files on CD, DVD, or external hard drive.
- Install anti-virus and anti-spyware software. Keep the software current.
- Use a firewall. Sharing an Internet connection from a single location usually involves the use of a router. Out of the box, these devices are not secured, BUT they can be secured by enabling the firewall options that are usually built into these devices.
- Make sure that the routers you use have a firewall option. Read the manual to learn how to prevent your information from being compromised.
- If and when you discard your computer, make sure your data has been completely erased. Use a program that digitally "shreds" and "overwrites" the data. Another option is to remove the hard drive and either keep it secured or physically destroy it. Or you can hire a reputable technical service to "erase and overwrite" the contents of the hard drive.



Tips for Using E-mail

- Try not to use the e-mail address provided by your Internet Service Provider (ISP). Use web based e-mail (Yahoo!, Hotmail, Gmail) because:
 - It's free.
 - It's disposable.
- If you decide to use a web based e-mail account, be careful when giving your:
 - Real name
 - Address
 - Telephone numbers
 - Photos
- Make sure your anti-virus and anti-spyware programs are running whenever you use your e-mail program, especially before opening e-mails to read.
- If your e-mail program or ISP allows you to read or view your e-mails "offline" (which means you are not connected to the Internet), you should use this option.



KEEP IN MIND

- When receiving e-mails, scrutinize the following fields:
 - SENDER:** If you do not recognize the e-mail address of the sender, do not open the e-mail.
 - SUBJECT:** If you are not interested in the subject — do not open the e-mail.
- Disable your e-mail program's feature to "preview" and/or to automatically open the e-mails. You should be able to select which e-mail you wish to read. Don't let your e-mail program decide for you.
- After reading an e-mail, the program should always default back to the "inbox" for you to choose which e-mail to open next.
- Do not click on hyperlinks in the body of e-mails. They may transport you to a website which may infect your computer with a virus and/or spyware. If you wish to view the website that's referenced by the hyperlink, then open another browser window and type the address in.
- Check for "typos" before hitting send/return/enter key.
- Review the message you are sending and decide if that is what you wish to send.
- Verify the address of the recipient of the e-mail.
- And finally, e-mail messages are like postcards. Anyone and everyone can read it unless you encrypt the message. Nothing is private when using e-mail. Furthermore, what you've written can be edited and forwarded without your knowledge.



Tips for Securing Passwords

Passwords are meant to be kept secret. Therefore, do not give out your password!

- A “strong” password consists of:
 - At least eight (8) characters.
 - One character is upper case.
 - One is a numeral.
 - One is a special character (e.g., “&” or “#”).

An example of a password using all the above would be “a3Veuk*d”.

- Create a password using a non-English language, for example, Hawaiian, Filipino, or Chinese. You could also use pidgin or slang terms (e.g., “WassupBrah!”).
- Create a password using the first characters of a “pass phrase,” (e.g., “Jack and Jill went up the hill to...” would result in the password, “JaJwutht”).
- Do not use the following for passwords:
 - Names, including last names.
 - Date of birth.
 - Social Security number.
 - Account numbers.
 - Identification numbers (e.g., addresses).
 - Any word that can be found in an English dictionary.
- Do not use the same password for everything.
- Change passwords periodically.

If you have to write your passwords down, secure them in a locked container or in a safe.

- Do not keep your password near, on, or in the computer; in your wallet or purse; or in your car.
- And do not write, "This password is for..."

Password:

* * * * |



Tips for Finances

- Make sure you're receiving your monthly statements/bills. For missing statements/bills, contact the companies immediately.
- Obtain an annual free credit report from all three companies, www.annualcreditreport.com.
- Review your monthly financial statements/bills regularly.
- Report any discrepancies on statements/bills to the company immediately.
- Insert credit card and bank customer care phone numbers into your cell phone.
- Take immediate action on unexpected transactions on credit card or account statements, denials of credit for no apparent reason, calls or letters about purchases you did not make, and any other suspicious activity relating to your credit.
- Do not give out your financial account passwords and PIN numbers.
- Change your financial account passwords and PIN numbers regularly.



Tips for Mail

- Place all outgoing mail into a secure, locked post office box.
- Install a locking mailbox for incoming mail or promptly remove incoming mail after delivery.
- If traveling, contact your local post office to hold your mail or have someone you trust retrieve your mail.
- Shred mail with your personal information.
- Monitor your monthly bills and financial statements. Contact the companies if you are missing any monthly bills or financial statements.





Tips for Phone

- Do not give out your personal information on the phone unless you initiated the contact and are certain of who you contacted.
- Ask questions before giving personal information:
 - Why do you need my information?
 - How will my information be used?
 - Who will be looking at my information?
 - Where will my information be stored and will it be secure?
 - What will happen if I don't give you my information?
- If someone asks you to provide personal information over the phone:
 - Always ask for the caller's full name, business number, and company and tell the caller you'll call them back.
 - Don't call the number that was provided to you by the caller, instead, look up the company and phone number in a telephone book and call that number.



If You Are a Victim

STEPS TO RECOVERY

PREVENTION IS YOUR MAIN DEFENSE from becoming a victim of fraud, which can often lead to identity theft. We hope the information provided in the previous pages will assist you in making informed decisions concerning your finances and identity. However, if you are a victim and need resources, the following pages have been provided to assist you in contacting the proper authorities and agencies. Sample letters, along with the Department of Commerce and Consumer Affairs Securities Enforcement Complaint Form, are included in this section to help you with steps to recovery.



Victim Journal Log

IDENTITY THEFT VICTIM'S LOG

Contact any one of the credit bureaus listed below to place a 90-day Fraud Alert on your credit file. Ask them to contact you before an account can be opened or changed. Request copies of your credit report (by phone or by visiting any of these websites) and review them carefully.

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

DATE: _____ CONTACT PERSON: _____

COMMENTS/NOTES: _____

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

DATE: _____ CONTACT PERSON: _____

COMMENTS/NOTES: _____

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

DATE: _____ CONTACT PERSON: _____

COMMENTS/NOTES: _____



Where to Get Help: EQUIFAX

How to Place a Fraud Alert by Phone

Follow these 8 Easy Steps:

Call	1-800-525-6285 Welcome to the Equifax Automated Fraud and Active Duty Alert System.
Press 1	To add an "Initial 90-Day" fraud alert to the credit file.
Enter:	9-digit Social Security number.
Enter:	Number of your street address. (e.g., 123 5th Avenue, enter ONLY the numbers 123.)
Enter:	Last 2-digits of your birth year. (e.g., born in 1932, enter ONLY the numbers 32.)
Enter:	Day phone number with area code. (The area code for Hawaii is 808.)
Enter:	Evening phone number with area code.
Equifax Confirmation Number:	

If for some reason your request is unable to be processed, you will need to submit your request in writing with the following pieces of information: full name, current and former addresses, Social Security number, date of birth, a copy of your driver's license or utility bill to confirm your address, and an official document containing your Social Security number (e.g., Social Security card, pay stub, W-2 Form).

Submit your request and the above information to:

EQUIFAX, OFFICE OF FRAUD ASSISTANCE
P. O. Box 105069
Atlanta, GA 30348-5069.

The fraud alert information and menu options in this document are subject to change at any time.



