Hawaii's

FRAUD PREVENTION & RESOURCE GUIDE

2ND EDITION

Hawaii's Fraud Prevention & Resource Guide 2nd Edition

LETTER FROM GOVERNOR DAVID IGE

Aloha! I am proud to introduce the second edition of Hawaii's Fraud Prevention & Resource Guide.

My administration is deeply committed to protecting our families, caring for our kupuna and providing for our keiki. As part of this ongoing effort, the Department of Commerce and Consumer Affairs, the Department of Health and the Department of the Attorney General have collaborated to produce this helpful guide, one of the most popular state anti-fraud resources.

Along with information on how to protect yourself against fraud and who to call to receive help, this guide describes some of the most common types of fraud in Hawaii to help consumers recognize and avoid them.

A big mahalo to the state agencies that worked together to develop this important resource for Hawaii consumers.

Mahalo nui loa,

David Ige
Governor of the State of Hawaii

Hawaii's Fraud Prevention & Resource Guide, 2nd Edition

This guide is provided by the Department of Commerce and Consumer Affairs, Office of the Securities Commissioner; Department of Health, Executive Office on Aging, Senior Medicare Patrol (SMP Hawaii) and the Department of the Attorney General, Crime Prevention and Justice Assistance Division.

Primary funding for this guide is provided by the State of Hawaii Department of Commerce and Consumer Affairs, Office of the Securities Commissioner with additional funding provided by the Department of Health, Executive Office on Aging, Senior Medicare Patrol (SMP Hawaii).

This guide was supported in part by Grant No. 90SP-0100-01 from the Administration on Aging (AoA), Administration for Community Living (ACL), U.S. Department of Health and Human Services (DHHS). Grantees carrying out projects under government sponsorship are encouraged to express freely their findings and conclusions. Therefore, points of view or opinions do not necessarily represent official AoA, ACL, or DHHS policy.

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.

October 2015

TABLE OF CONTENTS

INTRODUCTION 8
Tactics of Scam Artists 8

1 WAYS WE GET SCAMMED: METHODS 10
Internet 11
Social Networks 15
Mail 18
Person-to-Person 20
Phone 21

2 ADVANCE FEE FRAUD 23
Inheritance Scam 25
Foreign Money Transfer Scam 26
Lottery or Sweepstakes Scam 27

3 COMMON CONSUMER FRAUDS 31
Overpayment, Fake Refund and Fake Check Fraud 32
Charity Fraud 34
Construction and Home Repair 36
Solar Panels/Photovoltaic (PV) Panels 40
Rental Scam 44
Security Alarm System Fraud 46
Hearing Aid Dealers and Fitters 47
Car Repairs and Sales 47
Utility Company Scams 48
Purchasing Online 48
Check a Professional License and Complaint History for more than 48 Industries 49

4 IDENTITY THEFT 51
How Do Thieves Get Your Information? 52
What Kinds of Information Are Most Important to Protect? 57
What Should You Do If You Think Your Information Has Been Lost or Stolen? 57
If You Are a Victim of Identity Theft 58
If Your Child Is a Victim of Identity Theft 60
If You Are a Victim of Tax Identity Theft 60
How to Get Your FREE Credit Report 61

5 FINANCIAL FRAUD 62
Credit Card Fraud 63
Insurance Fraud 65
Investment Fraud 67
Ponzi Schemes 68
Affinity Fraud 72
Home Loan Fraud 73
Mortgage Reduction/Servicing or Debt Relief Fraud 76

6 HEALTHCARE AND MEDICARE FRAUD 79
Professional Licenses: Dentists, Nurses, Doctors 80
Medicare Fraud 80

7 KEEPING OUR KUPUNA (SENIORS) SAFE 87
Common Consumer Scams Against Kupuna 88
Talking Story with Our Kupuna 91
Ponzi and Affinity Fraud 92
Variable Annuities 94
Life Settlements 95
Indexed Annuities 97
Medicare 100

Charity 102
Kupuna Online 103
Caregivers 105
What is a Fiduciary 106
Different Types of Fiduciaries 107
Protecting our Kupuna 107
Where to Get Help for Kupuna and Caregivers 110

8 RESOURCES 113
County Resources
City and County of Honolulu 114
Hawaii County 115
Kauai County 117
Maui County 118
State Resources 120
National Resources 132

INTRODUCTION

Aloha. Welcome to the second edition of Hawaii's Fraud Prevention & Resource Guide. This guide is one of the first state multi-agency guides developed in the nation to focus on you, the consumer, and the many different popular frauds and scams trying to separate you from your hard-earned money. After publishing the first edition in 2008, we felt it was time to offer users an updated version.

In Hawaii, we have a local way of life that many of us cherish. It includes generosity, and deep bonds of family and friendship. Our sense of ohana is strong, but even in Hawaii, the darker sides of human nature lurk. Financial and consumer fraud happens right here in our islands, and they are not limited to a specific ethnicity, gender or age group. This guide was developed to introduce consumers to common scams happening in our islands today, to offer information on how to protect yourself and your family and to direct consumers to where to get help. Please take the time to read this guide. By protecting yourself and your family and reporting fraud, you can help make our islands safer and preserve the best parts of our way of life.

TACTICS OF SCAM ARTISTS

Scam artists tailor their pitch to match the psychological profiles of their targets. They work to find out what motivates you so they can take advantage of your resources and money. Here are some of the age-old tactics that scam artists use again and again.

Get to know these tactics so the next time anyone tries to use them on you, you know you're dealing with a hard sell and/or maybe even fraud.

COMMON PERSUASION TACTICS INCLUDE:

- Phantom Riches – dangling the prospect of wealth, enticing you with something you want but can't have. "These Hawaiian water systems are guaranteed to produce $6,800 per month in income."
- Source Credibility – trying to build credibility by claiming to be with a reputable firm, or to have a special credential or experience. "Believe me, as a senior vice president of XYZ Firm, I would never sell an investment that doesn't produce."
- Social Consensus – leading you to believe that other savvy investors have already invested. "This is how ___ got his start. I know it's a lot of money, but I'm in—and so is my mom and half of her church—and it's worth every dime."
- Reciprocity – offering to do a small favor for you in return for a big favor. "I'll give you a break on my commission if you buy now—half off."
- Scarcity – creating a false sense of urgency by claiming limited supply. "There are only two units left, so I'd sign today if I were you."

Source: FINRA. Fighting Fraud 101. Retrieved from http://www.finra.org/investors/avoid-fraud

HERE ARE TYPES OF SCAMS COVERED IN THIS GUIDE

- Affinity Fraud
- Car Repair
- Charity
- Construction & Home Repair
- Credit Card Fraud
- Foreign Money Transfer
- Health Care Insurance
- Hearing Aids
- Home Loans
- Inheritance
- Insurance
- Investment
- Lottery
- Mortgage
- Phishing
- Ponzi Schemes
- Rental Scams
- Utility

METHODS

WAYS WE GET SCAMMED:

METHODS

Scammers reach us through the Internet, social networks, mail, person-to-person, and phone. This section will describe each approach, some of the common risks and tips to protect yourself.

INTERNET

The evolution of the Internet has its advantages and disadvantages. It can improve our quality of life, but it can also put us at risk. Below, we discuss some of the ways scammers are using the Internet to perpetrate fraud.

IDENTITY THEFT

Identity theft was a problem even before the Internet, but identity theft happens faster and the threat is more widespread through the Internet. There are different ways your personal information can be stolen electronically. Some techniques used by identity thieves include hacking into computers that don't have a firewall, installing keystroke loggers or other malicious codes hidden in email attachments and hiding viruses in images, downloads or free software. For more information on Identity Theft, see page 51.

MALWARE

Malware, short for malicious software, includes any codes, scripts or other software that infect your computer to damage it, to take your private information and to gain access to your private system. It includes computer viruses, spyware, worms and many other malicious programs.

The most common ways to get infected with Malware are through downloading materials from the Internet, opening unsafe attachments sent by email, clicking on internet ads and surfing sites with flashy ads.

Beware of where you surf and what you download or open.

ADWARE

This is a type of malware used to run a good old fashioned scam. The scammer first secretly infects your computer through your

unsafe download or attachment. They place an ad in your system but disguise the ad so you do not suspect it. As you use your computer, a surprise pop up says "You have a virus. Call us immediately at 1-800-XXX-XXXX." This pop up looks like a genuine message from your computer system, not like an ad. You call the number and the person on the phone proceeds to scam you out of your credit card number and personal information and may even persuade you to give them remote access to your computer to help you "fix it."

Beware, don't call random pop up numbers. Don't let strangers remotely access your computer. To get help, take your computer to a local reputable store.

The Internet has led to scams uniquely suited for the fast pace of the Internet and the ease in which scammers can disguise their identities through email and social media. **HERE ARE SOME COMMON INTERNET SCAMS COVERED IN THIS GUIDE.**

- Advance Fee Fraud, page 23
- Nigerian Letter (also known as 419), page 26
- Phishing, page 52
- Purchasing Online, page 48

HELPFUL TIPS WHEN USING THE INTERNET

- Make passwords long, strong and unique. You should have a different password for each online account, using a combination of upper and lower case letters, numbers and symbols.
- Think before you act. Most organizations - banks, charities, universities, reputable companies, etc., will not

ask for personal information via email. Be wary of email requests to update or "confirm" your information.

- Post with caution. Information you post online, especially on social networking sites, can be collected and used to steal your identity. Keep information such as social security numbers, account numbers, birthdates and home addresses confidential.
- Own your online presence. Understand how privacy settings work on social networks and websites you frequent. Set them to your comfort level of sharing.

KEEP A CLEAN COMPUTER

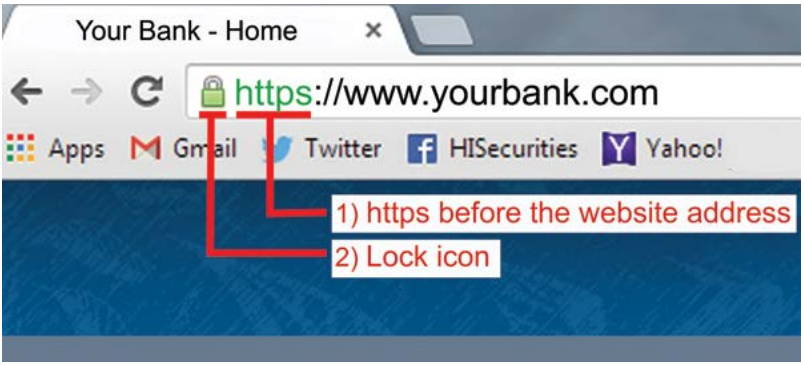
- Keep software updated. Install the latest security software, web browser and operating system on your computer. Enable the auto-update feature to ensure you have the most up-to-date security software.

PROTECT YOUR WIRELESS NETWORK

- Create a secure password for your wireless router.

CONNECT WITH CARE

- Check to make sure the URL is encrypted. When banking or shopping online, enter information only into security-enabled sites that begin with https://. The "s" means the data is encrypted in transit. Never enter bank or credit card information into a website that begins http://
- Check for the lock icon. The lock icon should be displayed in the URL bar, also known as the address bar.



BE WEB WISE

- When in doubt, throw it out. Links and attachments in emails, social media posts, and online ads are often how scammers gain access to your computer. If you are instructed to click a link or attachment in a message you don't trust, even if you know the sender, delete the message or mark it as junk mail.
- Back it up. Store valuable work, photos, music and other information on a backup hard drive and online in the "cloud."
- If you have been a victim of a cybercrime, file a complaint with the Internet Crime Complaint Center at www.victimvoice.org

Source: Multi-State Newsletter. Keeping Senior Citizens Safe Online.
http://msisac.cisecurity.org/newsletters/2013-06.cfm

INTERNET: SOCIAL NETWORKS

Internet social networking describes web-based online applications that allow users to interact and connect with groups of people, all at once, over the Internet. Participants can post text, videos and pictures that are viewable by other users anywhere throughout the world. Some examples of Internet social networks are Facebook, LinkedIn, Instagram, and Twitter.

Many users of online social networks post too much personal information online. Scammers can take advantage of all the background and personal information shared online and use it to make a skillful and highly targeted pitch to scam the potential victim. The scam can spread rapidly through a social network as the scammer gains access to the friends and colleagues of the initial victim.

Users of social media should be careful about posting personal information, vacation times or other details about when they are away from home. This information can lead to burglary and other crimes. Users of social media should also consider privacy settings to limit who can access private posts.

AFFINITY FRAUD AND SOCIAL NETWORKING

Social networks and the Internet have made it easier than ever to connect with others that share a common interest whether it is based on hobbies, lifestyle, faith, career advancement or business interest. Strong bonds can develop quickly within these groups. Because of this, scammers can quickly and thoroughly infiltrate groups and scam them. Scams that leverage group loyalties and relationships are a form of Affinity Fraud.

Once the bond has been established, the scammer enlists their potential victim to donate money to a particular cause or charity that is nonexistent or invest in a sketchy enterprise. Beware, don't let emotions override your own common sense.

COMMON INTERNET SOCIAL NETWORK SCAMS

- Identity Theft, page 51
- Nigerian Letter (also known as 419), page 26

HELPFUL TIPS WHEN USING SOCIAL NETWORKS

- Be careful of what you share. Limit posting personal information. Don't post banking information and information such as full birthdates, mother's maiden name, vacation dates, social security numbers and full home addresses.
- Be skeptical when approached by someone you don't know.

- Don't let your guard down just because they are a friend of a friend. Let the relationship develop slowly and try to be neutral when you assess investment opportunities.
- Don't open or download attachments from strangers or suspicious posts.

RED FLAGS FOR INTERNET SCAMS

Online investment fraud has many of the same characteristics as offline investment fraud. Learn to recognize these red flags:

- Promises of high returns with no risk. Many online scams promise unreasonably high short-term profits. Guarantees of returns around 2 percent a day, 14 percent a week or 40 percent a month are too good to be true. Remember that risk and reward go hand in hand.
- Offshore operations. Many scams are headquartered offshore, making it more difficult for regulators to shut down the scam and recover investors' funds.
- E-Currency sites. If you have to open an e-currency account to transfer money, use caution. These sites may not be regulated, and the scammer can use them to cover up the money trail.
- Recruit your friends. Many con artists will offer bonuses if you recruit your friends into the scheme.
- Professional websites with little or no information. These days, anyone can put up a website. Scam sites may look professional, but be suspicious if they offer little to no

information about the company's management, location or details about the investment

- No written information. Online scam promoters often fail to provide a prospectus or other form of written information detailing the risks of the investment and procedures to get your money out.

Source: NASAA. Social Networking. Retrieved from http://www.nasaa.org/wp-content/uploads/2011/09/NASAA_Advisory_Social-Networking.pdf

MAIL

IDENTITY THEFT

People send and receive mail on a daily basis, and our mail contains information that identity thieves want. For example, bank statements, utility bills, credit card bills, credit card offers, and blank checks contain account information that the thieves can use to assume your identity or gain access to your

money. The methods identity thieves use to steal mail are not sophisticated. Mail thieves will steal mail from your garbage, your mail box, or anywhere they can find your mail. They target neighborhoods by observing the time mail is delivered, the presence or absence of residents at a particular time, and if the red flag on the mailbox is raised. For more information about protecting your personal mail or mail fraud, call the U.S. Postal Inspection Service at 1-877-876-2455, and say "Mail Fraud."

HELPFUL TIPS FOR PREVENTING MAIL FRAUD

- Place all outgoing mail in a secure, locked United States Postal Services mail 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 that contains personal information.
- Monitor your monthly bills and financial statements. Contact the companies if you are missing your monthly bill or financial statement.
- To stop receiving junk mail, visit dmachoice.org or call 1-888-567-8688.
- To "Opt-Out" of unsolicited commercial mail, go to dmachoice.org or write to P. O. Box 643 Carmel, NY 10512.
- To "Opt-Out" of pre-approved offers of credit or insurance, go to optoutprescreen.com or call 1-888-567-8688 or write to P. O. Box 2033-A Rock Island, IL 61204-2033.

Below are some of the common and well known scams perpetrated through the mail.

COMMON MAIL SCAMS

- Charity Fraud Scams, page 34
- Lottery/Sweepstakes Scams, page 27
- Inheritance Scam, page 25

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.

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 or to steal your information or money. Scammers use

their communication skills to gain your trust and elicit information from you.

Often a person-to-person fraud starts through a free lunch or dinner seminar that involves props, fake documents, or the inappropriate solicitation of attendees to invest in a scam.

