

HAWAII'S FRAUD PREVENTION AND RESOURCE GUIDE 3RD EDITION



LETTER FROM GOVERNOR DAVID IGE



Aloha!

I am proud to introduce the third edition of Hawaii's Fraud Prevention and Resource Guide.

Fraud activity continues to grow at an alarming rate. In 2018, nearly \$1.5 billion was lost nationally, and in Hawaii \$6 million. Local families are devastated by the depletion of their savings, retirement, and investments. Fraud is a major concern for the elderly, but ultimately anyone can be victimized.

As Governor, I continue to support the efforts of the Department of the Attorney General, Crime Prevention and Justice Assistance Division; Department of Commerce and Consumer Affairs, Office of the Securities Commissioner; the Department of Health, Executive Office on Aging who collaborated to produce this guide on fraud awareness. Being informed, is the best tool to prevent individuals from becoming victims of fraud and identity theft. We must practice preventative strategies and help our fellow community members.

It is important to report these crimes to the proper authorities.

Let's continue to work together to protect our citizens.

With warmest regards,

David Y. Ige
Governor, State of Hawaii

Hawaii's Fraud Prevention and Resource Guide, 3rd Edition

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

This guide was supported in part by grant number 90MPPG0053 from the U.S. Administration for Community Living, Department of Health and Human Services, Washington D.C. 20201. Grantees undertaking projects with government sponsorship are encouraged to express freely their findings and conclusions. Points of view or opinions do not, therefore, necessarily represent official ACL policy.

This guide is provided as a public service. The information contained within is for general informational purposes and may not be applicable or relevant to every situation. Neither the State of Hawaii nor any agency, officer, or employee of the State of Hawaii makes any representations, guarantees, or warranties as to the accuracy, completeness, reliability, or suitability of the information provided in this guide. Accordingly, under no circumstances shall the State of Hawaii or any agency, officer, or employee of the State of Hawaii be liable for any special, consequential, or incidental damages that may result from the use of or reliance upon the information in this guide.

©2020 State of Hawaii, Department of the Attorney General, Crime Prevention and Justice Assistance Division; Department of Commerce and Consumer Affairs, Office of the Securities Commissioner; and the Department of Health, Executive Office on Aging, Senior Medicare Patrol (SMP Hawaii). For more information about reprint permission, contact the Department of the Attorney General, Crime Prevention and Justice Assistance Division, (808) 586-1444.

May 2020

Table of Contents

INTRODUCTION	8
IDENTITY THEFT	9
How Do Thieves Get Your Information?	10
Internet Phishing.....	10
Social Networks.....	10
Mail	11
Phone.....	11
Person-To-Person.....	11
Preventive Tips To Protect Yourself Against Identity Theft.....	12
HOW SCAMMERS ACCESS YOU	13
Malware	14
Adware	14
Ransomware	14
Scammer Tactics.....	14
ONLINE COMMUNICATIONS: SOCIAL NETWORKS	16
Top 5 Social Media Scams	
Hidden Urls	17
Phishing Requests	18
Hidden Charges.....	18
Cash Grabs	18
Chain Letters	19
Preventive Tips When Using	
Online Communications: Social Networks	19
MAIL	20
Common Mail Fraud and Scams.....	20
If You Suspect A Mail Scam.....	20
Preventive Tips For Mail Fraud.....	21
PERSON-TO-PERSON	22
Common Person-to-Person Scams.....	22
Preventive Tips For Person-to-Person Fraud.....	22
PHONE	23
Common Phone Scams	23
Preventive Tips For Phone Scams.....	23