Where to Get Help: EXPERIAN

How to Place a Fraud Alert by Phone

Follow these 11 Easy Steps:

Call	1-888-397-3742 Thank you for calling Experian.
Press ②	All others (This includes Fraud Alert.)
Press ③	If you believe that your credit information is being used fraudulently.
Press ②	To add an alert to your credit file using our automated system.
Press ①	To add a "Temporary Initial (90-Day)" fraud security alert.
Press ②	To continue to our automated alert system.
Enter:	9-digit Social Security number followed by the # key.
Enter:	5-digit zip code followed by the # key.
Enter:	Numeric address followed by the # key. (e.g., for 123 5th Avenue, enter ONLY the numbers 123.)
Enter:	U.S. phone number with area code. (The area code for Hawaii is 808.)
Experian Confirmation Number:	

Send written inquiries to:

EXPERIAN

P.O. Box 9532

Allen, TX 75013

The fraud alert information and menu options in this document are subject to change at any time.



Where to Get Help: TRANSUNION

How to Place a Fraud Alert by Phone

Follow these 11 Easy Steps:

Call	1-800-680-7289 Remain on the line for all other TransUnion Fraud Victim Assistance Options.
Press or Say:	Current mailing zip code.
Press or Say 1	To add a fraud alert to your credit report.
Press or Say 1	To add an "initial 90-Day" fraud alert to your credit report.
Enter or Say:	9-digit Social Security number. If this is correct, say YES or press 1 .
Enter or Say:	6-digit date of birth followed by the # key. (e.g., born May 4, 1933, enter 050433.)
Enter or Say:	4-digit year of birth followed by the # key.
Enter or Say:	Numeric address followed by the # key. (e.g., 123 5th Avenue, enter ONLY the numbers 123.)
Enter or Say:	10-digit daytime phone number. (The area code for Hawaii is 808.) If this is correct, say YES or press 1 .
Enter or Say:	10-digit evening phone number. (The area code for Hawaii is 808.) If this is correct, say YES or press 1 .
TransUnion Confirmation Number:	

Send written inquiries to:

TRANSUNION, FRAUD VICTIM ASSISTANCE
P.O. Box 6790
Fullerton, CA 92834.

The fraud alert information and menu options in this document are subject to change at any time.

- Close any financial accounts that have been tampered with or established fraudulently. See pages 95–98 for sample letters.

CREDITOR:

ADDRESS:

PHONE:

DATE:

CONTACT PERSON:

COMMENTS/NOTES:

CREDITOR:

ADDRESS:

PHONE:

DATE:

CONTACT PERSON:

COMMENTS/NOTES:

CREDITOR:

ADDRESS:

PHONE:

DATE:

CONTACT PERSON:

COMMENTS/NOTES:

CREDITOR:

ADDRESS:

PHONE:

DATE:

CONTACT PERSON:

COMMENTS/NOTES:

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

HAWAII COUNTY POLICE DEPARTMENT: (808) 935-3311

HONOLULU POLICE DEPARTMENT: 911

KAUAI POLICE DEPARTMENT: (808) 241-1711

MAUI POLICE DEPARTMENT: (808) 244-6400

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

AGENCY/ DEPARTMENT:

PHONE:

REPORT #:

DATE:

CONTACT PERSON:

COMMENTS/NOTES:

AGENCY/ DEPARTMENT:

PHONE:

REPORT #:

DATE:

CONTACT PERSON:

COMMENTS/NOTES:

- File a complaint with the Federal Trade Commission (FTC) and complete the Identity Theft Complaint Form and the Identity Theft Affidavit. Contact the FTC for the forms:

FEDERAL TRADE COMMISSION

1-877-438-4338

www.ftc.gov

1-866-653-4261 (TTY)

Or write to:

IDENTITY THEFT CLEARINGHOUSE

FEDERAL TRADE COMMISSION

600 Pennsylvania Avenue, NW

Washington, DC 20580

Identity Theft Complaint Form:

DATE: _____

COMMENTS/NOTES: _____

Identity Theft Affidavit:

DATE: _____

COMMENTS/NOTES: _____



How to obtain your free credit report

Call these companies or visit their websites to obtain your free credit report. You are entitled to one free credit report per year from each of the three credit bureaus listed below. Annual Credit Report Request Service is a centralized service for consumers to request free annual credit reports.

ANNUAL CREDIT REPORT REQUEST SERVICE

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

If you are a victim, you can request a free credit report directly from the three major credit bureaus:

EQUIFAX 1-800-525-6285 or www.equifax.com

EXPERIAN 1-888-397-3742 or www.experian.com/fraud

TRANSUNION 1-800-680-7289 or www.transunion.com



Sample Letters to Help You with Recovery

Use the following sample letters as a starting point for writing your own.

Sample Letter 1: Sent to a Credit Bureau

Send this letter to a credit bureau (Equifax, Experian and TransUnion) to:

- Dispute fraudulent information or charges.
- Place a 90-Day Fraud Alert.
- Request a victim's statement so that creditors must contact you before opening or changing an account in your name.
- Protect your credit standing.

Sample Letter 2: Sent to a Creditor of a New Account Opened Fraudulently in Your Name

Send this letter to a creditor to:

- Dispute an account that was fraudulently opened in your name.
- Deny responsibility for any charges incurred.
- Close the account.

Sample Letter 3: Sent to a Creditor of an Existing Credit or Debit Account Used Fraudulently Without Your Knowledge

Send this letter to a creditor to:

- Dispute a fraudulent charge or charges made to an existing account in your name.
- Deny responsibility for any charges incurred and request an investigation to clear you of obligation.

SAMPLE FOLLOW UP LETTER 1

Send to a Credit Bureau

Date

Your Name

Your Address

Your City, State, Zip Code

Name of Creditor

Fraud Department

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute are also circled on the attached copy of the report I received. [Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as a credit account, judgment, etc.]

I am a victim of identity theft, and did not make the charge(s). I am requesting that the item(s) be blocked to correct my credit report. In addition, I'd like to request a fraud alert placed on my file along with a victim's statement asking creditors to call me before opening any new accounts.

Enclosed are copies of [use this sentence if applicable and describe any enclosed documentation] supporting my position. Please investigate this (these) matter(s) and block the disputed item(s) as soon as possible.

Sincerely,

Your Name

Enclosure(s): [list of any additional documents you're sending]

SAMPLE FOLLOW UP LETTER 2

Send to a Creditor of a New Account Opened Fraudulently in Your Name

Date

Your Name

Your Address

Your City, State, Zip Code

Name of Creditor

Fraud Department

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute an account opened fraudulently in my name. I am a victim of identity theft and did not open account number [give number of fraudulent account]. Please close the account opened fraudulently in my name. I am not responsible for any charges made to this account.

Enclosed are copies of [use this sentence to describe any enclosed information, such as a police report, ID Theft Affidavit, request for Fraudulent Account Information forms] supporting my position. I am also requesting copies of any documentation, such as applications and transaction records, showing the activity on this (these) fraudulent account(s).