HELPFUL TIPS FOR PREVENTING PERSON-TO-PERSON FRAUD

- Give yourself time to research the person and the company before you invest.
- Check the license or registration of anyone who purports to be a professional.
- Remember — it's okay to say "no." It can be really hard to say "no" to someone face-to-face. But it is your money and you have the right to protect it.

PHONE

IDENTITY THEFT

Scammers often use pay phones, cell phones, or Voice Over Internet Protocol (VoIP) to carry out their schemes and to scam their potential victims out of money or steal their personal information. For example, the targeted victims may receive a text or voice message that appears to be from a financial institution or bank asking the consumer to text back or call to confirm account information or other personal information. This type of scam is called "phishing" because the scammer is trying to "fish" for your information. The best way to handle "phishing" is to not respond. See page 52 for more information.

COMMON PHONE SCAMS

- Lottery/Sweepstakes Scams, page 27
- Identity Theft, page 51
- Nigerian Letter Scams (also known as 419 Scam), page 26

HELPFUL TIPS FOR PREVENTING PHONE SCAMS

- Do not respond to a text or call from an unknown number that is requesting personal account numbers, social security numbers or any other personal information.
- Do not provide any personal information over the phone unless you initiated the call and are certain of who you contacted.
- If the caller makes you feel uncomfortable, hang up the phone.
- To reduce telemarketing calls on your home and cell phone, go to donotcall.gov or call 1-888-382-1222 or 1-866-290-4236 (TTY).

ADVANCE FEE FRAUD

Advance Fee Fraud is a scam where the victim believes paying an advanced fee will lead to a big windfall payment. It is also known as a confidence trick, in which the target or victim is persuaded to send small sums of money in advance in the hopes of realizing a much larger gain.

Advance fee fraud tends to have some or all of the following characteristics:

- The proposals are unsolicited.
- Urgency and secrecy of the deal.
- Victim is asked to pay upfront fees for processing, legal expenses, taxes or government fees in order to get a large windfall such as an inheritance, lottery win, or bank account sum to be released to the victim.

ADVANCE FEE

RED FLAGS FOR ADVANCE FEE FRAUD

Learn to recognize these red flags:

- You receive an offer from someone you do not know for a huge sum of money based on some outlandish story.
- You are asked to provide money up front for a processing fee, legal costs, transfer fees or some other cost in order for you to receive a huge sum of money.
- You are promised huge sums of money for little or no effort on your part.
- 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 and secrecy.
- 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).
- You receive an email from a distant country to which you have few or no ties.
- You receive an email with a lot of misspellings and stilted or poor English.
- You receive an email that "begs" for help to get money "unstuck."

HELPFUL TIPS FOR PREVENTING ADVANCE FEE FRAUD

- If you get an email from an unknown long lost relative, foreign diplomat or executive that needs your help to release millions of dollars to you, delete it. Do not reply.
- Do not make any advance payments upfront based on the hope of getting a big windfall. Scammers use the promise of future millions to distract you and separate you from your money.
- Be careful when a letter states "Confidential" or "Top Secret." Unless you actually work for the CIA or in that kind of business, this email is probably part of a scam.
- Do not provide your personal information to strangers over the Internet.
- Do not click on attachments or links in suspicious emails.
- If you've been scammed, call and report it to your local police department, the DCCA Office of Consumer Protection at (808) 586-2630, and the FBI at (808) 566-4300.

INHERITANCE SCAM

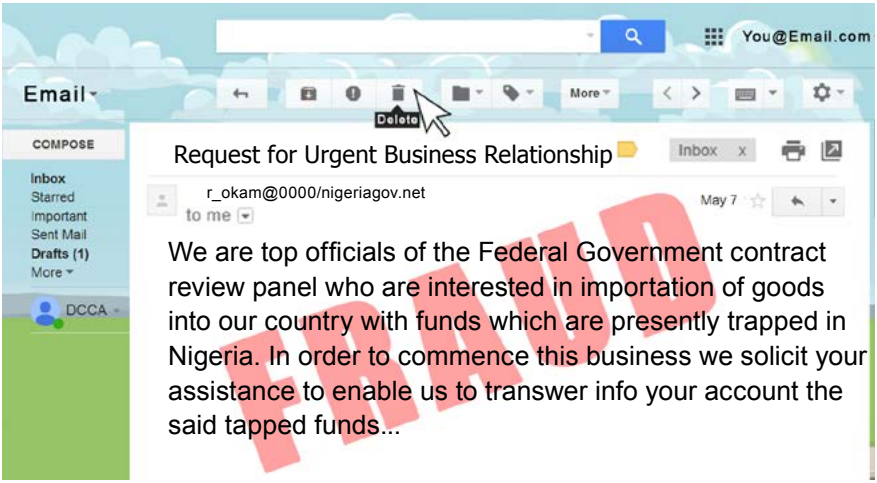
An inheritance scam is a type of Advance Fee Fraud and may also expose you to identity theft. Scammers email or somehow distribute a story about how a fictional individual—often with the same last name as the victim—died without heirs in remote parts of the world. If the recipient replies to the solicitation, the scammer will tell the victim to send money in advance to pay for legal fees, bribes, processing fees or other expenses in exchange for a large inheritance. The scammer may also attempt to obtain

copies of the victim's personal information, identification cards, financial account information, and other information, which can be used to forge bank drafts, empty the victim's bank account, obtain credit under the victim's name, or commit other acts of identity theft. The scammer may even send a fake check to the victim. But in reality, the victim will never receive the inheritance and will lose all the money he or she advanced.

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 email 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, royalty, or business executive, is trying to transfer illegally out of the foreign country.



Many people have fallen for this scam that was popularized by scams originating from Nigeria. The victims send an advance amount of money to help get the 'illegal funds' out of the foreign

country. They are lured into the scam with the promise that the scammer will give them a share of a very large payment from these illegal funds, a sum far greater than the fee the victims have to advance. In reality, there is no payout. Victims lose the money they sent and receive nothing in return. Victims also open themselves up to identity theft, having sent personal information to the scammers. Once victims 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 or others. Report the fraud.

LOTTERY OR SWEEPSTAKES SCAM

A typical lottery scam begins with an unexpected notification through email, text, postal mail, or fax that claims you have won a large sum of money or prize 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 pays the fees but never receives any lottery or sweepstakes payment. Many email lottery or sweepstakes 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 email asking you to participate in a lottery. Avoid companies that offer the convenient purchase of lottery tickets, with promises of unbelievable odds and high winnings.

No Hawaii State public official, in his or her official capacity, will authenticate any prizes or sweepstakes.

Reference No. 9-22-22-22
Batch No. HI-5-0/TI-TA

Free Lotto Lottery

FREE LOTTO LOTTERY
P.O. Box 00000
Kingston, Jamaica JMAAW003

CONGRATULATIONS! You have won ONE MILLION FIVE HUNDRED THOUSAND UNITED STATES DOLLARS (U.S. $1,500,000.00)!

Your prize money is in the wire system of our payee bank inured with your winning. You must contact your Claim Agent, Mrs. Jane Smith, without delay for immediate processing of your winnings to your nominated bank account.

Yours Sincerely,

Mr. John Doe
Mr. John Doe

FRAUD

LOTTERIES AND SWEEPSTAKES

- Legitimate sweepstakes and lotteries don't require you to pay processing fees or taxes in order to claim your prize.
- Legitimate offers clearly disclose terms and conditions of the contest.
- Purchasing foreign lottery tickets is illegal. United States law prohibits mailing payments to purchase any ticket, share, or chance in a foreign lottery.
- Foreign lottery solicitations sent to addresses in the United States do not come from foreign government agencies. They come from scammers.
- In some cases, the soliciting company uses high-pressure telemarketing techniques to obtain credit card account numbers. Once credit card numbers have been obtained, the theives often make unauthorized transactions. Do not give out your credit card number to claim a prize.

WHAT TO DO

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

- If notified by mail, check disclosed terms and conditions of the contest.
- If notified by mail, check the postmark on the envelope. If it was sent at a 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.
- Do not wire transfer funds to claim your prize.
- Do not be deceived by endorsements from well-known celebrities that fraudulent promoters may use to elicit confidence in their offer.
- Do a simple Internet search to find out more about the company, its rules and any online complaints. Try typing the company's name and the word "scam" in the Internet search to see what kinds of scams or issues others have been experiencing.
- Be skeptical when asked to attend a sales meeting to win a prize.
- For help, call the Better Business Bureau Fraud Hotline on Oahu at (808) 628-3950 or toll-free from the neighbor islands at 1-888-333-1593 for more information.
- Report fraud to your local police deparment, the DCCA Office of Consumer Protection at (808) 586-2630 and the FBI at (808) 566-4300.

COMMON CONSUMER FRAUDS

The following section covers a vast range of common consumer frauds from construction to charity fraud. We discuss the frauds and offer red flags, tips and where to go for help.

CONSUMER

OVERPAYMENT, FAKE REFUND AND FAKE CHECK FRAUD

This type of scam is one of the most common and deceptive scams. It's not surprising why so many people fall for this scam. The scam builds fake trust and it often starts when you try to sell something online (for example on Craigslist, eBay or any other legitimate online site) or you offer a service for hire (like a law firm). For example, you want to sell your phone for $500. The scammer pretends to be a buyer from far away. At this point, you have a normal amount of doubt - will the scammer pay?

The scammer puts your trust at ease by sending an official certified bank check, a cashier's check, postal money order, travelers check or some other "safe" check to you from an actual foreign bank. In fact, he overpays and sends you $50,000 instead of $500. Now you trust him because he has not only paid, but overpaid by a lot. He says his check had a typo and asks you for a refund. In fact, he even offers to let you keep half of the $50,000 as long as you send him $25,000 back.

To retrieve the overpayment, the scammer asks you to deposit his $50,000 check in your account and to wire the agreed overpayment of $25,000 back to him. You deposit his check and you see $50,000 in your bank account, so you wire him the $25,000. You think you have received a windfall.

What you don't know is that foreign checks take longer to clear in a US bank account. The money may appear to be in your account, but it has not actually been cleared by the foreign bank, yet. By the time the foreign bank tells your bank that the scammer's $50,000 check was fraudulent, you have already wired $25,000 out of your account. Your bank will not honor the fraudulent $50,000 check and will not pay you back for your $25,000 wire transfer. You are now out a lot of money.

HELPFUL TIPS ON PREVENTING OVERPAYMENT, FAKE REFUND, AND FAKE CHECK FRAUD

- Do not deposit a check for more than the agreed amount. If they overpaid, they need to cut you a new check and you can return the old check.
- Make a photocopy of the scammer's check for your records before you deposit it or return it.
- If you must provide a refund, do not do it through wire transfer. Foreign checks may take as long as six weeks, sometimes longer to clear. Call your bank to confirm full clearance. If the repayment amount is very large, it may make sense to contact the foreign bank itself and make sure the check is real. Send the foreign bank a fax or email copy of the check and let the foreign bank examine it.

WHERE TO GET HELP:

For more information on these scams:

1. Call the Federal Trade Commission 1-877-438-4338.
2. Call the Better Business Bureau Fraud Hotline on Oahu at (808) 628-3950 or toll free from the neighbor islands at 1-888-333-1593.

If it happens to you, report it.

1. Call your Local Police Department 9-1-1.
2. Call and report to the DCCA Office of Consumer Protection at (808) 586-2630.
3. Call the Federal Bureau of Investigation (808) 566-4300.

CHARITY FRAUD

Charity Fraud is committed when a perpetrator creates a bogus fundraising operation often by exploiting a fake personal tragedy or taking advantage of natural disasters, such as a typhoon or earthquake. These unscrupulous scammers take advantage of our sympathies, goodwill and generosity. 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 donating. These tips will help ensure that your donations are put to good use.

HELPFUL TIPS FOR AVOIDING CHARITY FRAUD

- 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.

- Check registration. Every charity that solicits contributions in Hawaii must register with the Tax and Charities Division of the Department of the Attorney General (808) 586-1480. Before you give, search the Attorney General registered charities database: ag.ehawaii.gov/charity.
- Check the IRS website "EO Select Check" (http://www.irs.gov/Charities-&-Non-Profits/Exempt-Organizations-Select-Check). You can type in a charity name and see if its federal tax standing is valid.
- 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 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 towards administrative costs. There is no specific 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 ag.hawaii.gov/tax.
- Do not pay over the phone. Always ask for written information. But be careful; just because an organization sends you information, it 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 fundraising reports on the charity on the Attorney General's website and with charity watchdogs such as:
  - American Institute of Philanthropy (charitywatch.org)
  - Better Business Bureau's Wise Giving Alliance (give.org)
- Call the organization back to verify the solicitor's name and request.
- Do a quick Internet search on the charity.

WHERE TO GET HELP:

If you are scammed:

1. Call your Local Police Department 9-1-1.
2. Call the Department of the Attorney General, Tax and Charities Division (808) 586-1480.
3. Call the Federal Bureau of Investigation (808) 566-4300.

CONSTRUCTION AND HOME REPAIR

Construction and Home Repair Fraud involves situations where you have paid someone to do a job and he or she has either done work that is poor quality, left the work incomplete, or even done no work at all. In Hawaii, contractors must be licensed by the Department of Commerce and Consumer Affairs (DCCA) Division of Professional and Vocational Licensing (PVL). The Regulated Industries Complaints Office (RICO) of the DCCA takes complaints regarding licensed and unlicensed contractors and investigates and enforces against fraud. RICO also provides consumers with a searchable database of complaints and a consumer resource center. Go to cca.hawaii.gov/rico or call (808) 587-4272.

Your home may be the single biggest investment you'll ever make, so take your time, do your homework, and hire a licensed contractor.

RED FLAGS FOR CONSTRUCTION AND HOME REPAIR FRAUD

- Unlicensed contractors may go door-to-door claiming they "just finished a job down the street," or "have materials left over from another job."
- They may try to pressure you, offering a discounted price, but only if you act today. Remember, a great deal today will probably be just as good a deal tomorrow, so take the time you need to consider the situation carefully.
- Unlicensed contractors may ask for cash payments, substantial down payments, or for all of the money to be paid in advance. After they get the money, they may move a little dirt or, worse, demolish a wall or driveway, and never return.

WHAT TO DO IF YOU ARE APPROACHED FOR HOME REPAIRS

If someone knocks on your door or approaches you in your yard offering to perform home repairs such as fixing your roof, repaving your driveway, painting, or power-washing your house, be careful…

Check with a friend or family member and ask yourself

1. Is the work really necessary?
2. What exactly do I need done?
3. Is this person licensed?

Then, contact RICO's Consumer Resource Center (808) 587-4272 to see if the person is licensed and to check their complaint history.

In Hawaii, a contractor is required to have a license to perform remodeling, repair, and yard work over $1,000 (or if a building permit is required). Remember, three bids or estimates, preferably from licensed contractors, may help you decide if the work they're proposing is really necessary.

HELPFUL TIPS FOR HIRING LICENSED CONTRACTORS

- Ask to see a picture I.D. so you know exactly who you're dealing with.
- Never pay all of the money up front and avoid paying in cash. Pay as you go by setting up a payment schedule that follows the amount of work completed. Get the payment schedule in writing.
- Remember to check the complaint history of the contractor and check his/her license. You can do this by contacting the DCCA Consumer Resource Center (808) 587-4272 or visit their website at businesscheck.hawaii.gov.

- Know how much you can spend. Fix your budget in advance and keep some in reserve to pay for changes or unanticipated costs.
- Shop around. Get at least three bids or estimates. Make sure the bids are based on the same work and the same materials. If bid amounts vary significantly, ask why.
- Ask for references. Call trade organizations or ask friends or relatives for referrals. Ask to see other projects the contractor has completed and to meet other clients.
- Insist on a written contract. Among other things, a written contract should include the contractor's license number, total cost, start and stop date, the work to be performed, and the materials to be used. Get any promises, guarantees or warranties in writing!
- Make sure your project is in compliance with city and county codes. If building, electrical, or plumbing permits are required, ask the contractor who will be responsible for the permitting process. Know the risks and responsibilities of being an "owner-builder."
- Monitor the job and keep good records. Keep a file with the contract, cancelled checks, and correspondence. Make sure any change orders are in writing.
- Know who your subcontractors are and avoid liens. Request partial lien releases for partial payments made and a final lien release for final payments made. Make sure a notice of completion is published in a newspaper.
- Do a thorough "walk-through" and take care of any "punch list" items immediately.