WHAT KINDS OF INFORMATION ARE MOST IMPORTANT TO PROTECT?	24
WHAT SHOULD YOU DO IF YOU THINK YOUR INFORMATION HAS BEEN LOST OR STOLEN?	24
WHERE TO GET HELP	25
If You Are A Victim Of Identity Theft	25
If Your Child Is A Victim Of Identity Theft	26
If You Are A Victim Of Tax Identity Theft	27
How To Get Your Free Credit Report	28
Security Freeze	28
PREVENTIVE TIPS WHEN USING YOUR ELECTRONIC DEVICES	29
Be Alert To Impersonators	31
Safely Dispose Of Personal Information	31
Encrypt Your Data	31
Keep Passwords Private	32
Don't Overshare On Social Networking Sites	32
Securing Your Social Security Number	33
Keeping Your Devices Secure And Use Security Software	33
Avoid Phishing Emails	33
Be Wise About Wi-Fi	34
Lock Up Your Laptop	34
Read Privacy Policies	34
KEEPING OUR KUPUNA (SENIORS) SAFE	35
Check Professional Licenses: Doctors, Dentists, Nurses, Physical Therapists and Pharmacists	36
HEALTHCARE AND MEDICARE FRAUD	36
\$60 Billion Lost Annually	37
Who Commits Medicare Fraud?	37
Medicare Fraud	38
Types Of Fraudulent Claims	39
Medical Identity Theft	41
Health Impact	41
Personal Financial Losses	41
The Consequences Of Medicare Fraud	42
Future Generations	42
Preventive Tips For Medicare Fraud	42

Open Enrollment.....	45
Volunteer.....	45
A Story About Medicare: Tutu! Remember, Your Medicare Card Number Is Sacred!.....	46
COMMON CONSUMER SCAMS AGAINST KUPUNA (SENIORS)	47
Elder Financial Exploitation.....	49
Warning Signs of Financial Abuse.....	50
Forms Of Elder Exploitation.....	51
Scam Prevention Tips for Kupuna (Seniors).....	53
HOW TO SPOT A CON ARTIST	54
Financial Designations.....	58
ONLINE COMMUNICATION: SOCIAL NETWORKING	59
How Do Con Artists Exploit Social Networks?.....	60
Warning Signs of an Online Investment Scams.....	60
How Can I Protect Myself From Fraud In Social Networking?	61
VARIABLE ANNUITIES.....	62
Ask Questions.....	63
Beware Of Fees And Charges.....	64
HOW TO PROTECT YOUR NEST EGG	65
You Can Avoid Becoming A Victim By Following 10 Self-Defense Tips.....	66
CARING FOR OUR CAREGIVERS.....	68
What Is A Fiduciary?.....	69
Different Types Of Fiduciaries.....	69
Protecting Our Kupuna (Seniors).....	70
Warning Signs for Indicating Possible Financial Abuse of Elderly	71
Family Caregiver Support Program.....	72
Caregiver Support Services.....	72
Preventive Tips for Family Members and Caregivers	73
KUPUNA ALERT PARTNERS.....	74
Hawaii Medication Drop Box Program	75

METHODS OF COMMON FRAUDS AND SCAMS	76
Advance Fee Fraud	77
Warning Signs for Advance Fee Fraud.....	77
Preventive Tips For Advance Fee Fraud	78
 CHECK A PROFESSIONAL LICENSE AND CONSUMER COMPLAINT HISTORY	79
 TYPES OF FRAUDS AND SCAMS	81
Affinity Fraud (also known as Friendly Fraud)	82
Car Repairs And Sales Fraud	84
Charity Fraud	84
Computer Repair Scam.....	86
Construction and Home Repair Fraud	87
Credit Card Fraud	91
Diploma Mill Scam	93
Foreign Money Transfer Scam	94
Genetic Testing (Medical) Fraud.....	94
Hearing Aid Dealers And Fitters Fraud	95
Home Loan Fraud.....	95
Inheritance Scam.....	98
Insurance Fraud.....	98
Investment (Securities) Fraud	101
Lottery Or Sweepstakes Scam.....	103
Mortgage Reduction/Servicing Or Debt Relief Fraud	105
Obituary Scam.....	107
Overpayment, Fake Refund, And Fake Check Fraud.....	107
Ponzi Schemes	110
Purchasing Online Scam.....	113
Rental Scams	114
Romance Scam	116
Security Alarm System Fraud	116
Solar Panels/Photovoltaic (PV) Panels Or Other Distributed Energy Resources (DER) Scam	116
Tax Fraud And Scams	121
Utility Company Scam.....	121

RESOURCES 122

- County Resources
 - City And County Of Honolulu..... 123
 - County of Hawaii..... 124
 - County of Kauai 125
 - County of Maui 126
- State Resources 127
- National Resources 141



INTRODUCTION

Aloha. Welcome to the third edition of Hawaii’s Fraud Prevention and Resource Guide. This guide is a multi-agency collaboration developed to help you, the consumer, with the many different frauds and scams trying to separate you from your hard-earned money. In Hawaii, we have a local way of life that many of us cherish. It includes trust, generosity, and deep bonds of family and friendship. Our sense of family is strong, but even in Hawaii, criminal elements can lurk behind our bonds of family and friendship.