Sincerely,

Your Name

Enclosure(s): [list of any additional documents you're sending]

SAMPLE FOLLOW UP LETTER 3

Send to a Creditor of an Existing Credit or Debit Account Used Fraudulently Without Your Knowledge

Date

Your Name

Your Address

Your City, State, Zip Code

Name of Creditor

Fraud Department

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) attributed to my account in the amount of \$_____. I am a victim of identity theft and did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of [use this sentence to describe any enclosed information, such as a police report, ID Theft Affidavit] supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

Your Name

Enclosure(s): [list of any additional documents you're sending]

DCCA SECURITIES ENFORCEMENT COMPLAINT FORM

Mr. () Complainants Name: _____ Social Security Number: _____

Mrs. () _____

Ms. () _____

Home Address: _____

Mailing Address: _____

Home Telephone: _____ Work Telephone: _____

Name(s) of company and/or individual your complaint is against: SSN/FEIN

Address: _____

Telephone: _____

Witness Name(s): _____

Address: _____

Telephone: _____

Witness Name(s): _____

Address: _____

Telephone: _____

Witness Name(s): _____

Address: _____

Telephone: _____

1. Did you sign any contract/agreement? If yes, please include a copy of the contract/agreement. Who negotiated the contract for the Respondent(s)? If the contract/agreement was not in writing, explain your understanding of the terms of your contract/agreement.

2. Did you and/or the Respondent(s) modify or amend the contractual terms? If yes, explain the modification or amendment.

3. Were any guarantees and/or promises made? If yes, please include copies of any guarantees or written promises. If not in writing, explain your understanding of the terms of the verbal guarantees and/or promises.

4. If the contract was made because of an advertisement, please provide a copy of the advertisement. If not available, then provide the date of the advertisement and where it was located, such as a sign, newspaper, radio, television, magazine, leaflet, etc.

5. Have you attempted to settle your complaint with the Respondent(s)? If yes, provide detailed facts on your attempt. Include the date you complained and name and title of person to whom you complained.

6. Have you attempted to settle your complaint with another agency or with the courts? If yes, what agency or court (provide the name and address of person contacted)?

7. What would you consider to be a fair resolution to your complaint and why?

8. Please attach relevant documentation to support your complaint. If documents are not attached, explain why you are not providing documents to support your complaint.

Certification of Complaint:

This complaint will not be processed unless this form is complete, legible and signed.

I hereby certify that all statements in this complaint are true and correct to the best of my knowledge, and I agree to testify.

Complainant's Signature

Date

Submit this completed form to:

State of Hawaii, Securities Enforcement Branch, Department of Commerce and Consumer Affairs. *In person* at 335 Merchant Street, Suite 205, Honolulu, HI 96813 *or by mail* to P.O. Box 40, Honolulu, HI 96810.

Directory of

RESOURCES



FOR YOUR QUICK REFERENCE, we have provided a Directory of Resources by county, state, and national contacts with a short description to identify their area of expertise. Please feel free to contact these agencies or organizations should you have any questions or, for those that have websites, visit them on-line.

Within the categories of County, State and Local, and National, resources are listed alphabetically.



County Resources City & County of Honolulu

DEPARTMENT OF COMMUNITY SERVICES

Elderly Affairs Division

Information & Assistance

715 S. King Street, Suite 200, Honolulu, HI 96813

PHONE: (808) 768-7700

ADDITIONAL CONTACT NUMBERS: (808) 768-7705

FAX: (808) 527-6895

WEBSITE: www.elderlyaffairs.com

DESCRIPTION: The Information and Assistance section of the Elderly Affairs Division conducts outreach, provides information, and links senior citizens with programs and services they need to remain independent and well. It staffs a telephone help line; conducts client assessments; provides information about aging and programs and services for older adults and caregivers; makes referrals to service agencies; gives public presentations; exhibits at fairs and community events; produces a newsletter, brochures, and resource directory.

AUDIENCE: Seniors 60 years and older and family caregivers.

AFFILIATIONS: National Eldercare Locator 1-800-677-1116

DEPARTMENT OF THE PROSECUTING ATTORNEY

1060 Richards Street, Honolulu, HI 96813

PHONE: (808) 547-7400

TOLL-FREE: 1-800-531-5538

FAX: (808) 527-6552

WEBSITE: www.honolulu.gov/prosecuting

DESCRIPTION: Criminal prosecution of physical and financial abuse of the elderly. Holds community meetings, talks, training, and school lectures regarding awareness and prevention of abuse.

AUDIENCE: General public.

HONOLULU POLICE DEPARTMENT Criminal Investigation Division

Alapai Headquarters, 801 S. Beretania Street, Honolulu, HI 96813

PHONE: 911

ADDITIONAL CONTACT NUMBERS: (808) 529-3115

FAX: (808) 529-3013

WEBSITE: www.honolulupd.org

DESCRIPTION: Offers an informational presentation about how to protect yourself against identity theft, credit card fraud, forgery, and related subjects. Performs investigations into financial fraud type crimes including forgery and fraudulent use of credit cards or bank accounts.

AUDIENCE: Financial institutions and their customers, businesses, and any person with credit cards or bank accounts.

AFFILIATIONS: All Federal law enforcement agencies, financial institutions and businesses.



County Resources Hawaii County

HAWAII COUNTY OFFICE OF AGING

101 Aupuni Street, Suite 342, Hilo, HI 96720

PHONE: (808) 961-8600

FAX: (808) 961-8603

75-5706 Kuakini Highway, Kailua-Kona, HI 96740-1751

PHONE: (808) 327-3597

FAX: (808) 327-3599

WEBSITE: www.hcoahawaii.org

DESCRIPTION: The Office of Aging provides program planning, grants management, service coordination, advocacy, training, and public information to residents. Services include: adult day care, assisted transportation, caregiver support and resource center, case management, chores, community planning, congregate meals, education and training, employment, home delivered meals, homemaker/housekeeping, home modification, information and assistance, legal assistance, long-term care access, nutrition education, outreach, personal care, respite and volunteer services. The office also produces a newsletter, brochure, and a resource directory.

AUDIENCE: Seniors 60 years and older and family caregivers.

AFFILIATIONS: Administration on Aging (AOA), American Society on Aging (ASA), National Association of Area Agencies on Aging (N4A), Alliance of Information & Referrals Systems (AIRS), National Family Caregiver Association (NFCA).

HAWAII COUNTY POLICE DEPARTMENT

Criminal Investigation Section

349 Kapiolani Street, Hilo, HI 96720

PHONE: (808) 935-3311 or 911

ADDITIONAL CONTACT NUMBERS:

HILO: (808) 961-2255

KONA: (808) 326-4646 ext. 268

FAX: (808) 961-2376

WEBSITE: www.hawaiipolice.com

DESCRIPTION: Offers presentations to private and public agencies and groups about how to protect yourself against identity theft, credit card fraud, forgery, and related subjects. Provides law enforcement and investigations of financial fraud including identity theft.

AUDIENCE: General public.

OFFICE OF THE PROSECUTING ATTORNEY COUNTY OF HAWAII

655 Kilauea Avenue, Hilo, HI 96720

EAST HAWAII: (808) 961-0466 (main office)

FAX: (808) 961-8908

WEST HAWAII: (808) 322-2552

NORTH HAWAII: (808) 887-3017

WEBSITE: www.hawaiicountyprosecutor.com

DESCRIPTION: Legal agency responsible for the prosecution of all criminal offenses occurring on the island of Hawaii.

AUDIENCE: General public.

AFFILIATIONS: Law enforcement and criminal justice agencies, crime victim service agencies, and other community organizations.



County Resources Kauai County

KAUAI COUNTY AGENCY ON ELDERLY AFFAIRS

4444 Rice Street, Suite 330, Lihue, HI 96766

PHONE: (808) 241-4470

FAX: (808) 241-5113

WEBSITE: www.kauai.gov

DESCRIPTION: Plans, implements, supports, and advocates for the well-being of Kauai's older adults. Agency on Elderly Affairs contracts with community organizations to provide home-delivered and congregate meals, legal assistance, transportation, caregiver training, and an array of home-based services.