As always, be wary of any offers that require immediate cash payments on your part, and remember, if it sounds too good to be true, it probably is.

SOLAR PANELS/PHOTOVOLTAIC (PV) PANELS

The pursuit of installing photovoltaic (PV) panels on rooftops to cut down monthly electric bills remains popular, and unfortunately some are using this interest to take advantage of unsuspecting consumers.

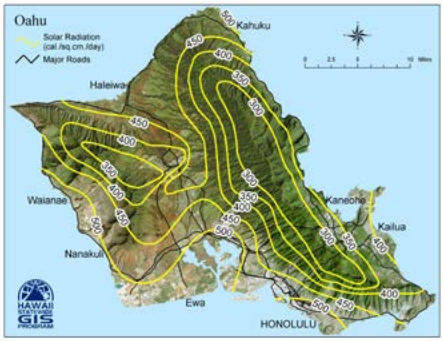
Do not be afraid to ask many questions, and also double check with the utility company to verify that everything is in line with proper procedure. For more information, contact your utility company and the DCCA Division of Consumer Advocacy at (808) 586-2800.

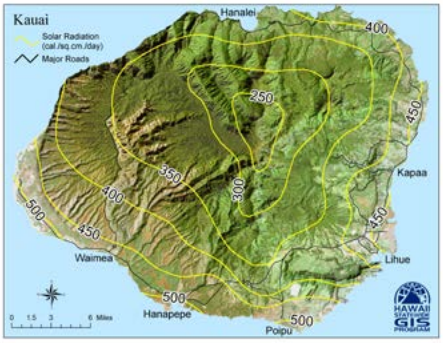
HELPFUL TIPS WHEN INSTALLING PV PANELS

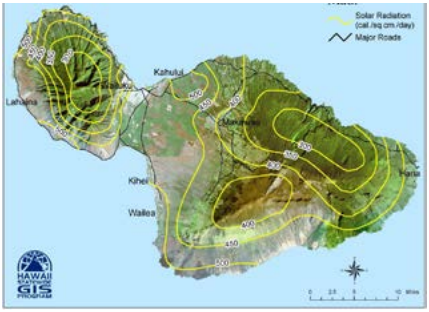
- Get Multiple Quotes. Try to get at least three or more quotes. Getting multiple quotes will help you get the best price, and allow you to determine who might be more knowledgeable and experienced in PV installations. It can give you a sense of who may be attempting to take advantage of you.
- Understand All Terms. Once you get the contract in writing, make sure you understand all the terms before you sign. What's being guaranteed? With so many components in a PV system, one part may be covered under warranty by one company, while another

is covered by a completely separate entity. Will the installation void your roofing warranty? You may want to double check with your roofer first. There are also a variety of financing options when it comes to PV. Leasing, power purchase agreements, and loans can look attractive on paper, but make sure you understand the costs involved.

- Size It Right. When purchasing a PV system, make sure you are not buying more panels than you really need to be cost effective. While not all companies will engage in such practices, understand the possibility of a seller boosting their profit margin by suggesting more panels than you actually need, or placing panels in areas that may not be cost effective because they are shaded. The National Renewable Energy Laboratory (NREL) has an online calculator tool to help estimate the performance and cost of PV systems. (pvwatts.nrel.gov/).
- Hire a Licensed Contractor. Trying to cut costs by taking up an offer from an unlicensed worker is like playing with fire. Do it right and hire a reputable licensed contractor to avoid headaches. The DCCA, RICO office, is a great resource to check on contractor businesses and individuals. Go to cca.hawaii.gov/rico/business_online/ or give RICO a call at (808) 587-4272.
- The Hawaii State Energy Office also publishes solar maps to help areas determine how many peak sun hours they can expect on a typical day. 500=5.8 hrs, 400=4.6 hrs, 300=3.5 hrs.







Here are samples of the Hawaii solar maps. If you would like to view them more closely, visit their website at energy.hawaii.gov/resources/hawaii-state-energy-office-publications#solar

- Check with the Utility Company First. The utility company may be unable to accept more PV customers in some areas at the moment, so double check that you are eligible to connect before you put any money down. While Oahu customers can check their area's circuit to see if it is full through the Locational Value Map on HECO's website (hawaiianelectric.com/portal/site/heco/lvmsearch), it is advised that

customers contact the utility company directly for the most up to date information. With growing popularity of PV installations, it is still possible that changes in penetration occur while preparing your application and you may miss the cutoff before your Net Energy Metering (NEM) agreement is approved. Contacting the utility company or submitting an application does not reserve your spot to interconnect.

  - Hawaiian Electric Company: (808) 543-4760, nem@heco.com
  - Maui Electric Company: (808) 871-8461 ext. 2455, meconem@mauielectric.com
  - Hawaii Electric Light Company: (808) 969-0358, LVM@helcohi.com

- No One Has a Special Relationship with the Utility Company. If a contractor claims to have a special arrangement with the utility to get you interconnected, it is a lie. No individual or company has any advantage or agreement with the electric utilities company to jump the queue. Customers told information along these lines should be wary of the next tip below.
- Do Not Hook Up Illegally. Some folks are telling customers it is okay to just go ahead and flip the switch on their PV systems without a proper NEM agreement in place with the utility company. This is not true and can be dangerous for your home, neighbors, and utility workers. The utility company is aware of "rogue" PV systems and is taking steps to crack down on customers that connect their systems without a proper NEM agreement. Customers in violation risk disconnection of electric service.

RENTAL SCAM

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

FAKE LANDLORD

A scammer advertises a high-end rental for below-market rent. A prospective tenant is asked to pay a deposit to secure the rental. The scammer disappears with the deposit, leaving the victim without a rental and without the deposit.

FAKE TENANT

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

In one scenario, the scammer will send the landlord a check with an **overpayment** asking the landlord to return the extra money to the scammer by money order or wire transfer. The victim sends a partial refund back not knowing that the initial overpayment check has either bounced or was a fake to begin with. The victim is left without money and without a tenant.

In another scenario, the scammer will send the landlord a check for the deposit. The scammer will then contact the landlord with a story about a death in the family or some other crisis and ask for a full refund to be wired back as soon as possible, before the initial check has cleared.

The scam is that the initial check will never clear and the victim who has sent that overpayment or refund by wire transfer will not be getting any money back. These two scenarios are classic examples of Overpayment, Fake Refund and Fake Check Fraud. For more information about Overpayment, Fake Refund and Fake Check Fraud, see page 32.

FAKE VACATION RENTAL

In this scam, the victim is usually a non-resident who is planning to vacation in Hawaii. Typically, the scammer posts offers for luxury rentals on various websites that list vacation rentals. The offers often include idyllic beach front settings, seclusion, and easy access to visitor attractions. The "hook" is the below market cost of the rental. Of course, a security deposit is required and must be paid in advance. Our vacation visitor makes payments in advance but when our visitor arrives, he or she soon discovers that it's a scam. The island retreat either does not exist or is inhabited by its residents, who have no intention of renting their home and have not authorized anyone to make such an offer. The visitor has not only lost the money but now needs to find lodgings for his or her family.

HELPFUL TIPS FOR AVOIDING RENTAL SCAMS

For Renters:

- Before renting, someone you trust should physically go and check out the property you're interested in renting.
- Before renting, do a quick online search to make sure the renter is who he says he is and check out the property. Many times, if you check out the address online, you will find that the property is for sale, not for rent.

- If advance payment is required, ask to use a credit card or a service like PayPal, both of which offer some fraud protection.

For Landlords:

- Always inform your bank when a check you are cashing is from someone you do not know before you deposit it to your account.
- Never wire money as an overpayment or refund.
- Do not refund deposits until you are certain the original check has cleared. Call your bank to confirm.

WHERE TO GET HELP:

For help and to report fraud:

1. Call your Local Police Department 9-1-1
2. Call the Federal Bureau of Investigation (808) 566-4300

SECURITY ALARM SYSTEM FRAUD

A security alarm system can provide consumers with a sense of well-being, but the opposite is true when consumers feel pressured into buying an alarm system without first considering important information such as installation and permitting requirements.

If someone comes to your door offering to sell you a new alarm system or to change alarm companies, think before you buy. Get a copy of any alarm monitoring agreement they're offering and review it carefully. Remember, a contractor's license is required in Hawaii to install low-voltage alarms and to perform electrical work. For more information on how to check a license or complaint history, or to report fraud, call DCCA RICO at (808) 587-4272.

HEARING AID DEALERS AND FITTERS

A hearing aid dealer and fitter is required to be licensed by the Professional Vocational Licensing (PVL) Division of the DCCA to measure your hearing and to help you select, adapt, or sell you a hearing aid. A medical examination by a physician (preferably a physician who specializes in diseases of the ear) is required. For more information on how to check a license or complaint history, and to report fraud, call DCCA RICO at (808) 587-4272.

CAR REPAIRS AND SALES

A motor vehicle repair shop must be licensed by DCCA PVL Division to repair motor vehicles, so be wary if someone knocks on your door or approaches you in a parking lot offering to fix your car. While auto body shops do not require licensing, other auto repair shops do. When it comes to non-auto body repairs, look for an established shop with a licensed mechanic. For more information on how to check a license or complaint history, or to report fraud, call DCCA Consumer Resource Center at (808) 587-4272.

The same goes for car sales. Generally, a PVL motor vehicle sales license is required to sell three or more cars each year. Be wary if someone approaches you asking about buying your car or selling you a new one.

UTILITY COMPANY SCAMS

Utility company scams involve scammers impersonating utility company employees threatening to disconnect service unless the victim pays or provides personal information over the phone or in-person. When in doubt, contact the utilities company (such as electric, water, gas, phone, cable, etc.) directly to verify the request. Make payments directly to the utility company and keep a receipt as proof of payment.

PURCHASING ONLINE

One common online scam involves the sale of products at a discount. The seller advertises high value goods at low cost. The text of the ad instructs buyers to contact the seller directly, outside of the website, at a Yahoo or Gmail type of email account. When contact is made, the seller provides a story about his problems receiving payment via a third party payment service, such as credit cards or PayPal and instead insists on having the money wired. 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. However, if the buyer proceeds and wires the money, it will be gone forever and the buyer may receive a faulty product or no product at all.

HELPFUL TIPS WHEN PURCHASING ONLINE

- Do not wire money.
- Avoid doing business with anyone who wants to operate outside of a monitored website.
- Check history, seller and buyer rating online before making a purchase.
- Identify the seller and check their reputation with the Better Business Bureau.
- Evaluate the different payment options such as credit card, escrow services, Pay Pal or Cash on Delivery (C.O.D.).
- Be cautious if the seller insists on payment by wire transfer, cashier's check or money order.

Check a Professional License and Consumer Complaint History for more than 48 Industries

Many people are not aware that a professional or vocational license is required before you can work in certain industries. The Professional and Vocational Licensing (PVL) Division of the DCCA licenses more than 48 different professional or vocational industries. These industries are the kind that affect the health, safety, and welfare of Hawaii's residents. See the chart on page 50.

The Regulated Industries Complaints Office (RICO) of the DCCA investigates and prosecutes allegations of professional misconduct by licensees and unlicensed activity.

RICO offers the licensing information and complaint history for professionals in the following industries. For help, go to cca.hawaii.gov/rico. To report fraud in any of these 48 areas, call (808) 587-4272.

Licensed Professionals Regulated by PVL and RICO

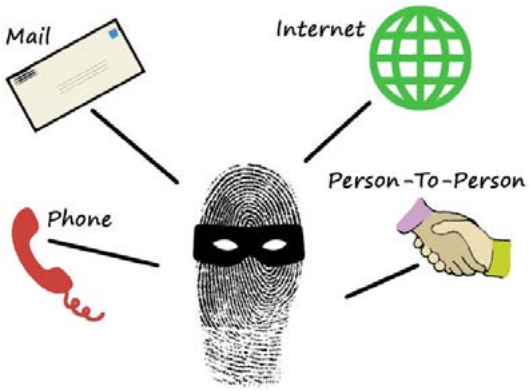
- Accountancy
- Activity Desk
- Acupuncture
- Athletic Trainers
- Architects and Landscape Architect
- Barbering and Cosmetology
- Boxing
- Cemetery and Pre-Need Funeral
- Chiropractor
- Collection Agency
- Commercial Employment Agencies
- Condominium Property Regimes
- Contractor
- Dentist and Dental Hygienist
- Dispensing Optician
- Electrician and Plumber
- Electrologist
- Elevator Mechanic
- Employment Agency
- Engineer
- Hearing Aid Dealer and Fitter
- Marriage and Family Therapist
- Mental Health Counselor
- Mixed Martial Arts Contests
- Motor Vehicle Industry
- Motor Vehicle Repair
- Naturopathic Medicine
- Nurse Aide
- Nursing
- Nursing Home Administrator
- Occupational Therapist
- Opticians, Dispensing
- Optometry
- Osteopathy
- Pest Control
- Pharmacy and Pharmacist
- Physical Therapy
- Port Pilot
- Private Detective and Guard
- Psychology
- Real Estate
- Real Estate Appraiser, Brokers, Salespersons, Commission, Education, Schools & Instructors
- Respiratory Therapist
- Social Worker
- Speech Pathology and Audiology
- Subdivision
- Time Share
- Travel Agency
- Uniform Athlete Agents
- Veterinary Medicine

IDENTITY THEFT

Identity theft happens when someone steals your identity by stealing your personal information. The thieves may use your personal information to empty bank accounts, open credit cards and make charges to those cards, take out loans against your mortgage, or even give your name during an arrest. It causes havoc with your finances, your credit history and reputation.

HOW DO THIEVES GET YOUR INFORMATION?

As we discussed earlier in this Guide under Methods (see page 10), scams like identity theft take place through all four communication methods: the Internet, phone, mail and person-to-person contact. Below are some of the ways we inadvertently "give" our information to thieves.



INTERNET PHISHING

This term plays on the homonym "fishing." Internet phishing refers to when identity thieves try to fish out personal information through communications with the victim. For example, they may send an email falsely claiming to come from a well-known bank in an attempt to get the victim to give out sensitive information like account numbers and passwords. The email may direct victims to a website to "update" their information when in reality, the bogus website is actually collecting all the information for the identity thieves to use.

Remember, any of the Internet scams we discuss in this Guide can open you up to phishing scams and identity theft. For example, if you are emailing with someone and get caught in an Overpayment Scam (see page 32) or an Advance Fee Scam (see page 23), you could also end up exposing your bank account numbers or other personal information that could lead to identity theft.

SOCIAL MEDIA

Phising scams also occur on social media sites. The scam takes on a different approach as social media sites involve public communication or, at least, group communication. Some thieves may gather information from your Facebook page or other social media page and take on your persona from there. But often, in order to get the personal information needed for stealing funds, the thieves use the social media relationships as an entry way. After a relationship is established on the social media site, the ongoing relationship may move to email, texting, phone or even person-to-person contact which is when the real phishing begins.

MAIL

With mail, the problem tends to be less about phishing and more about thieves finding ways to gain access to your mail. They may steal mail from your mailbox or even go through your garbage to find bills containing your account number, social security number or other important information.

PHONE

There has been an increase of phone "phishing" where the thief finds some basic information, like a name connected to a phone number and uses it to try to get money or information from the target victim. The thief calls the number and immediately pretends to know the person on the other end of the phone and immediately asks for help. For example, the thief might start out by saying, "Aunty Kalei, this is Keola. I am so glad I got you on the phone. I've been trying to reach you because my son is really sick." When the caller asks "who?" the thief responds with disbelief and continues to play the part until he can elicit account numbers or other important information from "Aunty Kalei."

More traditionally, thieves will pretend to be from an established company like a well-known bank. They call the victim to "update" information such as account number, birthdate, social security number and other key pieces of information. The thieves may even ask the victim to update their information, "through an automated response system" when in reality, the thieves are collecting the information through the phony automated system.

PERSON-TO-PERSON

In this approach, a scammer meets face-to-face with the target victim. The scammer may be impersonating an agent from a well-known company and may even be a friend or acquaintance of the victim. The scammer may pretend to be selling something such as group insurance or securities and may claim that he "needs" the victim's bank account numbers and social security number to "process" the paperwork. Be wary.