This guide was developed to inform you about common scams and fraud occurring within our local communities. Awareness and education are the key to protecting yourself. Recouping your lost assets, investments, savings, and other capital can be nearly impossible. You can protect yourself from becoming victimized by not providing personal information to anyone.

This guide provides you with awareness and resources on where to get help.



IDENTITY THEFT

Identity theft is when someone fraudulently uses your personal information, such as name, date of birth, Social Security Number, address, etc. to commit a crime. Scams include getting a loan, opening a bank account, getting a credit card account, and fake I.D. card. It causes havoc with your finances, your credit history, reputation and more.

Personal information can be obtained by a person-to-person, mail, or electronic means (email, social media, etc.), and other means, which are discussed in this section.

www.thoughtco.com/ways-identity-thieves-get-your-information-972208

HOW DO THIEVES GET YOUR INFORMATION?



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 such as 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 conversing with someone (via email or other methods) and get caught in an Overpayment Scam or an Advance Fee Scam, you could also end up exposing your bank account numbers or other personal information that could lead to identity theft.



SOCIAL NETWORKS

Phishing 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 your personal information, the thieves will use social media to build a relationship with you. After a relationship is established on the social media site, the relationship may move to email, texting, phone, or even person-to-person contact which is when the real phishing begins.



MAIL

Thieves 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 or you could receive an official letter requesting for your help to transfer millions of dollars in exchange for a fee they will provide you or request your bank account information to transfer funds electronically to you.



PHONE

There has been an increase in phone “phishing” where the thief finds some basic information, such as a name connected to a phone number and uses it to try to get money or information.. 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 personal information from “Aunty Kalei.”

More traditionally, thieves will pretend to be from an established company or government agency. 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 you to update their information, “through an automated response system” when in reality, the thieves are collecting your personal information through the phony automated system.



PERSON-TO-PERSON

In this approach, a scammer meets face-to-face with you. The scammer may be impersonating an agent from a well-known company or government agency 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 or she “needs” your bank account number and Social Security Number to “process” the paperwork. Be wary.



PREVENTIVE TIPS AGAINST IDENTITY THEFT

INTERNET AND SOCIAL MEDIA

- 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 from those you don't know. 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, insurance company, or government agency? 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 or government agency will call or text you and ask for personal information over the phone. If someone says they are calling from a bank, financial institution, health care provider, or government agency to update your information, ask for their name, employee ID and extension. Tell them you will call them back at the official number listed in the phone book or online to verify. Or even better, just hang up.
- Stop, check and verify the source.



HOW SCAMMERS ACCESS YOU

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

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

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 email attachments, 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. 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.

RANSOMWARE

Ransomware is a type of malware, or malicious software, designed to deny access to your computer system or data until a ransom is paid. Ransomware typically can be spread via phishing emails or by the person unknowingly visiting or “clicking” on an infected website or link.

SCAMMER TACTICS

Scam artists tailor their pitch to match the psychological profiles of their targets. They work to find out what motivates (emotional, financial, winnings, etc.) so they can take advantage of you and your 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 scam or fraud.



COMMON PERSUASION TACTICS INCLUDE:

- **Phantom Riches** – dangling the prospect of wealth, enticing you with something you want but can't have. "We can guarantee a 12% return on your investment if you invest in our company now."
- **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 family— 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."
- **Intimidation** – you are either threatened with violence, a lawsuit or arrest over missed loan payments, bogus court summons, or virus that will run on your computer unless you pay. In some cases, someone will actually appear at your front door.

Source: <https://www.arp.org/money/scams-fraud/info-08-2013/con-artists-use-fear-to-intimidate.html> FINRA. *Fighting Fraud 101*. Retrieved from <http://www.finra.org/investors/avoid-fraud>



ONLINE COMMUNICATIONS: 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. Per statistics revealed, over 2.6 billion users used social networking sites and apps in 2018. Some examples of Internet social media are Facebook, LinkedIn, Instagram, Twitter, YouTube, Line, Snapchat and others.