AUDIENCE: Seniors 60+, family caregivers including grandparents raising grandchildren, and general public.

AFFILIATIONS: Alliance of Information & Referral Systems (AIRS), American Society on Aging (ASA), National Association of Area Agencies on Aging (N4A).

KAUAI POLICE DEPARTMENT

3990 Kaana Street, Suite 200, Lihue, HI 96766

PHONE: (808) 241-1711 or 911

ADDITIONAL CONTACT NUMBERS: (808) 241-1677

FAX: (808) 241-1714

WEBSITE: www.kauai.gov/Police

DESCRIPTION: Investigations of fraud, theft, and associated crimes.

AUDIENCE: General public.

OFFICE OF THE PROSECUTING ATTORNEY COUNTY OF KAUAI

3990 Kaana Street, Suite 210, Lihue, HI 96766

PHONE: (808) 241-1888

FAX: (808) 241-1758

WEBSITE: www.kauai.gov/prosecutingattorney

DESCRIPTION: Criminal prosecution of physical and financial abuse of the elderly. Performs and participates in community meetings, training sessions, and various school lectures regarding awareness and prevention of abuse.

AUDIENCE: General public.



County Resources Maui County

MAUI COUNTY OFFICE ON AGING

2200 Main Street, Suite 547, Wailuku, HI 96793

PHONE: (808) 270-7774

FAX: (808) 270-7935

E-MAIL: aging@mauicounty.gov

WEBSITE: www.mauicounty.gov/departments/Housing/aging

DESCRIPTION: Provides information, assistance and outreach to Maui County's 60+ and caregivers. Includes assessment of individual's needs and linkage/referral to appropriate services; public education on fraud and elder abuse; participation in senior information, health and wellness events; annual caregiver's conference; Outstanding Older Americans Recognition; Maui Coordinated Aging Network (CAN); Interdisciplinary Team (IDT).

AUDIENCE: Seniors 60+, caregivers (including grandparents raising grandchildren), and general public.

AFFILIATIONS: Alliance of Information & Referral Systems (AIRS),

American Society on Aging (ASA), National Association of Area Agencies on Aging (N4A).

MAUI POLICE DEPARTMENT

55 Mahalani Street, Wailuku, HI 96793-2155

PHONE: (808) 244-6400 or 911

ADDITIONAL CONTACT NUMBERS: (808) 244-6300

FAX: (808) 244-5576

WEBSITE: www.co.maui.hi.us/departments/Police

DESCRIPTION: Provides law enforcement and investigation of personal and property crimes.

AUDIENCE: General public.

OFFICE OF THE PROSECUTING ATTORNEY COUNTY OF MAUI

150 S. High Street, Wailuku, HI 96793-2155

(or Investigative Division, One Main Street Plaza, 2200 Main Street, Suite 530, Wailuku, HI 96793)

PHONE: (808) 270-7777

FAX: (808) 270-7625

WEBSITE: www.co.maui.hi.us/departments/Prosecuting/

DESCRIPTION: Criminal prosecution of physical and financial abuse of the elderly. Holds community meetings, talks, training sessions, and school lectures regarding awareness and prevention of abuse.

AUDIENCE: General public.



State and Local Resources

AARP HAWAII

Campaign for Wise and Safe Investing

1132 Bishop Street, Suite 1920, Honolulu, HI 96813

TOLL-FREE: 1-866-295-7282

FAX: (808) 537-2288

WEBSITE: www.aarp.org/investmentfraud

DESCRIPTION: Increasing awareness among investors and potential investors on how to better manage financial decision-making, avoid financial fraud and marketplace abuse, and how to prevent investment fraud. Hosts events, workshops, and volunteer training.

AUDIENCE: People age 50+.

AFFILIATIONS: Investor Protection Trust.

ALU LIKE, INC.

Kumu Kahi Department

Ke Ola Pono No Na Kupuna

(Good Health And Living For The Elderly)

458 Keawe Street, Honolulu, HI 96813

PHONE: (808) 535-6700

FAX: (808) 524-1533

WEBSITE: www.alulike.org

DESCRIPTION: Provides nutrition and supportive services (recreation, education, promotion of well-being) to Native Hawaiians aged 60 years and older on the islands of Hawaii, Kauai, Maui, Molokai, and Oahu.

AUDIENCE: Native Hawaiians 60 years of age or older and family caregivers.

BETTER BUSINESS BUREAU OF HAWAII

1132 Bishop Street, Suite 615, Honolulu, HI 96813

PHONE: (808) 536-6956

TOLL-FREE: 1-877-222-6551

FAX: (808) 628-3970

OFFICE HOURS: Monday-Friday, 8:00 a.m. to 4:30 p.m.

E-MAIL: info@hawaii.bbb.org

WEBSITE: www.hawaii.bbb.org

DESCRIPTION: The Better Business Bureau of Hawaii provides dispute resolution (conciliation, mediation, and arbitration), autoline arbitration, advertising review, marketplace investigations, charity review and senior fraud education to create an ethical marketplace where buyers and sellers can trust each other. BBB's mission is to be the leader in advancing marketplace trust. BBB accomplishes this mission by: 1) creating a community of trustworthy businesses, 2) setting standards for marketplace trust, 3) encouraging and supporting best practices, 4) celebrating marketplace role models, and 5) denouncing substandard marketplace behavior.

AUDIENCE: General public.

SENIOR SCAM HOTLINE

PHONE: (808) 628-3950

TOLL-FREE: 1-888-333-1593

DEPARTMENT OF THE ATTORNEY GENERAL Crime Prevention & Justice Assistance Division Community & Crime Prevention Branch

235 S. Beretania Street, Suite 401, Honolulu, HI 96813

PHONE: (808) 586-1150

FAX: (808) 586-1373

WEBSITE: www.hawaii.gov/ag/cpja

DESCRIPTION: A partner, catalyst, leader, and resource to encourage work towards a comprehensive approach to crime prevention. The branch coordinates training sessions on ways to prevent crime and works with others in the community on the safety and well-being of neighborhoods. Also, the statewide coordinator of the McGruff Truck® Program and McGruff, “Take a Bite Out of Crime®” campaign. Provides trainers’ workshops on the Identity Theft Manual, titled “Your Identity is Your Kuleana” for law enforcement and community trainers.

The Crime Prevention & Justice Assistance Division serves as the central agency to provide the Attorney General with information and resources needed to address crime and crime prevention. The division researches crime issues and reports comprehensive crime statistics for the state, utilizing federal and state funds to address crime problems and criminal justice system issues; educates citizens on the prevention of crime and the promotion of community involvement; and develops and maintains a computerized juvenile offender information system.

AUDIENCE: Law enforcement, government agencies, service providers, and citizens.

AFFILIATIONS: National Crime Prevention Council (NCPC),
ncpc.org and mcgruff.org

DEPARTMENT OF THE ATTORNEY GENERAL

Criminal Justice Division

Hawaii Internet & Technology Crimes Unit (HiTeC)

425 Queen Street, Honolulu, HI 96813

PHONE: (808) 587-4111

FAX: (808) 587-4118

WEBSITE: www.hicac.com or www.hitechcrimes.com

DESCRIPTION: To increase investigations and prosecutions of computer-facilitated crimes, including Internet crimes against children. Participates

in investigations (including undercover operations), prosecutions, computer forensics, and community/public awareness.