HELPFUL TIPS TO PROTECT YOURSELF AGAINST IDENTITY THEFT

Internet	• Do NOT click on email attachments from strangers or from any suspicious email. • Do NOT click on links that lead you to update your information on another page. If you want to update your information for an online account, open your regular browser and type in the official website for your account. • Delete emails from strangers and any other shady emails. Someone might be pretending to know you.
Mail	• Shred mail with personal information before you throw it away. • Keep mail with personal information in a secure place. • Put a lock on your mailbox.

	• Mail important letters directly at the post office or through secure post boxes, not through office mail drops, doormen or unsecured mailboxes.
Person to Person	• Never fill in forms with personal information and hand them to a stranger without checking the person's background. Is that person actually employed by that bank, securities firm or insurance company? Are they registered to do this business in Hawaii? Have they been charged with fraud? Search online to research the stranger's background. • Ask to leave out key information. For example, why would they need your bank account information to sell you insurance? Leave it out. If the stranger is persistent, try to find out why or just walk away. • Get written copies of anything you sign.
Phone	• No established company will call or text you and ask for private information over the phone. If someone says they are calling from a bank or financial institution to update your information, ask for their name, employee ID and extension. Tell them you will call them back at the bank's official number and have the bank connect you to them. Or even better, just hang up.




WHAT KINDS OF INFORMATION ARE MOST IMPORTANT TO PROTECT?

- Social security numbers
- Bank account numbers
- Investment account numbers
- Mother's maiden name
- Full birthdate (month/day/year)
- Credit card numbers and security codes
- Home address
- Medicaid and Medicare numbers

WHAT SHOULD YOU DO IF YOU THINK YOUR INFORMATION HAS BEEN LOST OR STOLEN?

- Place a fraud alert on your credit file and see page 58 for instructions.
- Monitor your accounts for unusual activity. Examine your bank and credit card statements.
- Get a free copy of your credit report and look for unusual activity. For example, check to see if new credit lines or mortgages have been opened in your name without your knowledge.
- See page 61 on how to get a FREE credit report.

WHERE TO GET HELP:

1. Call your local Police Department 9-1-1.
2. Call DCCA Office of Consumer Protection (808) 586-2630.
3. Call the Federal Trade Commission 1-877-438-4338.

IF YOU ARE A VICTIM OF IDENTITY THEFT

PREVENTION IS YOUR MAIN DEFENSE from becoming a victim of identity theft. However, if you become a victim of identity theft:

1. Place a 90-day Fraud Alert on your credit file by contacting the three companies below.
2. Correct errors by contacting your creditors and ask creditors to call you before opening any new accounts or changing existing accounts. While you're at it, request copies of your credit report from these same three companies and review the credit report carefully for errors.

EQUIFAX®

Phone: 1-800-525-6285
Website: equifax.com
Mail: Fraud Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374

Experian℠

Phone: 1-888-397-3742
Website: experian.com/fraud
Mail: National Consumer Assistance
P.O. Box 2002
Allen, TX 75013

Phone: 1-800-680-7289
Website: transunion.com
Mail: Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

3. Close any financial accounts or credit cards that have been tampered with or established fraudulently.

4. File a police report to help you with creditors who may want proof of the crime or file a miscellaneous publication (misc. pub.).

   Hawaii (Big Island) Police Department
   Phone: (808) 935-3311

   Honolulu Police Department
   Phone: 9-1-1 (request non-emergency)
   Email: policereport@hawaii.gov

   Kauai Police Department
   Phone: (808) 241-1711

   Maui Police Department
   Phone: (808) 244-6400

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

6. Go to ftc.gov to file a complaint with the Federal Trade Commission and complete the Identity Theft Complaint Form and Identity Theft Affidavit.

IF YOUR CHILD IS A VICTIM OF IDENTITY THEFT

1. Do the same thing for your minor child that you would do for yourself in the previous section.
2. But also contact each of the three nationwide credit reporting companies.
    - Send a letter asking the companies to remove all accounts, inquiries and collection notices associated with the child's name or personal information.
    - Explain that the child is a minor (under 18 years old) and include a copy of the Uniform Minor's Status Declaration, which you can find at consumer.ftc.gov.

IF YOU ARE A VICTIM OF TAX IDENTITY THEFT

1. Contact the Internal Revenue Service.
   IRS Identity Protection Specialized Unit 1-800-908-4490
    - Report the fraud.
    - Send a copy of your police report or an IRS ID Theft Affidavit Form 14039 and proof of your identity, such as a copy of your Social Security card, driver's license or passport.
2. Update your files.
    - Record the dates you made calls or sent letters.
    - Keep copies of letters in your files.

3. Other steps to repair identity theft:

    - After you contact the IRS, It's important to limit the potential damage from identity theft.
        - Put a fraud alert on your credit reports.
        - Order your credit reports.
        - Create an Identity Theft Report by filing an identity theft complaint with the FTC at ftc.gov and filing a police report with your local police department.

How to get your FREE Credit Report

You can call the three credit reporting 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 above (Equifax, Experian and TransUnion). Another option is to contact the Annual Credit Report Request Service. This service is a centralized service for consumers to request free annual credit reports.

ANNUAL CREDIT REPORT REQUEST SERVICE
1-877-322-8228 or annualcreditreport.com

FINANCIAL

FINANCIAL FRAUD

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

In 2014, according to the Federal Trade Commission, Hawaii ranked 43rd in the nation in the number of fraud and other complaints per the size of our population.

The following are different types of financial frauds. This section will help you recognize the fraud before it happens, provide tips on preventing fraud and direct you to where to get help.

CREDIT CARD FRAUD

Credit card fraud can take two forms:

1. The perpetrator obtains credit card information and uses it to charge items, often via online purchases, to another person's credit card account. Gas station charges are popular too.
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 credit card was fake and the amount due will not be paid, or the payment received will be reclaimed by the credit card's issuing bank.

CREDIT/DEBIT CARD SKIMMING

The ease and convenience of using our credit or debit cards at the gas station, ATMs, restaurants, etc. can expose us to fraud. Consumers today need to be alert when they hand off or swipe their credit cards or debit cards. The threat we are seeing at many gas stations today with credit and debit card users is called skimming. Skimming involves a modified swiping machine with a card reader that has been illegally set up to steal information from the card's magnetic strip and record a PIN number if it is input.

Source: Privacy Sense. Debit and Credit Card Skimming. Retrieved from http://www.privacysense.net/debit-and-credit-card-skimming/

HELPFUL TIPS TO AVOID SKIMMING

- Review your bank statements.
- Inspect the card reader and the area near the PIN pad.
- Look at other nearby gas pumps or ATM card readers to see if they match the one you are using.
- Avoid using your PIN number at the gas pump.

Source: O'Donnell, Andy. How to Avoid Credit Card Skimmers. Retrieved from http://netsecurity.about.com/od/securityadvisorie1/a/How-To-Avoid-Credit-Card-Skimmers.htm

HELPFUL TIPS TO KEEP YOUR CREDIT AND DEBIT ACCOUNTS SECURE

- 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 card-issuing bank in a secure place.
- Keep an eye on your card during any transaction.
- Save receipts to compare with billing statements. Keep receipts in a secure place and destroy them when no longer needed.
- Open bills promptly and reconcile accounts monthly. Report any questionable charges promptly and preferably in writing to the card company.
- Notify card companies in advance of a change in address.

- Use a credit card and not a debit card for online purchases since many credit cards offer online fraud protection. Credit card charges can be disputed.

INSURANCE FRAUD

Insurance is an important tool that helps consumers manage risk when it comes to their health, home and belongings. Unfortunately, some insurance agents try to take advantage of consumers by selling false policies, overpromising in order to secure business, or stealing money and personal information.

BEWARE OF BUNDLING

Consumers need to be aware of the types of false claims made by insurance agents. One type of practice consumers should be aware of is known as "conditional sales" or "bundling." It is illegal for an insurance agent to tell their clients that they are unable to write a policy unless another plan is purchased. Consumers have the option of buying their policies separately from various agents, and are not required to purchase multiple policies in order to secure coverage with one insurance agent or company.

HELPFUL TIPS TO PREVENT INSURANCE FRAUD

- Take your time.
- Ask questions.
- Request copies of signed documents.
- Get a second opinion and estimate from another seller.

WHERE TO GET HELP

Consumers who feel that they have been taken advantage of should contact the DCCA Hawaii Insurance Division's Investigations Branch at (808) 586-2790. For more information about Hawaii's insurance industry and tools to help protect against fraud, visit cca.hawaii.gov/ins.

HEALTH INSURANCE FRAUD

Since the advent of the Affordable Care Act (ACA), also known as Obamacare, there are additional opportunities for agents to take advantage of consumers. When purchasing a health insurance policy, always remember to buy directly from an approved and licensed health insurance carrier in Hawaii or the Hawaii Health Connector. To check if a company or agent is licensed, visit insurance.ehawaii.gov/hils.

Supplemental or limited coverage plans advertised on the radio, television or by mail do not satisfy the requirement to carry health insurance under the ACA. Fraudulent insurance agents may try to trick consumers into giving personal information for this type of coverage over the phone or in the mail. Beware.

WHERE TO GET HELP

Consumers that feel like they may have purchased a false health insurance policy or have any questions should contact the DCCA Hawaii Insurance Division's Health Investigations Branch at (808) 586-2804.

HOMEOWNER & AUTOMOBILE INSURANCE FRAUD

Insurance companies can also be victims when it comes to insurance fraud. When this happens, consumers feel the impact

because their insurance premiums increase. Since insurance is a tool used to help mitigate loss by creating a risk pool, the addition of fraudulent claims causes insurance premiums to go up in order to help the company cover the costs. Insurance fraud practices include, but are not limited to, falsifying a theft, exaggerating property damage, obtaining a policy after a loss has occurred and making a claim, and falsifying property receipts.

Reducing the number of fraudulent claims helps to drive down the cost of homeowner and automobile policies in the long run. Consumers can help protect themselves and others by reporting suspicious claims to their insurance company and the DCCA Hawaii Insurance Division's Insurance Fraud Investigations Branch at (808) 587-7416.

INVESTMENT FRAUD

Investment fraud happens through the sale or solicitation of securities, Ponzi schemes and other investments. Often the fraud involves financial advisers or sales agents persuading a target to make investments based on misleading or dishonest information. The appeal of the fraud usually involves a promise of higher-than-market interest, and a low or no-risk guarantee. It is important to remember that all legitimate investments have risk — the reality is that higher returns involve higher risk and a greater chance of losing your money. Beware of any promises to the contrary.

Con artists know that investors want to make a lot of money without risk. They know everyone wants to feel safe, secure and lucky while bringing in high returns. Con artists play on this fantasy. Don't fall for it.

HELPFUL TIPS FOR PREVENTING 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. Beware.
- You should always be mindful of whether an investment is suitable for your goals and needs.
- Call the DCCA Office of the Securities Commissioner at 587-2267 to see if the investment adviser, representative, broker-dealer, agent or the investment is properly registered or go to brokercheck.org to check background and complaint history.

PONZI SCHEMES

WHAT IS A PONZI SCHEME

The "Ponzi scheme," named after the 1920's swindler Charles Ponzi, is a ploy where earlier investors are paid with funds of subsequent investors. In a Ponzi scheme, claims of underlying investments are bogus; the whole scheme depends on the money coming in from new investors. Very few, if any, actual physical assets or financial investments exist to generate any true returns. As the number of total investors grows and the supply of potential new investors dwindles, there is not enough money to pay off early investors. A Ponzi scheme's bubble bursts when the con artist simply cannot keep up with the required payments. In many cases, the perpetrator has spent investment money on personal expenses, depleting funds and accelerating the bursting of the bubble.

1)

A con artist lures investors by offering no risk and high return investments.

2)

Earlier investors are paid with funds given by later investors, rather than from profits earned.

3)

Since investors have received payouts, they invest more or encourage others (friends/family) to invest too.

4)

The scheme collapses when the con artist simply cannot keep up with the required payments. In many cases, the scammer runs off with the money.

EXAMPLE: THE MADOFF CASE

Bernard Madoff perpetrated a multi-billion dollar scam that defrauded investors around the world for decades until his arrest in December 2008. Madoff investors were told they were getting consistent and steady annual returns through elaborate, fabricated account statements made to convince investors that their money had been placed in actual investments. The investments "appeared" legitimate, especially to people receiving small payments here and there. But in reality, there were no actual investments and no actual returns. Madoff paid the initial investor's "returns" with money provided him by a steady flow of new investors. In 2008, as the global economy began to decline, large numbers of Madoff investors needed money and began asking to cash in their investments. That's when Madoff's Ponzi scheme burst – he did not have assets or money to cover his investors' requests for payment and new investor money was hard to be found in the economic downturn.

HELPFUL TIPS TO PROTECT AGAINST PONZI SCHEMES

- Beware of promises of unrealistic returns. This is perhaps the easiest way to spot a Ponzi scheme. Any legitimate investment involves risk. Guarantees of unrealistically high returns are a clear warning sign. But delivering consistent 10 percent returns for decades, as Madoff purported to do, is unrealistic too, if not impossible. Beware of any deal that is "too good to be true."
- Diversify – everything. Don't put all of your eggs in one basket. Diversify not only your assets but also your money managers, accounts, and financial institutions. Spreading your money around will limit your exposure to the financial problems of any one institution. Victims in the Madoff case who were financially stable after the scam were the ones who invested only a percentage of their assets with Madoff, not their entire life savings.
- Don't rely on reputation or word of mouth alone. Con artists are experts at building networks of trust, making investors think they are getting an "inside" track on a hot investment. Many of Madoff's victims invested because they were part of a network of trust within the Jewish community. Madoff was considered a prominent and well-regarded member of that community. Be alert to any sales pitch that plays on your emotions, including your feelings of trust and friendship.
- Understand the investment. Ask detailed questions about the investments and those selling the investments, and get clear and direct answers before you invest. Don't let an "inside" tip override careful judgment. In the Madoff case, clients were told that the investment strategy was proprietary and would not be disclosed. If the investments are not explained to you in detail, walk

away. If you don't understand an investment, don't invest.

- Auditors. Check the auditor, or ask your financial adviser to check the auditor of any fund or company for you. Auditors sign and certify financial statements of companies and investment funds. Investors rely on these audit reports since auditors are liable for inaccuracies. A legitimate investment company managing multi-billion dollars of assets under management would use a reputable, nationally known auditing firm. In the Madoff case, with over $50 billion in purported funds, the fact that the auditor was unknown, hard-to-locate and had only three purported employees should have been a red flag to investors.
- Background Check. Check with the Hawaii Office of the Securities Commissioner to determine if the securities, the individuals and the firms selling the investment are properly registered with the State of Hawaii. You can also check the seller's complaint history when you call the office (808) 586-2722.
- Where to report Ponzi schemes. If you're a victim of a Ponzi scheme, call the DCCA Securities Enforcement Branch at (808) 586-2740. We can investigate the matter and take legal action where appropriate. We might be able to get some money back for you and your call may help others from being victimized by the same scam.

Source: NASAA. Madoff A 21st Century Ponzi Scheme. Retrieved from http://www.nasaa.org/4303/madoff-a-21st-century-ponzi-scheme/

AFFINITY FRAUD

WHAT IS AFFINITY FRAUD

Affinity fraud refers to an investment scam that targets groups and uses the trust among group members to spread the fraud. Con artists leverage that network to gain trust, cloak themselves in credibility and lower the guard of their target victim. It could be called "relationship" fraud because the con artists use relationships to get their "friends" to buy into fake investments, often Ponzi schemes.

The Madoff Ponzi scheme covered on page 69, is also an example of Affinity Fraud. Madoff was a prominent and respected member of the Jewish community. Many investors within that community let their guard down because Madoff had cloaked himself with the strong ties and well-regarded position he held in the group.

EXAMPLE IN HAWAII: BILLIONS COUPON CASE

In the Billions Coupon Inc. case, Marvin Ray Cooper was a leader in the Deaf Community in Hawaii. He used his position to convince over 129 investors to invest over $3.9 million dollars with him. There was no underlying investment.

The Office of the Securities Commissioner investigated the case and issued a Cease and Desist order banning Mr. Cooper from the industry, ordering rescission and charging him with an administrative penalty of $500,000.

HELPFUL TIPS FOR AVOIDING AFFINITY FRAUD

- Never make an investment solely based on the reputation of or "friendship" with a member of a group to which you belong.