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 use privacy settings to limit who can access private posts.

*<https://makeawebsitehub.com/social-media-sites/>
Copyright: 2019 Make a Website Hub. Updated June 5, 2019.*

TOP 5 SOCIAL MEDIA SCAMS

HIDDEN URLS

Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL ("Uniform Resource Locator," the Web address) hides the full location. Clicking on such a link could direct you to your intended site, or to a site that installs all sorts of malware on your computer.

URL shorteners can be quite useful. Just be aware of their potential pitfalls and make sure you have real-time protection against spyware and viruses.

Bottom line: Sites that attract a significant number of visitors are going to lure in a criminal element, too. If you take security precautions ahead of time, such as using antivirus and anti-spyware protection, you can defend yourself against these dangers and surf with confidence.

Source: <https://us.norton.com/internetsecurity-online-scams-top-5-social-media-scams.html>



PHISHING REQUESTS

“Somebody just posted some cute pictures of you! Check ‘em out here!” Huh? Let me see that! Immediately, you click on the enclosed link, which takes you to your Twitter or Facebook login page. There, you enter your account info -- and a cybercriminal now has your password, along with total control of your account.

How did this happen? Both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social media site. It’s called phishing, and you’ve just been had. To prevent this, make sure your Internet security includes antiphishing defenses. Many freeware programs don’t include this essential protection.

HIDDEN CHARGES

“What type of animal character are you? Find out with our quiz! All of your friends have taken it!” Hmm, this sounds interesting, so you enter your info and cell number, as instructed. After a few minutes, a text turns up. It turns out you’re more a bear than a snake. Well, that’s interesting ... but not as much as your next month’s cell bill.

You’ve also just unwittingly subscribed to some dubious service that charges \$9.95 every month. As it turns out, that “free, fun service” is neither. Be wary of these bait-and-switch games. They tend to thrive on social media sites.

CASH GRABS

By their very nature, social media sites make it easy for us to stay in touch with friends, while reaching out to meet new ones. But how well do you really know these new acquaintances? That person with the attractive profile picture who just friended you — and suddenly needs money — is probably some cybercriminal looking for easy cash. Think twice before acting. In fact, the same advice applies even if you know the person. Picture this: You just received an urgent request from one of your real friends who “lost his wallet on vacation and needs some cash to get home.” So, being the helpful person you are, you send some money right away, per his instructions. But there’s a problem: Your friend never sent this request. In fact, he isn’t even aware of it. His malware-infected computer grabbed all of his contacts and forwarded the bogus email to everyone, waiting to see who would bite. Again, think before acting. Call your friend. Inform him of the request and see if it’s true. Next, make sure your computer isn’t infected as well.

CHAIN LETTERS

You've likely seen this one before — the dreaded chain letter has returned. It may appear in the form of, "Retweet this and Bill Gates will donate \$5 million to charity!" But hold on, let's think about this. Bill Gates already does a lot for charity. Why would he wait for something like this to take action? Answer: He wouldn't. Both the cause and claim are fake.

So why would someone post this? Good question. It could be some prankster looking for a laugh or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others. Break the chain and inform the sender of the likely ruse.



PREVENTIVE TIPS WHEN USING ONLINE COMMUNICATIONS: SOCIAL NETWORKS

- Use a unique password for each social network you belong to. When you use one password for multiple services, you're only as safe as the least secure service you use.
- Watch your mailbox. Messages come in from what seems to be your friend, colleague, or family member as a direct message to you via a link, attachment, etc. Don't open it.
- Don't be too personal and share too much information about yourself. Hackers who have access to public profiles – date of birth, education, interests, could use this information to answer security questions about yourself.
- Lock your phone. There are both faceless scammers and those who will just steal phones. Once they have your phone, they can access everything and anything that is on it.
- Use the block button. When a spammer sends you links, always report the account as a spam. The social network service will monitor it and can take action.
- Think about using free applications to monitor scams and unsafe links.

MAIL

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.

COMMON MAIL FRAUD AND SCAMS

- Charity Fraud and Scams
- Lottery or Sweepstakes Scam
- Inheritance Scam

For more types of fraud and scams see pg 81.