AUDIENCE: General public.

AFFILIATIONS: Oversees 22-agency task force of state, federal, and county law enforcement; also collaborates with Children’s Justice Center of Hawaii, Missing Child Center Hawaii, Sex Abuse Treatment Center, probation and parole agencies.

DEPARTMENT OF THE ATTORNEY GENERAL

Criminal Justice Division

Medicaid Fraud Control Unit (MFCU)

333 Queen Street, 10th Floor, Honolulu, HI 96813

PHONE: (808) 586-1058

FAX: (808) 586-1077

DESCRIPTION: Investigates allegations of provider fraud committed against the State Medicaid program, and patient abuse and neglect allegations against licensed and non-licensed care providers. Prosecutes confirmed allegations both criminally and civilly.

AUDIENCE: General public, seniors, Medicaid beneficiaries, health care providers.

AFFILIATIONS: State, federal and county law enforcement; State Department of Health, and State Department of Human Services.

DEPARTMENT OF THE ATTORNEY GENERAL

Tax Division

425 Queen Street, Honolulu, HI 96813

PHONE: (808) 586-1470

FAX: (808) 586-1477

WEBSITE: www.hawaii.gov/ag/charities

DESCRIPTION: The Tax Division provides legal representation and advice to the Department of Taxation in the areas of tax litigation, legislation, rules, investigations, and opinions and advice. The division contains an informal bankruptcy unit devoted to handling all bankruptcy cases for the Department of Taxation, and occasionally assists other agencies in bankruptcy matters. The division provides oversight and enforcement of laws pertaining to charitable trusts, public charities, public benefit corporations, and private foundations.

The division is also responsible for the department's registration and bonding function for professional solicitors and professional fundraising counsels under Chapter 467B of the Hawaii Revised Statutes, and the enforcement of the State's charitable solicitation laws. The division is also the custodian of certifications by charities that issue charitable gift annuities under section 431:204(b) of the Hawaii Revised Statutes.

AUDIENCE: Donors, nonprofit directors and officers and their legal advisors, professional fundraisers.

AFFILIATIONS: National Association of State Charity Officials (NASCO), www.nasconet.org.

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)

Consumer Education Program

King Kalakaua Building, 335 Merchant Street, Honolulu, HI 96813

Leiopapa A Kamehameha Building, 235 S. Beretania Street, Honolulu, HI 96813

WEBSITE: www.hawaii.gov/dcca

DESCRIPTION: Provides consumer education information statewide to Hawaii residents to help them make wise choices in today's ever-changing marketplace. Sponsors the Consumer Education Fair (February), LifeSmarts Consumer Education Competition (September – April), Money Smart financial education program, and senior fairs and community events throughout the state (year round).

AUDIENCE: General public.

CONSUMER INFORMATION LINE

PHONE: (808) 587-1234

NEIGHBOR ISLAND: To contact the Consumer Information Line, residents may call the following numbers, followed by 7-1234 and the **#** key: Hawaii (808) 974-4000, Kauai (808) 274-3141, Maui (808) 984-2400, Lanai & Molokai toll-free 1-800-468-4644.

Press **1**: For Landlord-Tenant Information

Press **2**: For Consumer Dial Messages

Press **3**: For DCCA Hours of Service

DESCRIPTION: 24-hour, automated response and fax-back system that contains pre-recorded consumer messages and DCCA departmental information.

OFFICE OF CONSUMER PROTECTION DIVISION (OCP)

PHONE: (808) 586-2630

NEIGHBOR ISLAND: To contact the OCP office, residents may call the following numbers, followed by 6-2630 and the **#** key: Hawaii (808) 974-4000, Kauai (808) 274-3141, Maui (808) 984-2400, Lanai & Molokai toll-free 1-800-468-4644.

E-MAIL: ocp@dcca.hawaii.gov

WEBSITE: www.hawaii.gov/dcca/areas/ocp

OFFICE HOURS: Monday-Friday, 7:45 a.m. to 4:30 p.m., except state holidays.

DESCRIPTION: Investigates consumer complaints alleging unfair or deceptive business practices.

LANDLORD-TENANT CODE INFORMATION LINE

PHONE: (808) 586-2634

NEIGHBOR ISLAND: To contact the Landlord-Tenant Code Information Line, residents may call the following numbers, followed by 6-2634 and the **#** key: Hawaii (808) 974-4000, Kauai (808) 274-3141, Maui (808) 984-2400, Lanai & Molokai toll-free 1-800-468-4644.

PHONE HOURS: Monday-Friday, 8:00 a.m. to 12:00 p.m., except state holidays.

WEBSITE: www.hawaii.gov/dcca/areas/ocp/landlord_tenant

DESCRIPTION: Call for information on landlord-tenant matters.

REGULATED INDUSTRIES COMPLAINTS OFFICE DIVISION (RICO)

PHONE: (808) 586-2666

NEIGHBOR ISLAND: To contact the RICO office, residents may call the following numbers, followed by 6-2666 and the [#] key: Hawaii (808) 974-4000, Kauai (808) 274-3141, Maui (808) 984-2400, Lanai & Molokai toll-free 1-800-468-4644.

OFFICE HOURS: Monday-Friday, 7:45 a.m. to 4:30 p.m., except state holidays.

E-MAIL: rico@dcca.hawaii.gov

WEBSITE: www.hawaii.gov/dcca/areas/rico

DESCRIPTION: Investigates and prosecutes complaints relating to industries regulated by the DCCA.

CONSUMER RESOURCE CENTER

PHONE: (808) 587-3222

TOLL-FREE: 1-800-394-1902

TELEPHONE HOURS: Monday-Friday, 7:45 a.m. to 4:30 p.m., except state holidays.

WEBSITE: www.hawaii.gov/dcca/quicklinks/consumer_resource_center

DESCRIPTION: Call for license verification and complaint history of professionals or businesses, information on identity theft, and other general consumer information.



DCCA ONLINE SERVICES

WEBSITE: <http://www.hawaii.gov/dcca/quicklinks/online/>

DESCRIPTION: Search on-line for business license and complaint history. Additional searches available: business name, certificate of good standing, various business filings, and insurance and professional/vocational license renewal.

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA) Business Registration Division (BREG) Business Action Center (BAC)

OAHU: 1130 North Nimitz Highway, Suite A-220, Honolulu, HI 96817

MAUI: 70 E. Kaahumanu Avenue, Unit B-9, Kahului, HI 96732

PHONE: Oahu (808) 586-2545; Maui (808) 873-8247

NEIGHBOR ISLAND: To contact the Oahu BAC Office, neighbor island residents may call the following numbers, followed by 6-2545 and the key: Hawaii (808) 974-4000, Kauai (808) 274-3141, Maui (808) 984-2400, Lanai & Molokai toll-free 1-800-468-4644.

FAX: (808) 586-2544 (Oahu) or (808) 871-9160 (Maui)

E-MAIL: bac@dcca.hawaii.gov

WEBSITE: www.hawaii.gov/dcca

DESCRIPTION: Offers business counseling services to startup or expanding businesses in the state and provides information on state filing requirements in the areas of business, labor, and tax. Serves as an information clearinghouse that provides general information on state and federal laws and rules, county ordinances and financial assistance programs related to business or commerce activities. Participates in business fairs, workshops, and other outreach events in conjunction with various federal, state, and county agencies as well as nonprofit educational programs.