- Remember, you have the right to say "no" even if it is a friend trying to sell you an investment.
- Beware of investment opportunities that sound too good to be true.
- Do not let a "friendship" stop you from getting the offer in writing and asking hard questions.
- Be suspicious if you are told NOT to share details of the investment with people outside of the group or to keep the investment opportunity confidential.
- Use common sense – just because someone you know made money or claims to have made money doesn't mean you will make money too.
- **WHERE TO REPORT AFFINITY FRAUD.** Report Affinity Fraud even if the scam artist is your "friend." It could help save you, your family and your community lots of money and heartache. Contact the Office of the Securities Commissioner at (808) 586-2740 or Toll Free 1-877-447-2267.

HOME LOAN FRAUD

There are many different types of fraud when it comes to home ownership and loans. Here are some common frauds.

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. Or a homeowner signs a blank document and the signature is used on a lien or transfer document.

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 from the swindler and when they cannot afford to repay it, the swindler forecloses, evicts and gets the whole property.

For example, a woman on a fixed income was persuaded to sign a loan contract secured by her home 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.

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 a type of 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 TO AVOID HOME LOAN FRAUD

- 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.

MORTGAGE REDUCTION/ SERVICING OR DEBT RELIEF FRAUD

In this type of fraud, individuals represent themselves as attorneys, foreclosure counselors, mortgage servicers or mortgage lenders who claim they can help reduce mortgage payments or eliminate mortgage debt. The con artists running these scams have often targeted vulnerable groups like non-English speaking

immigrants. They work hard to infiltrate trusted networks of family and friends.

The con artists advise consumers to stop making payments to their lender in order to qualify for a mortgage modification, or to eliminate the mortgage. The consumers are directed to pay an upfront fee, transfer title or even make payments to the con artists and their fictional company in return for the loan modification or forgiveness. In reality, the victim loses the money paid to the con artists, gets in trouble with the actual lender who the consumer stopped paying and may even lose the home. These missed payments harm the consumer's credit score and can trigger penalties, high interest rates on the original loan and even foreclosure action.

HELP FOR HOMEOWNERS

If you are experiencing any difficulty with your mortgage or in dealing with your lender or mortgage servicer, there are Department of Housing and Urban Development (HUD) certified housing counselors located at various non-profit agencies here in Hawaii that can provide assistance on buying a home, renting, defaults, foreclosures, and credit issues at no cost to you. Please do not delay before contacting a HUD-certified counselor. The earlier you contact a counselor, the more likely they can help you. For more information as well as a list of HUD approved housing counseling agencies in your area, visit cca.hawaii.gov/hfic/ or contact the Hawaii Foreclosure Information Center at (808) 587-3222.

If you have been victimized, you can file a complaint with the DCCA Office of Consumer Protection (OCP). Contact the Consumer Resource Center at (808) 587-4272 or visit the OCP website at cca.hawaii.gov/ocp/ for more information about filing a complaint.

HELPFUL TIPS TO PROTECT AGAINST MORTGAGE REDUCTION OR DEBT RELIEF FRAUD

If you are looking for help to prevent foreclosure, avoid any business or individual that:

- Promises they can stop the foreclosure process, no matter your circumstances.
- Instructs you not to contact your lender, lawyer or HUD approved housing counselor or credit counseling agency.
- Recommends that you stop making your mortgage payments.
- Recommends that you make your mortgage payments directly to them, rather than your lender.
- Collects a fee before providing any services.
- Recommends that you hire an out-of-state lawyer who isn't licensed to practice law in Hawaii.
- Pressures you to sign papers you haven't had a chance to read thoroughly or that you don't understand.

HEALTHCARE AND MEDICARE FRAUD

Healthcare fraud can take various forms. This section gives you information on how to check medical professionals and discusses scams, fraud, billing errors and/or abuse against Medicare and insurance companies.

PROFESSIONAL LICENSES: DENTISTS, NURSES, DOCTORS (PHYSICIANS)

Dentists, nurses and doctors must be licensed to practice in Hawaii. A license means the State has vetted the healthcare professional for qualifications such as education and training.

You can check your healthcare provider's license and complaint history by contacting the Regulated Industries Complaints Office (RICO) and the Professional and Vocational Licensing (PVL) Divisions of the Department of Commerce and Consumer Affairs.

For more information on how to check a license or complaint history, and to report fraud, call RICO at (808) 587-4272 or visit their website at cca.hawaii.gov/rico/business_online/.

MEDICARE FRAUD

Medicare scams, billing errors, abuse, and fraud cost taxpayers over $80 billion dollars each year. One type of fraud is Medicare Identity Theft where someone steals your name, social security number, or Medicare number to get medical care, buy drugs, or send fake billing to Medicare. Sometimes false claims are intentionally sent to Medicare in order to obtain payment. See the chart on your right for ways that fraudulent claims are billed to Medicare.

Types of Fraudulent Claims

Physicians/ Practitioners	• Upcoding to a higher-level of service to obtain more payment from Medicare • Billing for services not provided • Misrepresenting diagnoses on the claim forms to obtain payment from Medicare
Mental Health Services	• Upcoding • Using non-licensed staff to provide services when a license is required • False billing (e.g. billing group therapy sessions as individual treatments)
Home Health Agencies	• Billing for more visits than provided • Billing custodial care as skilled nursing services • Billing for services to patients who do not meet the definition of homebound
Hospice	• In-home hospice care: Cutting staff to a minimum to reduce the level of care and pressure family to place the patient in a hospice facility • Hospice facility care: Refusing to discharge a patient no longer eligible for hospice care or who wants to stop receiving hospice care • Private billing patients' families for drugs or procedures and then billing Medicare and/ or Medicaid
Clinical / Independent Physiological Laboratories	• Adding tests not ordered by the physician or splitting up panels of tests to bill for tests separately • Falsifying test results to substantiate the need for services

	• Using "rolling labs" to visit senior centers, elderly housing projects, or malls to offer "free" or unnecessary diagnostic tests and using Medicare numbers to bill Medicare
Hospitals	• Billing for tests, therapy, or supplies not provided to the patient • Misrepresenting the patient's condition on the claim form in order to obtain payment or higher payment • Holding patients under observation status in order to obtain higher payment (Note: Days under observation status will not count towards meeting Medicare's requirement for coverage in a skilled nursing facility after leaving the hospital.)
Nursing Facilities	• Billing for medical supplies not provided to the patient • Understaffing to reduce costs and neglecting necessary care • Falsifying documents to avoid liability (e.g. faking duty rosters and altering patient records)
Ambulances	• Falsifying documents to bill for non-emergency trips • Billing for advanced life support services when only basic life support services were provided • Listing ambulance transports as emergency services when ambulance was used as a taxi service

Durable Medical Equipment and Supplies	• Forging signatures on certificates of medical necessity • Offering free products or paying beneficiaries to get their Medicare number • Conspiring with practitioners and laboratories to falsify examination results to qualify for Medicare
Pharmacies	• Billing for drugs not medically necessary or actually not dispensed • Billing for brand name drugs but dispensing generics • Conspiring with Medicare beneficiaries and physicians to divert filled prescriptions to drug traffickers in exchange for a kickback • Selling fake, expired, or contaminated drugs through fraudulent online pharmacies
Medical Identity Theft	• Stealing Medicare beneficiary and provider numbers to steal identities and commit fraud • Selling Medicare numbers to criminals to use to falsely bill Medicare • Using another person's Medicare number to get medical services or prescription drugs

PREVENT MEDICARE FRAUD

Protect: Here are some ways to take an active role in protecting your healthcare benefits and preventing Medicare errors, fraud, and abuse:

- Protect your Medicare, Medicaid, and Social Security numbers. Your Medicare and Medicaid numbers are the same as your social security number. Be careful when you share this information.
- Record doctor visits, tests, and procedures in your personal healthcare journal (PHCJ) or calendar.
- Remember, Medicare doesn't call or visit to sell you anything.
- Don't be fooled. If it sounds too good to be true, it probably is.
- Read and save Medicare Summary Notices (MSN) and Part C and D Explanation of Benefits (EOB). Shred the documents when they are no longer useful.

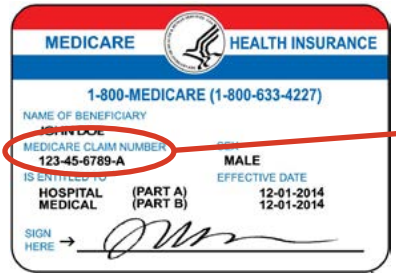
Detect: Learn to detect potential errors, abuse, and fraud. Here are some steps you can take:

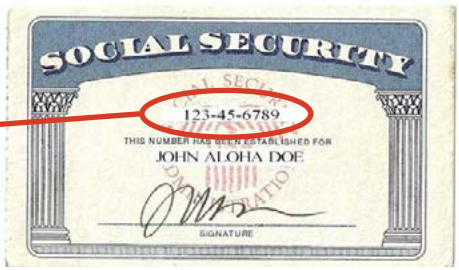
- Always review your MSN and EOB for mistakes.
- Compare your MSN and EOB to your personal healthcare journal and prescription receipts to make sure they are correct.
- Look for these three things in your billing statement:
    1. Charges for something you didn't receive
    2. Billing for the same thing twice
    3. Services and supplies that your doctor did not order

Report: If you find billing errors, or possible fraud, report it. You may prevent others from becoming victims and help to save your Medicare benefits.

- If you are not comfortable calling your provider or plan or are not satisfied with the response, call SMP Hawaii at (808) 586-7281 or toll free 1-800-296-9422 or visit us online at smphawaii.org.

- Your Medicare number is your Social Security number. You may be more willing to give out your Medicare number thinking that it is a random number assigned to you, but in reality, that number is 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.





- Fraud targeting the Medicare Advantage and 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 together to protect, detect, and report potential healthcare scams, fraud, abuse, and errors.

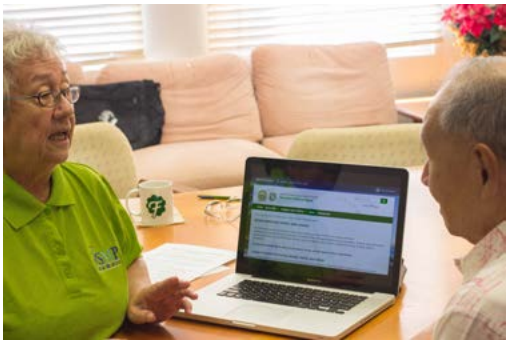
To be a part of the **Senior Medicare Patrol (SMP) Volunteer Program**, contact the volunteer coordinator at (808) 586-7319 or toll free at 1-800-296-9422.

Please contact **SMP Hawaii** if you have questions or concerns regarding potential healthcare scams, fraud, waste, abuse, or billing errors:

By Phone: (808) 586-7281 or toll-free at 1-800-296-9422
By Email: Report@SMPHawaii.org
Website: smphawaii.org

For more information, see the Resources section.

SMP HAWAII
State Executive Office on Aging



KEEPING OUR KUPUNA (SENIORS) SAFE

The largest generation in our nation's history, the Baby Boomers, are entering their senior years, and with it, our nation has seen increasing incidents of fraud against seniors. It may be in part due to the sheer number of people and their vast cumulative wealth that make the baby boomer seniors a preferred target. In addition, there is no denying that new technology has added an extra wrinkle to the mix. This section looks at 21st century fraud with a lens focused on seniors.

COMMON CONSUMER SCAMS AGAINST KUPUNA

Read through the list below. If you become familiar with these scams, it may help you and your loved ones to avoid them.

Relative in Need	Someone who pretends to be a family member or friend calls or emails you to say they are in trouble and needs you to wire money right away.
Charity Appeals	You get a call or letter from someone asking for money for a fake charity – either the charity does not exist or the caller was an imposter and the real charity did not call or write to you. *Learn more on page 34*
Lottery or Sweepstakes	You get a call or email saying that you have a chance to win a lot of money through a foreign country's sweepstakes or lottery. The caller will offer tips about how to win if you pay a fee or buy something. Or the caller or email says you have already won and you must give your bank account information or pay a fee to collect your winnings. *Learn more on page 27*
Home Improvement	Scammers take money for repairs and then they never return to do the work or they do bad work. Sometimes they break something to create more work or they say that things need work when they don't. *Learn more on page 36*
Free Lunch	Scammers invite you to receive a free lunch if you attend a seminar, and then pressure you to invest money with them. They offer you "tips" or "guaranteed returns."

Free Trip	Scammers say you've won a free trip but they ask for a credit card number or advance cash to hold the reservation.
Government Money	You get a call or letter that seems to be from a government agency. Scammers say that if you give a credit card number or send a money order, you can apply for government assistance with housing, home repairs, utilities, or taxes.
Drug Plans	Scammers pretend they are with Medicare prescription drug plans, and try to sell Medicare discount drug cards that are not valid. Companies with Medicare drug plans are not allowed to send unsolicited mail or email, or make unsolicited phone calls.
Identity Theft	Scammers steal personal information – such as a name, date of birth, social security number, account number, and mother's maiden name – and use the information to open credit card accounts, get a mortgage in someone else's name or otherwise use the false identity. *Learn more on page 51*
Fake "Official" Mail	Scammers send letters or emails that look like they are from a legitimate bank, business, or agency to try to get your personal information or bank account information. *Learn more on page 18*
Source: CFPB. Managing Someone Else's Money: Help For Trustees Under a Revocable Living Trust. Retrieved from http://files.consumerfinance.gov/f/201310_cfpb_lay_fiduciary_guides_trustees.pdf	

Remember, these are common scams. If one has happened to you, don't be embarrassed or afraid to report it. Many have been in your shoes. Report now to protect yourself and others.

WHERE TO GET HELP:

1. Your Local Police Department 9-1-1.
2. Federal Bureau of Investigation (808) 566-4300.
3. Better Business Bureau on Oahu at (808) 628-3950 or toll free from neighbor islands at 1-888-333-1593.
4. Department of the Attorney General, Tax and Charities Division (808) 586-1480.
5. Regulated Industries Complaints Office (808) 587-4272.

HELPFUL TIPS FOR KUPUNA

The tips below can work in many different circumstances and have a universal application:

- Slow it down. Find a way to take the information home and review it slowly. Tell the seller, "I will get back to you." Don't fall for the pressure tactic of urgency.
- Thoroughly understand the offer. Ask questions and do your research about the offer and those promoting the offer. Get clear and direct answers before you invest or pay. Don't rely on reputation or word of mouth alone.
- Understand the costs. Ask about the risks, obligations, and costs of any offer before getting involved. Ask about commissions, sales charges, maintenance or service charges, transaction or redemption fees and penalties associated with the investment.
- Beware of unrealistic promises. Promises that promote high returns in a short period of time with no risk are unrealistic. If it's too good to be true, it probably is.

- Take the emotion out of the equation. Scammers use emotions to confuse targets. They use feelings of friendship, pressure of financial fear, deep desires for security and so much more to lure targets into making bad financial decisions. Don't fall for it. Try to review offers without overwhelming emotions.
- Just say no. Don't be afraid to say "no."

TALKING STORY WITH OUR KUPUNA

Seniors are preferred targets of fraud. Why? Because seniors tend to have more financial assets and better lines of credit. Many seniors have saved for decades and have more free time for scammers to approach them. Some have physical impairments that scammers can leverage. The following section presents fraud in story form and then offers preventive tips that can help kupuna, family members, and caregivers.

A Story About

PONZI AND AFFINITY FRAUD:

Tutu, just say "No."

Tutu was a widow who had worked her whole life as a secretary and who also inherited a small nest egg from her late husband. She had been saving a long time but didn't have quite enough to take care of her needs and help her children. One day, she was approached by the head of her community center, Keoni. He said he knew she was financially struggling and that he could help.

Keoni told Tutu to invest in his cousin's new business and he promised her 10% returns every month so that she would have enough money to help her children.

Keoni told her she could ask the other long-time community center seniors about his offer because many of them had invested and made money. Sure enough, when Tutu asked her friends at the center, many vouched for Keoni and said they invested too and received interest regularly. Keoni also told her this was a very secret special deal only for his favorite seniors at the community center so she should not tell anyone outside of the center about it. When she asked how the business worked, he said it was too complicated to explain and that she should just trust him.

Tutu gave Keoni $10,000. After a few months, she received a little interest back but it wasn't the promised 10%. When she asked Keoni about it, he ignored her. After 6 more months, Keoni left the community center. When Tutu tried to get her money back, she found out that Keoni had convinced almost everyone in the center to invest and no one at the center could get their money back. In the end, it turned out Keoni had never invested the money in any business. Instead, he had run a **Ponzi scheme** where he took some of the new investors' money to pay off a little bit of interest to the earlier investors just to make them think that there really was a business. He spent the rest of the money on

his own personal expenses. He committed **affinity fraud**. He used friendships in a tight community to get Tutu and others in the group to trust him and invest in his Ponzi scheme.