OTHER SCAMS COULD INCLUDE

Personal appeals for money or information from people you do not know and letters from psychics or religious figures offering to predict or change your future.

IF YOU SUSPECT A MAIL SCAM:

1. Contact your local police to report the scam.
2. If the victim is an older person or a person with a disability, contact your local adult protective services agency. You can find your state or local agency that receives and investigates reports of suspected elder financial exploitation by using the Eldercare locator or calling (800) 677-1116.

To report suspicious mail, you can file a complaint online with the Federal Trade Commission (FTC). You can also call 1-877-FTC-HELP (1-877-383-4357) or 1-866-653-4261 (TTY).

Note: Your complaint could help law enforcement detect patterns of fraud and abuse that may lead to investigations and can lead to eliminating scams.

The Better Business Bureau Northwest + Pacific 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.



PREVENTIVE TIPS FOR 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 unsolicited commercial mail, go to <https://www.dmachoice.org>, call 1-888-567-8688 or write to P. O. Box 643 Carmel, NY 10512.
- To “Opt-Out” of pre-approved offers of credit or insurance, go to <https://www.optoutprescreen.com>, call toll free at 1-888-567-8688 or write to Opt-Out Department, P. O. Box 530201, Atlanta, GA 30353.
- 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.”

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.

COMMON PERSON-TO-PERSON SCAMS (see page 81)

- Affinity Fraud
- Construction and Home Repair Fraud
- Romance Scam
- Investment (Securities) Fraud
- Ponzi Schemes



PREVENTIVE TIPS FOR 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 — while it can be difficult, it's okay to say “no.”

PHONE

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 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.

COMMON PHONE SCAMS (see page 81)

- Foreign Money Transfer Scam
- Identity Theft
- Lottery or Sweepstakes Scams



PREVENTIVE TIPS FOR 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 <https://www.donotcall.gov> or call 1-888-382-1222 or 1-866-290-4236 (TTY).

WHAT KINDS OF INFORMATION ARE MOST IMPORTANT TO PROTECT?

Here is a list in the order of importance:

- Social Security Numbers or last four digits
- Bank account numbers
- Investment account numbers
- Mother's maiden name
- Full birthdate (month/day/year)
- Home address
- Credit card numbers and security codes
- 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.
- 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.
- Place a security freeze, also known as a credit freeze, on your credit file.



WHERE TO GET HELP:

- Call your local Police Department 9-1-1.
- Call DCCA Office of Consumer Protection (808) 586-2630.
- 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 one-year Fraud Alert on your credit file by contacting the three companies: Equifax, Experian, and TransUnion.

Experian: www.experian.com/freeze **(888) 397-3742**

Equifax: www.help.equifax.com **(800) 685-1111**

TransUnion www.freeze.transunion.com **(888) 909-8872**

2. While you're at it, request copies of your credit report from these same three companies and review the credit report carefully for errors. Correct errors by contacting your creditors and ask creditors to call you before opening any new accounts or changing existing accounts.
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)

Kauai Police Department

Phone: (808) 241-1711

Maui Police Department

Phone: (808) 244-6400

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

5. Go to [ftc.gov](https://www.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. Parents can place a one-year fraud alert on your child's credit file and request a credit report for your minor child that you would do for yourself in the previous section: Equifax, Experian, and TransUnion.
2. 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 (Equifax, Experian and TransUnion) 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. 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**

SECURITY FREEZE

A security freeze, also known as a credit freeze, can help prevent identity theft because your credit file cannot be shared with potential creditors. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security Number would probably not be able to obtain credit in your name because access to your credit report is blocked. A fraud alert, on the other hand, alerts lenders to call you to verify your identity before extending new credit but does not block access to it.

Recent state and federal laws were passed allowing consumers, including children under 16, to request a security freeze without being charged. You can place a security freeze by contacting each of the credit reporting agencies:

Experian: www.experian.com/freeze **(888) 397-3742**

Equifax: www.help.equifax.com **(800) 685-1111**

TransUnion www.freeze.transunion.com **(888) 909-8872**

Remember: If you plan to apply for new credit, such as a car loan or mortgage, be sure to temporarily lift the freeze so that your financial institution can review your credit files. Once that process is done, re-freeze your account again for your continued protection.