AUDIENCE: General public.

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)
Business Registration Division (BREG)
Office Of The Securities Commissioner (OSC)

335 Merchant Street, Suite 203, Honolulu, HI 96813

OFFICE HOURS: Monday-Friday, 7:45 a.m. to 4:30 p.m., except state holidays.

WEBSITE: www.investing.hawaii.gov

INVESTOR EDUCATION PROGRAM (IEP)

PHONE: (808) 587-7400

DESCRIPTION: Provides practical and current information to assist the community statewide with making wise choices when investing, increasing their financial literacy and improving their ability to identify and avoid investor scams and schemes. Hosts Financial Literacy Fair (April) and participates in statewide community fairs and events. Call for more ways to protect yourself.

SECURITIES COMPLIANCE BRANCH (SEC)

PHONE: (808) 586-2722

DESCRIPTION: Registers securities sellers and advisers. Call to check if your adviser or broker is registered and has a delinquent history.

SECURITIES ENFORCEMENT BRANCH (SEB)

PHONE: (808) 586-2740

TOLL-FREE: 1-877-447-2267

DESCRIPTION: Investigates and takes legal action on violations of Hawaii securities laws. Report investment fraud to the Securities Enforcement Branch.

AUDIENCE: General public.

AFFILIATIONS: AARP, Financial Industry Regulation Authority (FINRA) (formerly known as NASD), Hawaii Council on Economic Education (HCEE), Investor

Protection Trust (IPT), North American Securities Administrators Association, Inc. (NASAA), United States Securities Exchange Commission (SEC).

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA) Insurance Division Insurance Fraud Investigation Branch

335 Merchant Street, Suite 213, Honolulu, HI 96813

PHONE: (808) 586-2790

FAX: (808) 586-2806

E-MAIL: insurance@dcca.hawaii.gov

WEBSITE: www.hawaii.gov/dcca/ins

DESCRIPTION: Oversees the Hawaii insurance industry, issues licenses, examines the fiscal condition of Hawaii-based companies, reviews rate and policy filings, investigates insurance-related complaints.

AUDIENCE: General public.

MOTOR VEHICLE INSURANCE FRAUD HOTLINE

PHONE: (808) 587-7416

NEIGHBOR ISLAND: To contact the Motor Vehicle Insurance Fraud Hotline, residents may call the following numbers, followed by 7-7416 and the **#** key: Hawaii (808) 974-4000, Kauai (808) 274-3141, Maui (808) 984-2400, Lanai & Molokai toll-free 1-800-468-4644.

OFFICE HOURS: Monday-Friday, 7:45 a.m. to 4:30 p.m.

WEBSITE: www.hawaii.gov/dcca/areas/ins/other_ins/

DESCRIPTION: Call to report actual or suspected insurance fraud.

EXECUTIVE OFFICE ON AGING

No. 1 Capitol District, 250 S. Hotel Street, Suite 406, Honolulu, HI 96813

PHONE: (808) 586-0100 **FAX:** (808) 586-0185

E-MAIL: eoah@doh.hawaii.gov **WEBSITE:** www4.hawaii.gov/eoa/

SMP HAWAII PROGRAM (FORMERLY SAGEWATCH)

PHONE: (808) 586-7281 **TOLL-FREE:** 1-800-296-9422

DESCRIPTION: Since 1997, SMP Hawaii has been providing education to Hawaii's Medicare members and Medicaid recipients, their families, and their caregivers about prevention of fraud and abuse in the Medicare/Medicaid programs.

SAGE PLUS PROGRAM

PHONE: (808) 586-7299

TOLL-FREE: 1-888-875-9229 or 1-866-810-4379 (TTY)

DESCRIPTION: The State Health Insurance Assistance Program (SHIP) is for people with Medicare. The volunteer based program assists individuals with questions about Medicare benefits, Medicare Advantage Program, Long-Term Care Financing, Medicare Part D – the prescription drug benefit, and appeals to Medicare and health plans.

HAWAII CREDIT UNION LEAGUE

1654 S. King Street, Honolulu, HI 96826-2097

PHONE: (808) 941-0556

TOLL-FREE: 1-888-331-5646

FAX: (808) 945-0019

E-MAIL: info@hcul.org

WEBSITE: www.hcul.org

DESCRIPTION: Training credit union personnel to prevent elder financial abuse through workshops dealing with how to identify and handle common abusive practices. The workshops can be adapted for delivery directly to elder members if requested by credit unions.

AUDIENCE: Credit union personnel and elder credit union members.

AFFILIATIONS: Credit Union National Association (CUNA), www.cuna.coop, National Endowment for Financial Education (NEFE), www.nefe.org.

KHON2/ACTION LINE

88 Piikoi Street, Honolulu, HI 96814

PHONE: (808) 591-0222

FAX: (808) 591-4276

WEBSITE: www.KHON2.com

DESCRIPTION: Volunteers answer consumer complaint assistance calls, guiding callers through the resolution of their problems with on-going support, suggestions, information, referrals, and education. Supported by stories airing on KHON2 to help educate and protect consumers from scams, fraud, and unethical business practices.

HONOLULU STAR-BULLETIN

Kokua Line

500 Ala Moana Boulevard, No. 7-210, Honolulu, HI 96813

PHONE: (808) 529-4773

FAX: (808) 529-4750

EMAIL: kokualine@starbulletin.com

WEBSITE: www.starbulletin.com

DESCRIPTION: Kokua Line attempts to find answers to everyday complaints or interesting questions; alert consumers to scams; and give useful information to help people resolve their problems. It also gives Star-Bulletin readers a chance to vent their frustrations or say mahalo to someone for an unexpected kindness.



National Resources

ANNUAL CREDIT REPORT REQUEST SERVICE

P.O. Box 105283, Atlanta, GA 30348-5283

TOLL-FREE: 1-877-322-8228

WEBSITE: www.annualcreditreport.com

DESCRIPTION: AnnualCreditReport.com is the only web source authorized by all three nationwide Consumer Credit Reporting Companies—Equifax, Experian and TransUnion—from which free annual credit file disclosures can be requested.

DIRECT MARKETING ASSOCIATION (DMA)

Mail Preference Service

P. O. Box 282, Carmel, NY 10512-0282

PHONE: (202) 955-5030

FAX: (202) 955-0085

WEBSITE: www.dmachoice.org/MPS/

DESCRIPTION: The Direct Marketing Association (DMA) Mail Preference Service removes your name and address from prospect mailing lists to decrease the amount of junk mail received.

FEDERAL BUREAU OF INVESTIGATION (FBI)

Hawaii Division

Prince Jonah Kuhio Kalanianaʻole Federal Building, 300 Ala Moana Boulevard, Honolulu, HI 96850-0053

PHONE: (808) 566-4300

TOLL-FREE: 1-800-732-0330

FAX: (808) 566-4470

E-MAIL: honolulu@fbi.gov

WEBSITE: honolulu.fbi.gov (do not type in www)

DESCRIPTION: Investigates federal crimes of fraud, theft, or embezzlement occurring within or against the national or international financial community.

FEDERAL TRADE COMMISSION (FTC)

Identity Theft Clearinghouse

600 Pennsylvania Avenue, N.W., Washington, DC 20580

TOLL-FREE: 1-877-438-4338 or 1-866-653-4261 (TTY)

WEBSITE: www.ftc.gov

DESCRIPTION: The Federal Trade Commission (FTC) is the only agency with both consumer protection and competition jurisdiction in broad sectors of the economy. They provide a place for citizens to report consumer complaints that help the FTC to investigate frauds that in some cases lead to law enforcement action.