Tutu filed a complaint with the Office of the Securities Commissioner and the Office started an investigation.

HELPFUL TIPS TO AVOID AFFINITY FRAUD

- Never make an investment solely based on the reputation of or "friendship" with a member of a group to which you belong.
- You can say "no" even to a friend. It is your money and you have a right to protect yourself.
- Beware of investment opportunities that sound too good to be true.
- Do not let a "friendship" stop you from getting the offer in writing and asking hard questions.
- Be suspicious if you are told NOT to share details of the investment with people outside of the group or to keep the investment opportunity confidential.
- Use common sense – just because someone you know made money or claims to have made money doesn't mean you will make money too.

A Story About

VARIABLE ANNUITIES:

Grandpa, your investment is locked up for 10 years.

Grandpa was 82 years old and attended a delicious free lunch seminar where a man named John introduced everyone to an investment opportunity to purchase **variable annuities**. Grandpa didn't know much about variable annuities, but John, the investment adviser and sales agent, told Grandpa to pay some money now and in return, Grandpa would receive a monthly payment for life! John was so nice, Grandpa just couldn't say no. John started to visit Grandpa at home regularly and would make time to talk to Grandpa about the family, bring manapua and snacks and make Grandpa feel he had a friend. John asked Grandpa to give him his social security number and sign blank forms to buy $75,000 in variable annuities. John reassured Grandpa that he would take care of everything and that Grandpa didn't need to worry about anything.

A couple months later, Grandpa needed money to pay for Grandma's medical bills. When he tried to get money out of his variable annuity, he found out John had sold him a variable annuity that was locked up for 10 years.

Grandpa would have to wait until he was 92 to get his money back or face a 40% penalty for early withdrawal.

Grandpa needed the money and so he took a 40% loss on his life savings. He lost $30,000 because John had sold him a product that was totally wrong for an 82 year old man.

Grandpa had no record of what he bought, he didn't know what he signed and he had no idea he'd be locked in and penalized.

Grandpa called the Office of the Securities Commissioner to file a complaint and an investigation was started.

CHECKLIST: PROTECT YOUR INVESTMENTS

- ☐ Ask about any lock-up period. If you are 82, you shouldn't be sold an investment that locks up your money for 10 years.
- ☐ Ask about penalties if you need your money back for unexpected expenses like medical bills or in-home care.
- ☐ Understand it before you buy it. Never be embarrassed to ask questions. If it's too confusing to understand, don't buy.
- ☐ Request a copy of the final signed document before handing over any money.
- ☐ Keep all of your records relating to your investments and instructions, including notes of conversations you have with your broker, sales agents, financial advisers, and others.
- ☐ For help or to report fraud, call the DCCA Securities Enforcement Branch at (808) 586-2740.

A Story About

LIFE SETTLEMENTS:

Grandpa, you made the right call.

Grandpa was worried about providing for his wife and family. He had an insurance policy of $500,000 and had been diagnosed with a long term illness. But he needed the money now. The insurance company said he could cash out for $150,000. He was thinking about it.

One day, he attended a free lunch seminar on life settlements. The speaker, Mr. Akito, came to Grandpa's table and after talking with Grandpa, he offered Grandpa a **life settlement**. Mr. Akito

would take over payments for Grandpa's policy and pay Grandpa a lump sum of $200,000 if Grandpa would make Mr. Akito the beneficiary. Grandpa would get $200,000 now but when Grandpa passed away, Mr. Akito would get the $500,000 policy. Grandpa asked for the contract in writing.

Then, Grandpa called a registered financial investment adviser and insurance agent, and asked about the deal. The adviser read the contract and told Grandpa that $200,000 was not a good price compared to the market. His adviser also warned Grandpa that the contract said Mr. Akito would get a whopping 30% commission and the fine print stated that Mr. Akito's company could resell Grandpa's policy to others which would include passing along all his private health records. In addition, Grandpa might lose his Medicaid benefits and pay high taxes if he were to get a lump sum.

Grandpa said NO to Mr. Akito's offer. The adviser helped Grandpa find other ways to get money upfront.

HELPFUL TIPS WHEN CONSIDERING LIFE SETTLEMENTS

- For complicated investments, work with a registered investment adviser to help you understand it. Call 808-586-2740 or go to brokercheck.finra.org to check if a professional is registered and to check background and complaint history.
- Be sure you understand how the life settlement works and what factors to consider. If you don't understand, don't buy it.
- Beware of aggressive sales tactics. Don't be afraid to say "No."

- Understand how taxes, social security, medicare and other benefits will be affected by the life settlement before you purchase.
- Ask questions:
    - What are the key terms to this agreement?
    - What company is actually responsible for fulfilling the terms of the agreement?
    - Are there other costs – fees, commissions, penalties, etc.?
    - Is this the best and fairest price for my policy?
    - Will my private health records be sold to anyone else?
    - What will happen if I change my mind? Is there a time limit?

REMINDER

Be sure to evaluate if a life settlement is beneficial given your specific situation – to keep or not to keep your current insurance policy. Either way, look at your options and proceed with much caution before purchasing a life settlement.

A Story About
INDEXED ANNUITIES:
Aunty Malia, you protected your life savings!

Aunty Malia was invited to a free lunch seminar about life insurance and annuities by her good friend Lisa. During the presentation, Lisa spoke about the benefits of investing in an indexed annuity based on the S&P 500. She said it was just like having the opportunity to invest in the best stocks on the New York Stock Exchange. Plus, she said that even if you don't get your profits, what you put in (also called the premium) is guaranteed up to 90% at a 3% interest rate. Lisa said this was a

once in lifetime opportunity to invest in the best indexed annuity she'd ever seen in her professional life.

Lisa explained that the annuity meant that Aunty Malia would pay a lump sum up front. In return, for the rest of her life, if she decided to annuitize, she would receive monthly payments based on all the gains of the S&P 500. It was like the best pension ever, and Lisa told Aunty Malia that at age 75, she had no time to waste in investing.

Aunty Malia was so excited. Lisa said this annuity was based on the best stocks on the New York Stock Exchange and it was guaranteed. How could she lose? Lisa pressed her to sign the paperwork right away in order to receive such a great deal. Lisa promised her if she signed up and changed her mind, she could get all her money back during the free look period.

Aunty Malia was just about to sign up but at the last minute, she decided to take the paperwork home and look more closely at it with her nephew who was a registered investment adviser and insurance agent.

He told her that indexed annuities are complex investments. He warned that the **indexed annuity** is NOT an actual investment in stocks but instead, an investment in the insurance company and its calculations on the gain or loss of a pool of stocks (called an "index"). He explained that an indexed annuity is a private contract between an insurance company and the buyer. The insurance company agrees to make periodic payments based on a variety of calculations modeled on the performance of an index.

He explained that one of the most confusing features is the method companies use to calculate the gain in the index (in Aunty Malia's case, the index was the S&P 500). It is never a straightforward dollar-to-dollar calculation. Formulas vary among companies and their complexity may make it difficult to compare and evaluate, even when they are based on the same index.

Her nephew also encouraged her to make sure she carefully reviewed the various costs associated with investing in an indexed annuity. It gave her 80% of any increase in the exchange (called a "participation rate" which varies widely among companies and contracts), put a cap on the maximum she could get (called an "interest rate cap") and also included a fee that would then be subtracted from any gains she received (called a "spread/ margin/asset fee"). He also warned that her contract said that the insurance company could change any of these terms without consulting her.

The "surrender period" for the annuity was 10 years, which meant that if she wanted or needed her lump sum investment back before she turned 85, she would pay a penalty rate. Based on her individual situation and finances, he was concerned that the annuity was not the right fit for Aunty Malia.

When Lisa called the next day to pressure Aunty Malia, Aunty Malia said "no." It was her life savings and she needed a different investment.

HELPFUL TIPS WHEN CONSIDERING INDEXED ANNUITIES

- Do not feel pressured to invest right away. Deals usually won't expire. If they do, you'll be able to find a similar deal elsewhere.
- Make sure the agent you're purchasing from is licensed. Just because they are a friend or family member, it does not mean that they're trustworthy or qualified to handle your finances.
- Annuities usually have long surrender periods compared to investments like a Certificate of Deposit (CD). Be sure to take this into consideration before tying your money up

long-term, and make sure you know the pros and cons of each investment vehicle.

- Investors have the right to a 10-day free look period after opening an annuity and 30-day free look period for a replacement. During this period of time, the contract can be returned without a penalty, and you will get 100 percent of your principal returned to you. Even though you can receive a refund, don't buy the investment until you are sure you want to keep it. Refunds are never easy and deadlines can expire before you know it.
- Shop around and get help from a trusted financial adviser, agent or accountant to help understand all the fine print. Call the DCCA Securities Enforcement Branch at (808) 586-2740 or go to brokercheck.finra.org to check if a professional is registered and to check his or her background and complaint history.
- If you are truly interested in the investment, ask about "participation rates," "spread/margin/asset" fees, "interest rate caps," and the "surrender period." Ask how any gains are actually calculated, and whether or not the insurance company has the power to change any of these important terms after you're locked into the investment.
- Remember, you are buying something from an insurance company, not stocks. If you buy, you should be sure you trust the insurance company.

A Story About **MEDICARE:**

Tutu! Remember, your Medicare card number is your social security number!

People have been calling Tutu on the phone, mailing her requests, coming to her door, emailing her, and even trying to get her

attention through commercials on late night television.

Tutu told her brother what great deals everyone was offering her. "They want to give me something for free or a very discounted price and all they need is my Medicare number." Her brother stopped her and reminded her that her Medicare number is her social security number. "That's how Medicare and identity theft happens," he told her. Tutu started saying "No!" to all the solicitations.

HELPFUL TIPS REGARDING MEDICARE

- Your Medicare Number is your personal information. It is actually the same as your Social Security number and you should never give it to anyone you don't know or trust. It is more important to thieves than a credit card or bank account number.
- Beware of people that you don't know calling, mailing, approaching you in person, emailing, and requesting personal information. Hang up the phone, shred all personal information, walk away, delete, and just say "no." Bottom line, be very careful to whom you give your personal information.
- Medicare will only call you if you contacted them first or to follow up on a complaint. Medicare will not contact you to sell you a product, service, or health plan. Don't be fooled by fake calls trying to get you to disclose your information.
- Don't let those commercials fool you. Medicare will only pay for medical supplies if they are medically necessary and your physician approves it. If you need medical equipment or services, go to your doctor who you know and trust.
- If something sounds too good to be true, it probably is.

A Story About
CHARITY:
Tutu, be careful with donations

Tutu received phone calls asking her to make a contribution to help out all the families affected by a typhoon in Japan. The caller said the money was needed immediately and that it would be easy to make a contribution over the phone, if Tutu would give them her social security number and bank account number, or she could just mail cash to them.

Tutu was about to give them her money when she remembered to ask the name of the charity and to tell the caller she would have to check with the State Charity Registry. The caller abruptly hung up and Tutu was safe.

HELPFUL TIPS FOR CHARITABLE GIVING

- Police Departments, Fire Departments, and other government agencies do not call members of the public asking for funds.
- If you receive a phone call asking for money for a charitable purpose, ask for the name of the charitable organization.
- Ask where the charity is located.
- Ask if the person calling you is an employee, volunteer, or telemarketer for the charitable organization.
- If the caller is a telemarketer for the charity, ask how much of your donation will go to the charity.
- Never give personal information over the phone.

- If you decide to make a donation, write a check. Do not send cash or wire transfer money.
- Check if the charity is registered in the State Charity Registry database at http://ag.ehawaii.gov/charity. All charities in Hawaii that solicit have to be registered with the Tax and Charities Division of the Department of the Attorney General.
- If you have questions about the charity or to report fraud, call the Attorney General Tax and Charities Division at (808) 586-1480.

KUPUNA ONLINE
How to be safer

There are risks for everyone online, and it's no different for kupuna. Remember, opening unsafe attachments or downloads from the Internet are the two most common ways viruses, spyware, worms and other malware are used to infect your computer, destroy your property and steal your information. Be very careful with opening attachments and downloads. For more information on Adware and Malware, please see page 11.

RED FLAGS FOR KUPUNA ONLINE

Look out for the following types of emails, websites, or social media messages that:

- Offer "free" gifts, prizes or vacations, or exclaim, "You're a winner!"
- Offer discount prescription medications or other "can't miss" deals.
- Appear to be from friends or family members, but the message is written in a style not usually used by that person, has numerous misspellings, or otherwise seems unusual. This is an indication your friend's or family member's account may have been hacked.
- Appear to be from official government agencies, such as Social Security Administration, or IRS, but request personal information online.
- Set ultimatums such as "your account will be closed," or "the deal will expire" to create a sense of urgency to lure you into providing personal information.
- Unexpected pop up screens that tell you to call a number to help "fix" your computer.

KEEP A CLEAN COMPUTER

- Keep software updated. Install the latest security software, web browser and operating system on your computer. Enable the auto-update feature to ensure you have the most up-to-date security software.

PROTECT YOUR WIRELESS NETWORK

- Create a secure password for your wireless router. A secure password includes a mix of capital and lower case letters, numbers and symbols. Do not use your name or birthdate.

BE WEB WISE

- When in doubt, throw it out. Links and attachments in emails, social media posts, and online ads are often how scammers access your computer. If you are instructed to click on a link or attachment in a message you don't trust, even if you know the sender, delete the message or mark it as junk mail.
- Back it up. Store valuable work, photos, music and other information on an external hard drive and/or online in the "cloud."

Source: Multi-State Newsletter. Keeping Senior Citizens Safe Online.
http://msisac.cisecurity.org/newsletters/2013-06.cfm

KUPUNA ALERT PARTNERS (KAP) EDUCATIONAL PRESENTATIONS

Kupuna Alert Partners is a state multi-agency partnership that offers presentations on Medicare fraud prevention, securities fraud prevention, and prescription drug misuse to the community. If you are interested in scheduling a presentation with your senior group, please call (808) 586-1487. Please see page 112 for more information.

CAREGIVERS

Today, more family and friends are becoming caregivers to our Kupuna (seniors). Caregiving can be a huge responsibility. To help caregivers understand their roles and responsibilities, this section reviews the different fiduciary relationships.

WHAT IS A FIDUCIARY?

If you have been named to manage money or property for someone else, you are a **fiduciary**. The law requires you to manage your family member's or a friend's money and property for his or her benefit, not yours. It does not matter if you are managing a lot of money or a little. It does not matter if you are a family member or not.

The role of a fiduciary carries with it legal responsibilities. When you act as a fiduciary for your family and friends, you have four basic duties that you must keep in mind:

1. Act only in the best interest of your family or friend
2. Manage his or her money and property carefully and in his or her best interest
3. Keep money and property separate from yours
4. Keep clear and accurate records

As a fiduciary, you must be trustworthy, honest, and act in good faith. If you do not meet these standards, you could be removed as a fiduciary, sued, or have to repay money. It is even possible that the police or sheriff could investigate you and you could go to jail. That's why it's always important to remember: It's not your money or property.

DIFFERENT TYPES OF FIDUCIARIES

In your role as agent, you may act as or deal with other types of fiduciaries. These may include:

- **Trustees under a revocable living trust** – someone names them to manage money and property.
- **Representative payees or, for veterans, VA fiduciaries** – a government agency names them to manage government money that is paid to someone.
- **Guardians or conservators** – a court names them to manage money and property for someone who needs help.

For more information about the duties of these fiduciaries, go to: consumerfinance.gov/managing-someone-elses-money

Source: CFPB. Managing Someone Else's Money: Help For Agents Under a Power of Attorney. Retrieved from http://files.consumerfinance.gov/f/201310_cfpb_lay_fiduciary_guides_agents.pdf

PROTECTING OUR KUPUNA

Caregiving for a loved one can be difficult. Often times, caregivers are juggling their own personal schedules and finances with that of their loved one's finances and health concerns.

Protecting your loved one's assets and knowing your rights as a caregiver are both important. With the increased number of cases of senior fraud, law enforcement, regulatory agencies, financial institutions and others are keeping a watchful eye out for any misuse of personal funds, and the medical and financial well-being of seniors. It's good to know there are others looking out for seniors but prevention still starts at home with the seniors and their caregivers.

We hope the following tips will help provide you with the resources you need to address the safety, healthcare and financial well-being for both your loved one and you, the caregiver.