FEDERAL TRADE COMMISSION (FTC)

National Do Not Call Registry

600 Pennsylvania Avenue, N.W., Washington, DC 20580

TOLL-FREE: 1-888-382-1222 or 1-866-290-4236 (TTY)

WEBSITE: www.donotcall.gov

DESCRIPTION: The free FTC National Do Not Call Registry will stop most telemarketing calls to your home or mobile phone. Most telemarketers should not call your number once it has been on the registry for 31 days. If they do, you can file a complaint by visiting the website.

FINANCIAL INDUSTRY REGULATION AUTHORITY (FINRA) (formerly known as NASD) District 1 — San Francisco

One Montgomery Street, Suite 2100, San Francisco, CA 94104

PHONE: (415) 217-1100

FAX: (415) 956-1931

WEBSITE: www.finra.org

DESCRIPTION: The Financial Industry Regulation Authority (FINRA) is the largest non-governmental regulator for all securities firms doing business in the United States. If you believe you have been defrauded or treated unfairly by a securities professional or firm, please send a written complaint via mail or fax to FINRA Complaints and Tips. See above for address and fax number.

NATIONAL CRIME PREVENTION COUNCIL (NCPC)

2345 Crystal Drive, Fifth Floor, Arlington, VA 22202-4801

PHONE: (202) 466-6272

FAX: (202) 296-1356

WEBSITE: www.ncpc.org and mcgruff.org

DESCRIPTION: Produces tools including publications and teaching materials on a variety of topics, that communities can use to learn crime prevention strategies, engage community members, and coordinate with local agencies.

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC. (NASAA)

750 First Street, N.E., Suite 1140, Washington, DC 20002

PHONE: (202) 737-0900

FAX: (202) 783-3571

FAX ON DEMAND: 1-888-846-2722

E-MAIL: info@nasaa.org

WEBSITE: www.nasaa.org

DESCRIPTION: Organized in 1919, the North American Securities Administrators Association (NASAA) is the oldest international organization devoted to investor protection. NASAA members license firms and their agents, investigate violations of state and provincial law, file enforcement actions when appropriate, and educate the public about investment fraud.

OPT OUT PRESCREEN.COM

P.O. Box 600344, Jacksonville, FL 32260

TOLL-FREE: 1-888-567-8688

WEBSITE: www.optoutprescreen.com

DESCRIPTION: Enrollment to “Opt-Out” of pre-approved offers of credit or insurance from lists supplied by Equifax, Experian, Innovis, and TransUnion.

UNITED STATES AIR FORCE Office of Special Investigations Detachment 601 Joint Fraud Program

265 McClelland Drive, Hickam Air Force Base, HI 96853

PHONE: (808) 449-0259

FAX: (808) 448-0908

DESCRIPTION: The United States Air Force Office of Special Investigations' (AFOSI) overall mission is to identify, exploit and neutralize criminal, terrorist, and intelligence threats to the United States Air Force, Department of Defense and the United States Government. Regarding fraudulent activities, AFOSI brings to bear a wide range of resources, including technological services and specialized techniques to investigate crimes perpetrated against, or by, members of the United States Air Force.

UNITED STATES ATTORNEY'S OFFICE

District of Hawaii

300 Ala Moana Boulevard, Suite 6-100 Honolulu, HI 96850

PHONE: (808) 541-2850

FAX: (808) 541-2958

WEBSITE: www.usdoj.gov/usao/hi/

DESCRIPTION: The U.S. Attorney's Office handles federal criminal prosecution on identity theft, fraud and financial abuse of the elderly. It also has a community outreach program that attends neighborhood meetings, talks, trainings, and school lectures regarding awareness and prevention of abuse. At times, other federal law enforcement agencies participate in this community outreach program.

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

Medicare

Centers for Medicare & Medicaid Services

7500 Security Boulevard, Baltimore, MD 21244

TOLL-FREE: 1-800-633-4227 or 1-877-486-2048 (TTY)

WEBSITE: www.medicare.gov

DESCRIPTION: Provides information and assistance to the public on Medicare benefits, complaints, appeals, and fraud and abuse in the Medicare system.

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

Office of the Inspector General (OIG)

P.O. Box 23489, Washington, D.C. 20026

TOLL-FREE: 1-800-447-8477 or 1-800-377-4950 (TTY)

TELEPHONE HOURS: Monday-Friday, 8:00 a.m. to 5:30 p.m., Eastern Time.

FAX: 1-800-223-8164

E-MAIL: HHSTips@oig.hhs.gov

WEBSITE: www.oig.hhs.gov

DESCRIPTION: Operates a hotline to receive calls concerning fraud against programs of the department such as Medicare Part-A and Medicare Part-B, and crimes involving departmental employees and contractors.

UNITED STATES DEPARTMENT OF JUSTICE

Office of the Inspector General (OIG)

Investigations Division

950 Pennsylvania Avenue, N.W., Room 4706, Washington, DC 20530

TOLL-FREE: 1-800-869-4499

FAX: (202) 616-9881

E-MAIL: oig.hotline@usdoj.gov

WEBSITE: www.usdoj.gov/oig/

DESCRIPTION: Conducts independent investigations, audits, inspections, and special reviews of United States Department of Justice personnel and programs to detect and deter waste, fraud, abuse, and misconduct, and to promote integrity, economy, efficiency, and effectiveness in Department of Justice operations.

UNITED STATES DEPARTMENT OF THE TREASURY

Go Direct Processing Center — MS/GDW

P. O. Box 650527, Dallas TX 75265-0527

TOLL-FREE: 1-800-333-1795

WEBSITE: www.godirect.gov

DESCRIPTION: Enrollment for direct deposit of your Social Security, Supplemental Security Income (SSI), Veterans, Railroad Retirement or Civil Service Benefits.

UNITED STATES POSTAL INSPECTION SERVICE

P.O. Box 30309, Honolulu, HI 96820-0309

TOLL-FREE: 1-877-876-2455

Press **3**: for Mail Theft

Press **4**: for Mail Fraud

FAX: (808) 422-2496

WEBSITE: postalinspectors.uspis.gov

DESCRIPTION: The United States Postal Inspection Service's mission is to protect the U.S. Postal Service, secure the mail system, and ensure public trust in mail. Enforces over 200 federal laws in investigations of crimes that affect or fraudulently use the U.S. Mail, the postal system, or postal employees. Presentations to communities on mail theft, mail fraud, ID theft, and crime prevention topics are available.

UNITED STATES SECRET SERVICE

Hawaii Office

Prince Jonah Kuhio Kalaniana'ole Federal Building, 300 Ala Moana Boulevard, Suite 6-210, Honolulu, HI 96850

PHONE: (808) 541-1912

FAX: (808) 545-4490

WEBSITE: www.secretsservice.gov

DESCRIPTION: Investigates financial and identity theft crimes such as bank fraud, access device fraud, false identification fraud, and identity theft.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION (SEC) Office of Investor Education and Advocacy Investor Complaint Center

100 F Street, N.E., Washington, DC 20549-0213

PHONE: (202) 551-6551

TOLL-FREE: 1-800-732-0330

FAX: (202) 772-9395

E-MAIL: help@sec.gov

WEBSITE: www.sec.gov/complaint.shtml

DESCRIPTION: If you encounter a problem with an investment or have a question, you can contact the SEC's Office of Investor Education and Advocacy.

UNITED STATES SOCIAL SECURITY ADMINISTRATION (SSA) Honolulu Office

Prince Jonah Kuhio Kalaniana'ole Federal Building, 300 Ala Moana Boulevard, Suite 1-114, Honolulu, HI 96850

TOLL-FREE: 1-800-772-1213 or 1-800-325-0778 (TTY)

WEBSITE: www.ssa.gov

DESCRIPTION: Provides a place for citizens to request a Social Security statement, to report theft or fraudulent use of their Social Security number, and to send their Social Security benefits directly to their bank.

OFFICE HOURS: Monday-Friday, 8:30 a.m. to 3:30 p.m.



GLOSSARY

Anti-Spyware Software: Computer program that detects and removes spyware from your computer.

Anti-Virus Software: Computer program that attempts to identify and block or eliminate computer viruses and other malicious software (or malware).

Bidz: On-line auction and shopping website in which people and businesses buy and sell goods and services worldwide.

Consumer: A person who purchases goods and services for personal use.

eBay: On-line auction and shopping website in which people and businesses buy and sell goods and services worldwide.

E-mail: Short for electronic mail, e-mail is a method of sending messages across a computer network, whether simply across the office or around the world. The text of the message is typed in on one computer and then sent to someone else's computer.

Equifax: A consumer credit reporting agency.

Experian: A consumer credit reporting agency.

External Hard Drive: An external device attached to the computer with a cable, used to store data. This may include programs and files (e.g., documents, photos, music, video, etc.)

Federal Trade Commission (FTC): A federal agency that deals with issues affecting American consumers' lives. It is the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy. FTC does not resolve individual consumer problems, but consumer complaints help FTC investigate fraud and can lead to law enforcement action.

Firewall: A protective software program and/or hardware device that shields a computer on a network from external attack.

Fraud: Deceit, trickery, or breach of confidence perpetrated for profit or to gain some unfair or dishonest advantage.

Fraud Alert: A "flag" that is placed on your credit report through the consumer reporting agencies — Equifax, Experian, and TransUnion.

Fraudulent Account: An account opened using personal information or identifying documents of an individual without his or her knowledge, permission or authorization.

FTC Consumer Complaint Form: A form used to submit complaints to the Federal Trade Commission Bureau of Consumer Protection about a particular company or organization.

Hack: The term is often used to indicate that a computer's security and/or software have been compromised, most times without the owner/user's permission or knowledge. The term is also used to indicate that a piece of technology has been altered in some way, which may make the technology easier to use or to make it inoperable.

Hotmail: A free web-based electronic mail service provided by the Microsoft Corporation.

HTTPS or Hypertext Transfer Protocol Security: Hypertext Transfer Protocol over Secure Socket Layers (HTTPS) is a protocol that ensures a secure connection and is usually used by e-commerce sites where credit card transactions are required or personal data is exchanged.

Identity Theft: Stolen confidential personal information of another person is used to commit crimes including theft, fraud, or forgery.

Identity Theft Affidavit: A form used to report the general information about yourself and the identity theft. The Fraudulent Account Statement form accompanies the Identity Theft Affidavit. Only for use where a new account was opened in the victim's name.

Internet Service Provider (ISP): A business that provides an individual with access to the Internet. Some methods of providing this service are through dial-up telephone, cable, or high-speed DSL circuit.

Kupuna: Grandparent, respected elder, ancestor.

Malware: Short for malicious software, a program or file that is designed to damage or disrupt a system, such as a virus, worm, Trojan horse, or some pop-up ads. This may result in someone stealing your identity.

Miscellaneous Public (Misc. Pub.): A police form used to document non-criminal cases.

PayPal: PayPal is an e-commerce business allowing payments and money transfers to be made through the Internet. It serves as an electronic alternative to traditional paper methods such as checks and money orders. It is the most popular way to conduct financial transactions via the Internet.

Personal Identification Number (PIN): Private access code or password, which is often used for ATMs and debit cards.

Personal Information: Information associated with an actual person or a fictitious person that is a name, an address, a telephone number, an electronic mail address, a driver's license number, a Social Security number, an employer, a place of employment, information related to employment, an employee identification number, a mother's maiden name, an identifying number of a depository account, a bank account number, a password used for accessing information, or any other name, number, or code that is used, alone or in conjunction with other information, to confirm the identity of an actual or a fictitious person.

Phishing: The act of falsely claiming to represent an established, legitimate company in an attempt to scam its customers into surrendering private information that will be used for identity theft.

Scam: A confidence game or other fraudulent scheme, especially for making a quick profit; swindle.

Secure Sockets Layer Certification: A cryptographic protocol which provides secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging, and other data transfers. It is identified by an image of a secure padlock on the tool bar at the bottom of the screen and is usually used in conjunction with HTTPS.

Software: A collection of computer programs, procedures, and documentation that perform some task on a computer system.

Spyware: Software, typically installed on your computer without your permission, that can track the user's downloads, web surfing habits, and individual key strokes. It serves as an unauthorized entry point for a remote user, or to transfer information to an external source.

Third Party Payment Service (TPPS): An online service to transfer money into an online account and make payments from that account, where you may: 1) make purchases on online auction sites, 2) purchase products from online retail sites, 3) donate money to different causes, and 4) send money to anyone with an e-mail account (certain services only). Payments are made without exposing your real credit card and bank account numbers.

TransUnion: A consumer credit reporting agency.

TRUSTe: An independent non-profit organization which certifies thousands of websites adhering to strict privacy standards.

Uniform Resource Locator (URL): Refers to the formal address of a document on the Internet. For example, <http://www.ftc.gov>.

Virus: Computer program that can copy itself and infect a computer without permission or knowledge of the user.

Website: A computer connected to the Internet that maintains a series of web pages on the World Wide Web.

Wiping Program: A computer program that allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.

Yahoo Mail: A free web-based electronic mail service.

MAHALO TO THE WORKING GROUP:

AARP Hawaii
ALU LIKE, Inc.
Better Business Bureau
Catholic Charities
CyberW0rx.8o8, LLC
Department of the Attorney General
Department of Commerce and Consumer Affairs
Department of Human Services
Department of the Prosecuting Attorney
Elderly Affairs Division, City & County of Honolulu
Executive Office on Aging
Federal Bureau of Investigation
First Hawaiian Bank
Hawaii Bankers Association
Hawaii County Office of Aging
Hawaii County Police Department
Hawaii Credit Union League
Hawaii Government Employees Association
Hawaii State Federation of Chapters-NARFE
Honolulu Police Department
Honolulu Star-Bulletin Kokua Line
Kauai Agency on Elderly Affairs
Kauai Police Department
KHON2 Action Line
Maui County Office on Aging, Elderly Affairs Division
Maui Police Department
Office of the Prosecuting Attorney, County of Hawaii
Office of the Prosecuting Attorney, County of Kauai
Office of the Prosecuting Attorney, County of Maui
United States Air Force, Office of Special Investigations
United States Attorney's Office
United States Postal Inspection Service



MAHALO

*Thank you to the following agencies
for their vision, partnership, and commitment to this guide.*

**Executive Office on Aging
SMP Hawaii Program**

**Department of Commerce and Consumer Affairs
Office of the Securities Commissioner**

**Department of the Attorney General
Crime Prevention and Justice Assistance Division**