HELPFUL TIPS FOR FAMILY MEMBERS AND CAREGIVERS

- Regularly evaluate how things are going for your loved one. Have them get a medical, financial and household evaluation periodically and check in with frequent calls and in-person visits.
- Share information about popular scams with your senior one and educate yourself on important issues such as protecting personal information, and how to report possible scams promptly. Check out the resources in this Guide for more information.
- Practice with your kupuna how to say "no" to solicitors. For example, you could work on a script like this: " No thank you, I have a family member/personal financial advisor/attorney who reviews everything before I make a decision."
- Use tools such as an answering machine and caller ID to cut down on the opportunity for possible scams.
- Organize everyone's medical information and legal documents so it's up to date and easy to find.
- Invest in a shredder and shred all discarded documents with your kupuna's personal information on them.
- Determine ways to simplify your kupuna's finances and consider a system for oversight. Consider regular reviews of financial and medical statements by a trusted professional or family member and report suspicious charges or errors right away.
- If possible, do not mail any documents with personal information from you or your kupuna's personal

mailbox with the flag up for thieves to see. Instead, drop it off at the post office or in a secured designated USPS mail box.

- It's very important for you to seek support from other caregivers. You are not alone! Accept offers of help.

Source: Caregiver Action Network. 10 Tips for Family Caregivers. Retrieved from http://caregiveraction.org/resources/10-tips-family-caregivers

REMINDER

Caregivers: give yourself credit for doing the best you can in one of the toughest jobs there is!

WARNING SIGNS TO INDICATE POSSIBLE FINANCIAL ABUSE OF ELDERLY

⚠ Appears worried about their finances; talks about unanticipated financial problems.

⚠ Is having unexplained purchases; missing cash or valuables.

⚠ Has difficulty or confusion over purchases; appearance of service contracts, excessive repairs or excessive new items being purchased for the home.

⚠ Unexpectedly gives financial control to a new caregiver, neighbor, or friend.

⚠ Shows signs of fear or intimidation signals (mentioning for example, that the person helping them with their finances "doesn't want me to talk about that" or doesn't allow them to review their own checkbook, accounts or statements).

Source: Aging Wisely. Phishing Scams, Identity Theft Fraud and Elder Abuse. Retrieved from om http://www.agingwisely.com/scams-on-the-elderly-senior-care-tips-for-fraud-prevention/

WHERE TO GET HELP
FOR KUPUNA (SENIORS) AND CAREGIVERS

If you need help or have questions, below is a list of agencies that can help. Learn more about these agencies in our resource section on page 113.

BETTER BUSINESS BUREAU OF HAWAII, INC.

1132 Bishop Street, Suite 615, Honolulu, HI 96813
HOTLINE: (808) 628-3950
TOLL-FREE: 1-888-333-1593
FAX: (808) 628-3970
WEBSITE: bbb.org/hawaii

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)
Office For The Older American

1625 Eye Street, NW, Washington DC 20552
PHONE: (202) 435-7121
TOLL-FREE: 1-855-411-2372
WEBSITE: consumerfinance.gov

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
WEBSITE: investing.hawaii.gov

DEPARTMENT OF HEALTH (DOH)
Executive Office On Aging

250 S. Hotel Street, Suite 406, Honolulu, HI 96813

PHONE: (808) 586-0100
FAX: (808) 586-0185
WEBSITE: health.hawaii.gov/eoa

HAWAII AGING AND DISABILITY RESOURCE CENTER (ADRC)

PHONE: (808) 643-2372
WEBSITE: hawaiiadrc.org

SENIOR MEDICARE PATROL (SMP) HAWAII

PHONE: (808) 586-7281
TOLL-FREE: 1-800-296-9422
WEBSITE: smphawaii.org/

DEPARTMENT OF HUMAN SERVICES (DHS)
Adult Protective And Community Services Branch

OAHU: 420 Waiakamilo Road #202, Honolulu, HI 96817
PHONE: (808) 832-5115
FAX: (808) 832-5391

HILO: 1055 Kinoole Street #201, Hilo, HI 96720
PHONE: (808) 933-8820
FAX: (808) 933-8859

KONA: 75-5995 Kuakini Highway #433, Kailua-Kona, HI 96740
PHONE: (808) 327-6280
FAX: (808) 327-6292

KAUAI: 4370 Kukui Grove Street #203, Lihue, HI 96766
PHONE: (808) 241-3337
FAX: (808) 241-3476

MAUI: 1773-B Wili Pa Loop, Wailuku, HI 96793
PHONE: (808) 243-5151
FAX: (808) 243-5166

WEBSITE: humanservices.hawaii.gov/ssd/home/adult-services/

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
WEBSITE: ag.hawaii.gov/cjd/
WEBSITE: ag.hawaii.gov/cjd/medicaid-fraud-control-unit/

DEPARTMENT OF THE ATTORNEY GENERAL
Tax And Charities Division

425 Queen Street, Honolulu, HI 96813
PHONE (808) 586-1480
FAX: (808) 586-8116
WEBSITE: ag.hawaii.gov/tax
CHARITIES REGISTRY: ag.ehawaii.gov/charity/welcome.html

DEPARTMENT OF THE PROSECUTING ATTORNEY
City and County of Honolulu
Elder Abuse Justice Unit

1060 Richards Street, Honolulu, HI 96813
PHONE (808) 768-7400
WEBSITE: honoluluprosecutor.org/elder-abuse-justice-unit

KUPUNA ALERT PARTNERS (KAP)

KAP was formed as a partnership between Department of the Attorney General, Department of Commerce and Consumer Affairs, Department of Health, and Department of Public Safety.
PHONE (808) 586-1487
WEBSITE: ag.hawaii.gov/cpja/ccp

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 online.

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

STATE AND COUNTY GOVERNMENT OFFICES ARE OPEN MONDAY – FRIDAY 7:45 A.M. – 4:30 P.M. EXCEPT STATE AND FEDERAL HOLIDAYS.

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) 768-7705
HOTLINE: (808) 768-7700
FAX: (808) 768-7720 or (808) 527-6895
WEBSITE: elderlyaffairs.com

DESCRIPTION: The Elderly Affairs Division (EAD), a division of the Department of Community Services of the City and County of Honolulu, is your local Area Agency on Aging. Its purpose is to plan, support and advocate for programs to promote the well-being of Oahu's older adults and caregivers and to address and respond to the priority needs of all seniors.

DEPARTMENT OF THE PROSECUTING ATTORNEY

1060 Richards Street, Honolulu, HI 96813
PHONE: (808) 768-7400
FAX: (808) 768-7515
WEBSITE: honoluluprosecutor.org

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.

HONOLULU POLICE DEPARTMENT
Criminal Investigation Division

Alapai Headquarters, 801 S. Beretania Street, Honolulu, HI 96813
PHONE: 9-1-1
ADDITIONAL CONTACT NUMBERS: (808) 723-3609
FAX: (808) 768-1680
WEBSITE: honolulupd.org

DESCRIPTION: Offers informational and educational presentations about how to protect against identity theft, credit card fraud, forgery, cybercrime and related subjects. Investigates various types of financial crimes including forgery, fraudulent use of credit cards, identity theft, computer crimes, cybercrime and elderly financial abuse.

COUNTY RESOURCES
Hawaii County

HAWAII COUNTY OFFICE OF AGING

HILO: 1055 Kinoole Street, Suite 101, Hilo, HI 96720
PHONE: (808) 961-8600
FAX: (808) 961-8603

KONA: 74-5044 Ane Keohokalole Hwy, Building B (1st Floor), Kona, HI 96740
PHONE: (808) 323-4390
FAX: (808) 323-4398

WEBSITE: hcoahawaii.org
EMAIL: hcoa@hawaiiantel.net

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.

HAWAII POLICE DEPARTMENT
Criminal Investigation Division

349 Kapiolani Street, Hilo, HI 96720
PHONE: (808) 935-3311 or 9-1-1
ADDITIONAL CONTACT NUMBERS:
HILO: (808) 961-2251
KONA: (808) 326-4646 ext. 268
FAX: (808) 961-2376
WEBSITE: hawaiipolice.com
EMAIL: rwagner@hawaiicounty.gov

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.

OFFICE OF THE PROSECUTING ATTORNEY

HILO: 655 Kilauea Avenue, Hilo, HI 96720
PHONE: (808) 961-0466 (main office)
FAX: (808) 961-8908

KONA: 81-980 Halekii Street, Suite 150, Kealakekua, HI 96750
PHONE: (808) 322-2552
FAX: (808) 322-6584

WAIMEA: 64-1067 Mamalahoa Hwy, Kamuela, HI 96743
PHONE: (808) 887-3014
FAX: (808) 887-3016

WEBSITE: hawaiicounty.gov/prosecuting-attorney
EMAIL: hilopros@co.hawaii.hi.us

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

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: kauaiadrc.org
EMAIL: elderlyaffairs@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.

KAUAI POLICE DEPARTMENT

3990 Kaana Street, Suite 200, Lihue, HI 96766
PHONE: (808) 241-1711 or 9-1-1
ADDITIONAL CONTACT NUMBERS:
INVESTIGATIVE SERVICES: (808) 241-1633
COMMUNITY RELATIONS: (808) 241-1669

FAX: (808) 241-1714
WEBSITE: kauai.gov/police

DESCRIPTION: Conducts investigations of fraud, theft, and associated crimes. Gives presentations to seniors on various topics such as protection against fraud, elder abuse, and neighborhood watch meetings.

OFFICE OF THE PROSECUTING ATTORNEY

3990 Kaana Street, Suite 210, Lihue, HI 96766
PHONE: (808) 241-1888
FAX: (808) 241-1758
WEBSITE: kauai.gov/prosecutingattorney
EMAIL: prosecutor@kauai.gov

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.

COUNTY RESOURCES
Maui County

DEPARTMENT OF THE PROSECUTING ATTORNEY

150 S. High Street, Wailuku, HI 96793-2155
PHONE: (808) 270-7777
FAX: (808) 270-7625
WEBSITE: co.maui.hi.us/departments/prosecuting/
EMAIL: prosecuting.attorney@mauicounty.gov

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.

MAUI COUNTY OFFICE ON AGING

95 Mahalani Street, Room 20, Wailuku, HI 96793
PHONE: (808) 270-7755
FAX: (808) 270-7935
WEBSITE: mauicounty.gov
EMAIL: aging@mauicounty.gov

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).

MAUI POLICE DEPARTMENT

55 Mahalani Street, Wailuku, HI 96793-2155
PHONE: (808) 244-6400 or 9-1-1
FAX: (808) 244-5576
WEBSITE: co.maui.hi.us/departments/police
EMAIL: crs@mpd.net

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

STATE RESOURCES

AARP HAWAII

1132 Bishop Street, Suite 1920, Honolulu, HI 96813
PHONE: (808) 545-6000
TOLL-FREE: 1-866-295-7282
FAX: (808) 537-2288
WEBSITE: aarp.org/money/scams-fraud/
HAWAII WEBSITE: aarp.org/states/hi/
EMAIL: hiaarp@aarp.org

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.

BETTER BUSINESS BUREAU OF HAWAII, INC.

1132 Bishop Street, Suite 615, Honolulu, HI 96813
PHONE: (808) 536-6956
FRAUD HOTLINE: (808) 628-3950
TOLL-FREE: 1-888-333-1593
FAX: (808) 628-3970
WEBSITE: bbb.org/hawaii
EMAIL: info@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.

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) 586-1444
FAX: (808) 586-1097
WEBSITE: ag.hawaii.gov/cpja
EMAIL: hawaiiag@hawaii.gov

DESCRIPTION: The Community & Crime Prevention Branch is responsible for the planning and implementation of informational and educational workshops and activities focused on community crime prevention. While criminal justice agencies can respond to crimes, it is the neighborhoods and communities that can help to prevent and reduce crimes. This is facilitated by the Branch providing information and training on how individuals, businesses, agencies/organizations, and communities can get involved.

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.

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
WEBSITE: ag.hawaii.gov/cjd
WEBSITE: ag.hawaii.gov/cjd/medicaid-fraud-control-unit/

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.

DEPARTMENT OF THE ATTORNEY GENERAL
Investigations Division
Hawaii Internet Crimes Against Children (ICAC)

235 S. Beretania Street, 16th Floor, Honolulu, HI 96813
PHONE: (808) 587-4111
FAX: (808) 587-4118
WEBSITE: ag.hawaii.gov/hicac
EMAIL: atg.icac@hawaii.gov

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.

The Hawaii ICAC Task Force is part of a cooperative nationwide network of ICAC Task Forces that are dedicated to protecting children in the online environment. In order to accomplish this goal, our ICAC Task Force makes Internet education, safety programs and information available for Hawaii's children, teachers and parents. If prevention efforts fail, Hawaii's ICAC Task Force investigates

and prosecutes persons who victimize children through the use of computers and the Internet. The ICAC Task Force also takes CyberTip complaints through a nationwide CyberTip line that is operated by the National Center for Missing and Exploited Children (NCMEC).

DEPARTMENT OF THE ATTORNEY GENERAL
Tax And Charities Division

425 Queen Street, Honolulu, HI 96813
PHONE: (808) 586-1480
FAX: (808) 586-8116
WEBSITE: ag.hawaii.gov/tax
CHARITIES REGISTRY: ag.ehawaii.gov/charity/welcome.html

DESCRIPTION: The Tax and Charities 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.

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)

Consumer Education Program

King Kalakaua Building, 335 Merchant Street, Honolulu, HI 96813
WEBSITE: cca.hawaii.gov

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 (March), Military Consumer Protection Day Fair (July), and participates in senior fairs and community events throughout the state (year round).

CONSUMER INFORMATION LINE

PHONE: (808) 587-1234
NEIGHBOR ISLAND: To contact the consumer information line, neighbor island 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.

DESCRIPTION: 24-hour, automated system that contains pre-recorded consumer messages.

OFFICE OF CONSUMER PROTECTION DIVISION (OCP)

OAHU: 235 S. Beretania Street, Suite 801, Honolulu, HI 96813
PHONE: (808) 586-2630
FAX: (808) 586-2640

HILO: 120 Pauahi Street, Suite 212, Hilo, HI 96720
PHONE: (808) 933-0910
FAX: (808) 933-8845

MAUI: 1063 Lower Main Street, Suite C-216, Wailuku, HI 96793
PHONE: (808) 243-4648
FAX: (808) 243-5807

NEIGHBOR ISLAND: To contact the Oahu OCP office, neighbor island 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.

WEBSITE: cca.hawaii.gov/ocp
EMAIL: ocp@dcca.hawaii.gov

DESCRIPTION: Investigates consumer complaints alleging unfair or deceptive business practices and conducts civil enforcement actions against violations of Hawaii's consumer protection laws.

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.
WEBSITE: cca.hawaii.gov/ocp/landlord_tenant
EMAIL: ocp@dcca.hawaii.gov

DESCRIPTION: Call for information on landlord-tenant matters.

REGULATED INDUSTRIES COMPLAINTS OFFICE DIVISION (RICO)

OAHU: 235 S. Beretania Street, 9th Floor, Honolulu, HI 96813
PHONE: (808) 587-4272

HILO: 120 Pauahi Street, Suite 212, Hilo, HI 96720
PHONE: (808) 933-8846

KONA: 75-170 Hualalai Road, Room C309, Kailua-Kona, HI 96740
PHONE: (808) 327-9590

KAUAI: 3060 Eiwa Street, Room 204, Lihue, HI 96766
PHONE: (808) 274-3200

MAUI: 1063 Lower Main Street, Suite C-216, Wailuku, HI 96793
PHONE: (808) 243-5808

NEIGHBOR ISLAND: To contact the RICO office toll-free, residents may call the following numbers, followed by 7-4272 and the # key: **HAWAII** (808) 974-4000, **KAUAI** (808) 274-3141, **MAUI** (808) 984-2400, **LANAI & MOLOKAI** 1-800-468-4644.

WEBSITE: cca.hawaii.gov/rico
EMAIL: rico@dcca.hawaii.gov

DESCRIPTION: Investigates and prosecutes complaints relating to licensed professionals and unlicensed activity.

CONSUMER RESOURCE CENTER

PHONE: (808) 587-4272
TOLL-FREE: 1-800-394-1902
WEBSITE: cca.hawaii.gov/resources/

DESCRIPTION: For questions about filing a complaint against a professional or vocational licensee, or to report unlicensed activity. Provides helpful information to consumers on a variety of topics, including hiring a licensed contractor and protecting yourself against unlicensed activity. CRC also accepts complaints for the Office of Consumer Protection.

LICENSE, BUSINESS, AND INFORMATION SECTION (LBIS)

PHONE: (808) 587-4272, Press 2
WEBSITE: businesscheck.hawaii.gov

DESCRIPTION: One stop for information. Consumers can get basic business registration information, find out if a business or individual is licensed, and get information about complaints filed with RICO and OCP.

DCCA ONLINE SERVICES

WEBSITE: cca.hawaii.gov/resources/

DESCRIPTION: Search online 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)

335 Merchant Street, Suite 201, Honolulu, HI 96813
WEBSITE: cca.hawaii.gov/breg
EMAIL: breg@dcca.hawaii.gov

BUSINESS ACTION CENTER (BAC)

OAHU: 1130 N. Nimitz Highway, Suite A-220, Honolulu, HI 96817
PHONE: (808) 586-2545
FAX: (808) 586-2544

HILO: 100 Pauahi Street, Suite 109, Hilo, HI 96720
PHONE: (808) 933-0773
FAX: (808) 933-0778

MAUI: 70 E. Kaahumanu Ave, Unit B-9, Kahului, HI 96732
PHONE: (808) 873-8247
FAX: (808) 871-9160

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.

WEBSITE: cca.hawaii.gov/breg
EMAIL: bac@dcca.hawaii.gov

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.

OFFICE OF THE SECURITIES COMMISSIONER (OSC)

335 Merchant Street, Suite 203, Honolulu, HI 96813

INVESTOR EDUCATION PROGRAM (IEP)

PHONE: (808) 587-7400
WEBSITE: investing.hawaii.gov
EMAIL: iep@dcca.hawaii.gov

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. State coordinator for LifeSmarts Consumer Education Competitions. Hosts Annual Financial Literacy Fair (April), offers free investor education presentations and participates in statewide community fairs and events.

SECURITIES COMPLIANCE BRANCH (SEC)

PHONE: (808) 586-2722
WEBSITE: investing.hawaii.gov

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

SECURITIES ENFORCEMENT BRANCH (SEB)

PHONE: (808) 586-2740
FRAUD HOTLINE: (808) 587-2267
TOLL-FREE: 1-877-447-2267
WEBSITE: investing.hawaii.gov

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

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

335 Merchant Street, Suite 213, Honolulu, HI 96813
PHONE: (808) 586-2790
FAX: (808) 587-6714
WEBSITE: cca.hawaii.gov/ins
EMAIL: insurance@dcca.hawaii.gov

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.

INSURANCE FRAUD HOTLINE

PHONE: (808) 587-7416
NEIGHBOR ISLAND: To contact the insurance fraud hotline, neighbor island 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.
WEBSITE: cca.hawaii.gov/ins
EMAIL: insurance@dcca.hawaii.gov

DESCRIPTION: Call to report actual or suspected insurance fraud.

DEPARTMENT OF HEALTH
Executive Office on Aging

250 S. Hotel Street, Suite 406, Honolulu, HI 96813
PHONE: (808) 586-0100
FAX: (808) 586-0185
WEBSITE: health.hawaii.gov/eoa
EMAIL: eoa@doh.hawaii.gov

DESCRIPTION: The Executive Office on Aging (EOA) is the designated lead agency in the coordination of a statewide system of aging and caregiver support services in the State of Hawaii, as authorized by federal and state laws.

HAWAII AGING AND DISABILITY RESOURCE CENTER (ADRC)

PHONE: (808) 643-2372
WEBSITE: hawaiiadrc.org

DESCRIPTION: Hawaii's Aging and Disability Resource Center (ADRC) helps older adults, individuals with disabilities, and family caregivers find options for long term supports and services available to them in the State of Hawaii.

SENIOR MEDICARE PATROL (SMP) HAWAII

PHONE: (808) 586-7281
TOLL-FREE: 1-800-296-9422
WEBSITE: smphawaii.org
EMAIL: smphi@doh.hawaii.gov

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. To volunteer for SMP, contact 586-7319.

DEPARTMENT OF HUMAN SERVICES (DHS)
Adult Protective and Community Services Branch

OAHU: 420 Waiakamilo Road, #202, Honolulu, HI 96817
PHONE: (808) 832-5115
FAX: (808) 832-5391
EMAIL: ssdoahuapcs@dhs.hawaii.gov

HILO: 1055 Kinoole Street, Suite 201, Hilo, HI 96720
PHONE: (808) 933-8820
FAX: (808) 933-8859
EMAIL: ssdeasthipcs@dhs.hawaii.gov

KONA: 75-5995 Kuakini Highway, Suite 433, Kailua-Kona, HI 96740
PHONE: (808) 327-6280
FAX: (808) 327-6292
EMAIL: ssdwesthipcs@dhs.hawaii.gov

KAUAI: 4370 Kukui Grove Street, Suite 203, Lihue, HI 96766
PHONE: (808) 241-3337
FAX: (808) 241-3476
EMAIL: ssdkauaipcs@dhs.hawaii.gov

MAUI: 1773-B Wili Pa Loop, Wailuku, HI 96793
PHONE: (808) 243-5151
FAX: (808) 243-5166
EMAIL: ssdmauipcs@dhs.hawaii.gov

WEBSITE: humanservices.hawaii.gov/ssd/home/adult-services/

DESCRIPTION: The Adult Protective Services (APS) Program provides crisis intervention, investigation and emergency services to vulnerable adults who are reported to be abused, neglected, or financially exploited by others or seriously endangered due to self-neglect.

DEPARTMENT OF PUBLIC SAFETY
Narcotics Enforcement Division (NED)

PHONE: (808) 837-8470
WEBSITE: dps.hawaii.gov/about/divisions/law-enforcement-division/ned
EMAIL: hawaiicsreg@ned.hawaii.gov

DESCRIPTION: The Narcotics Enforcement Division (NED) is a statewide law enforcement agency that serves and protects the public by enforcing State laws pertaining to controlled substances and regulated chemicals. They are responsible for the registration and control of the manufacture, distribution, prescription, and dispensing of controlled substances and precursor or essential chemicals within the State.

NED is also responsible for assuring that pharmaceutical controlled substances are used for legitimate medical purposes. They register and investigate all violation of persons who administer, prescribe, manufacture or dispense controlled substances in the State, including those who work at methadone clinics.

NATIONAL RESOURCES

ADULT PROTECTIVE SERVICES

1700 G Street, NW, Washington DC 20552
PHONE: (800) 677-1116

DESCRIPTION: Find the state or local agencies that receive and investigate reports of suspects elder or adult abuse, neglect, or exploitation by contacting the national Eldercare Locator.

ANTI-FRAUD HOTLINE

PHONE: (855) 303-9470
WEBSITE: aging.senate.gov/fraud-hotline

DESCRIPTION: The Committee's investigators have experience in fraud concerning retirement savings, identity theft, phone scams, Medicare, Social Security, and a variety of other consumer issues important to seniors and the elderly.

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB) Office For The Older American

1625 Eye Street, NW, Washington DC 20552
PHONE: (202) 435-7121
TOLL-FREE: (855) 411-2372
WEBSITE: consumerfinance.gov

DESCRIPTION: Ensures that consumers get the information they need to make the financial decisions they believe are best for themselves and their families—that prices are clear up front, that risks are visible, and that nothing is buried in fine print. In a market that works, consumers should be able to make direct comparisons among products and no provider should be able to use unfair, deceptive, or abusive practices.

DIRECT MARKETING ASSOCIATION (DMA) Mail Preference Service

P.O. Box 643 Carmel, NY 10512
PHONE: 1-888-567-8688
WEBSITE: dmachoice.org

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

FEDERAL BUREAU OF INVESTIGATION (FBI)

OAHU: 91-1300 Enterprise Street, Kapolei, HI 96707
PHONE: (808) 566-4300
FAX: (808) 566-4470

KONA: 75-5591 Palani Road, Suite 2008A, Kailua-Kona, HI 96740
PHONE: (808) 329-5105

MAUI: 2200 Main Street, Wailuku, HI 96793
PHONE: (808) 242-4849
WEBSITE: fbi.gov/honolulu
WEBSITE: fbi.gov/scams-safety/e-scams

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: 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. It provides a place for citizens to report consumer complaints that help the FTC investigate frauds that in some cases lead to law enforcement action.

FINANCIAL INDUSTRY REGULATORY AUTHORITY (FINRA)

1735 K Street, Washington, DC 20006
PHONE: (301) 590-6500
WEBSITE: finra.org

DESCRIPTION: FINRA, the Financial Industry Regulatory Authority, is the largest independent regulator for all securities firms doing business in the United States. FINRA touches virtually every aspect of the securities business – from registering and educating all industry participants to examining securities firms, writing rules, enforcing those rules and the federal securities laws, informing and educating the investing public, providing trade reporting and other industry utilities, and administering the largest dispute resolution forum for investors and firms. If you believe you have been defrauded or treated unfairly by a securities professional or firm, please file a complaint online or via mail or fax. See the Complaint Center at finra.org for more information.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS (NAIC)

1100 Walnut Street, Suite 1500, Kansas City, MO 64106
PHONE: (816) 783-8300
FAX: (816) 460-7593
WEBSITE: naic.org

DESCRIPTION: The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories.

NATIONAL CRIME PREVENTION COUNCIL (NCPC)

2001 Jefferson Davis Hwy, Suite 901, Arlington, VA 22202-4801
PHONE: (202) 466-6272
FAX: (202) 296-1356
WEBSITE: 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.

NATIONAL DO NOT CALL REGISTRY

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

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
WEBSITE: nasaa.org
EMAIL: info@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.

OPTOUTPRESCREEN.COM

P.O. Box 2033 A-Rock Island, IL 61204-2033
TOLL-FREE: 1-888-567-8688
WEBSITE: optoutprescreen.com

DESCRIPTION: Enrollment to "Opt-Out" of pre-approved offers of credit or insurance from lists supplied by Equifax, Experian, 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) 449-7759
EMAIL: afosi.det601.office@ogn.af.mil

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: 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. The U.S. Attorney's Office normally prosecutes cases that are referred by a federal law enforcement agency.

UNITED STATES COMMODITY FUTURES TRADING COMMISSION (CFTC)

1155 21st Street, NW, Washington DC 20581
PHONE: (202) 418-5000
TOLL-FREE: 1-866-366-2382
WEBSITE: www.smartcheck.gov

DESCRIPTION: The mission of the CFTC is to protect investors, traders and the public from fraud in the commodity futures and options markets. It accomplishes this by educating consumers about the futures markets, notifying the public about potential and ongoing frauds, offering guidance on how to file a complaint or tip, and taking disciplinary actions against those who violate rules or laws.

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: 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)

200 Independence Avenue, SW Washington, DC 20201
TOLL-FREE: 1-800-447-8477 or 1-800-377-4950 (TTY)
FAX: 1-800-223-8164

WEBSITE: hhs.gov
EMAIL: hhstips@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
PHONE: (202) 616-4760
TOLL-FREE: 1-800-869-4499
OIG PUBLIC COMMENT LINE: (202) 353-1555
WEBSITE: justice.gov/oig
EMAIL: oig.hotline@usdoj.gov

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: godirect.gov
EMAIL: godirectsupport@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 SERVICES

P.O. Box 882528 San Francisco, CA 94188-2528
PHONE: (877) 876-2455
PRESS 3: For Mail Theft
PRESS 4: For Mail Fraud
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 Kalanianaole Federal Building, 300 Ala Moana Boulevard, Suite 6-210, Honolulu, HI 96850
PHONE: (808) 541-1912
FAX: (808) 545-4490
WEBSITE: secretservice.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
WEBSITE: sec.gov/complaint.shtml
EMAIL: help@sec.gov

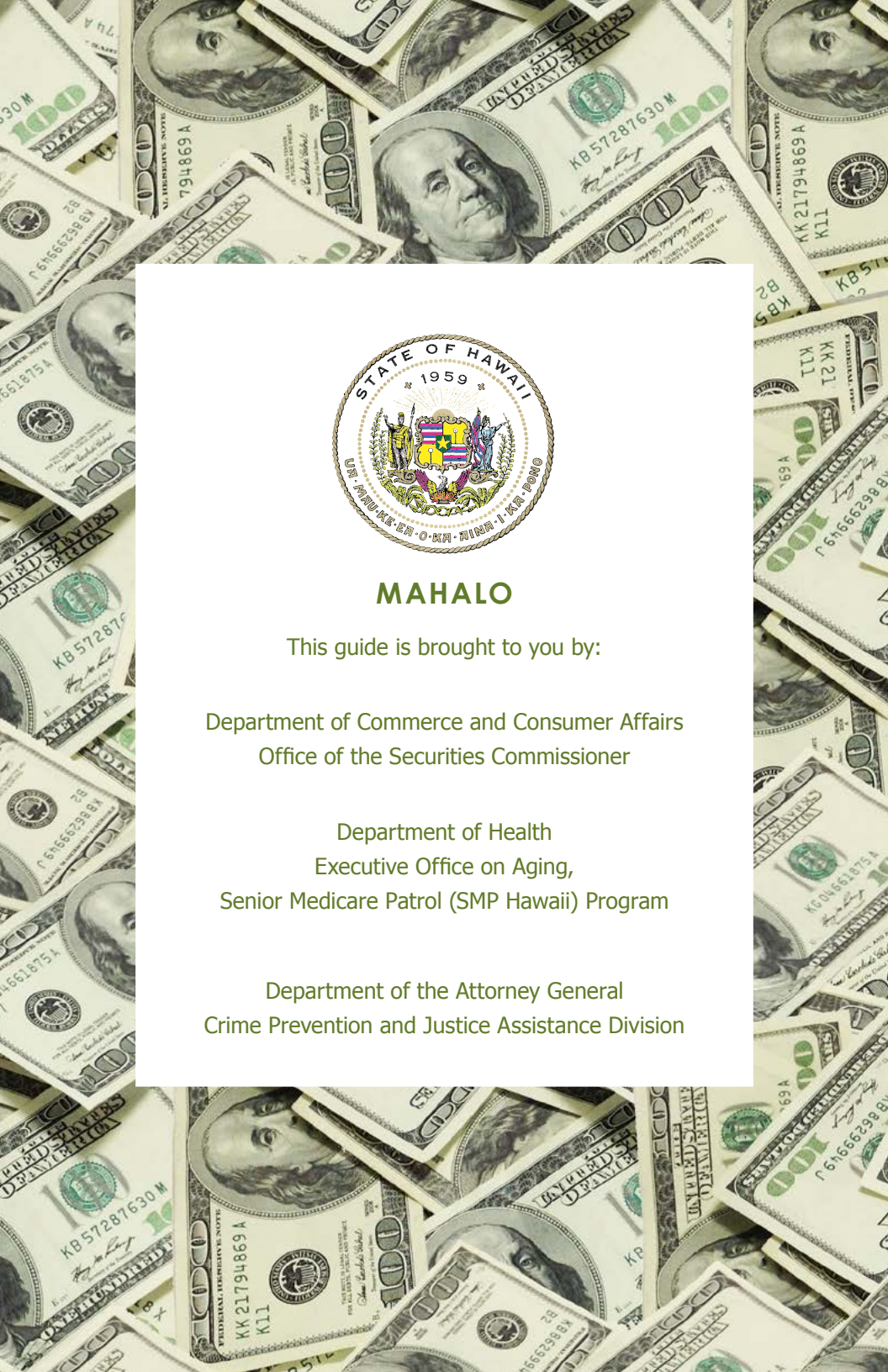
DESCRIPTION: If you encounter a problem with an investment or have a question, you can contact the SEC's Office of Investor Education and Advocacy.

UNITED STATES SOCIAL SECURITY ADMINISTRATION (SSA)
Honolulu Office

Prince Jonah Kuhio Kalanianaole 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: ssa.gov

TO REPORT FRAUD: 1-800-269-0271 (10am-4pm EST)
TO REPORT VIA WEBSITE: oig.ssa.gov/report

DESCRIPTION: Provides a place for citizens to assist their social security benefits, make changes to their social security records, and report potential fraud involving the social security programs.



MAHALO

This guide is brought to you by:

Department of Commerce and Consumer Affairs
Office of the Securities Commissioner

Department of Health
Executive Office on Aging,
Senior Medicare Patrol (SMP Hawaii) Program

Department of the Attorney General
Crime Prevention and Justice Assistance Division