PREVENTIVE TIPS WHEN USING YOUR ELECTRONIC DEVICES



Electronic devices can include your Smartphone, tablet, laptop, watch, computer, or gaming console.

- 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 hit SEND. 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.
- Think before you POST. 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.
- 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 and keep your account settings in private mode.
- 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.
- Know who you share information with.
- Store and dispose of your personal information securely, especially your Social Security Number.
- Ask questions before deciding to share your personal information.
- Maintain appropriate security on your computers and other electronic devices.
- Be AWARE of your DIGITAL FOOTPRINT. Understand how privacy settings work on social networks and websites you frequent. Set them to your comfort level of sharing.



Source: <https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure>



BE ALERT TO IMPERSONATORS

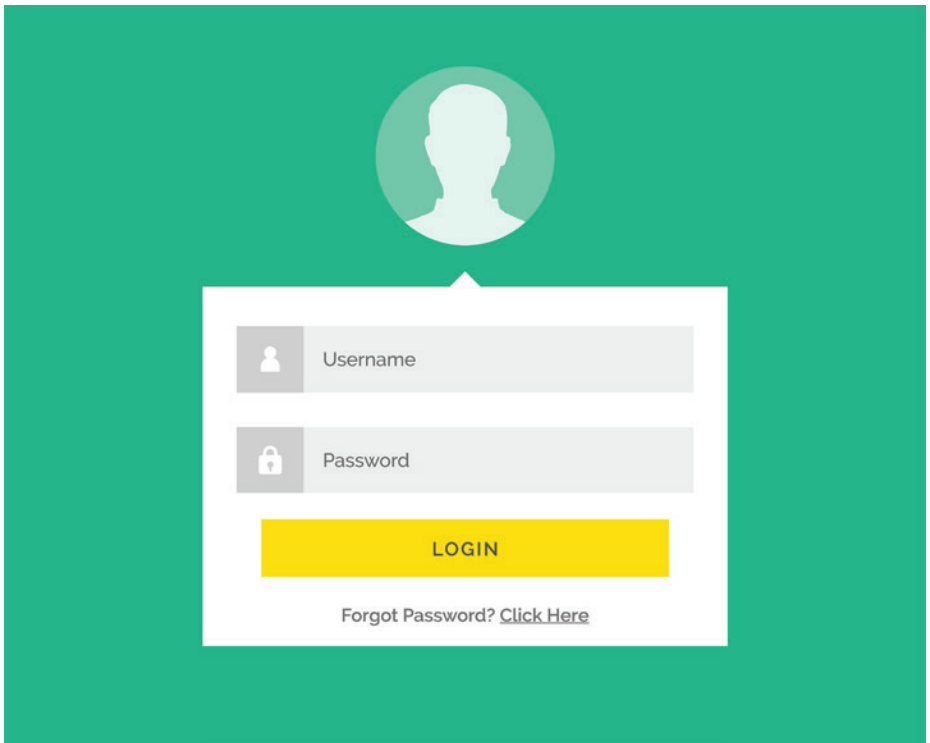
Make sure you know who is requesting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact. If a company that claims to have an account with you sends an email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

SAFELY DISPOSE OF PERSONAL INFORMATION

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

ENCRYPT YOUR DATA

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the Internet. A "lock" icon on the status bar of your Internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.



KEEP PASSWORDS PRIVATE

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, “I want to see the Pacific Ocean” could become 1W2CtPo.

DON'T OVERSHARE ON SOCIAL NETWORKING SITES

If you post too much information about yourself, an identity thief can find information about your life, use it to answer ‘challenge’ questions on your accounts, and gain access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security Number, address, phone number, or account numbers in publicly accessible sites.



SECURING YOUR SOCIAL SECURITY NUMBER (SSN)

Keep a close hold on your Social Security Number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's SSN, ask:

- Why is it needed?
- How it will be used?
- How they will protect it?
- What happens if you don't share the number?

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

KEEPING YOUR DEVICES SECURE AND USE SECURITY SOFTWARE

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

AVOID PHISHING EMAILS

Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.



BE WISE ABOUT Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

LOCK UP YOUR LAPTOP

Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to access your personal information.

READ PRIVACY POLICIES

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.



If you have been a victim of a cybercrime, file a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov


Source: Multi-State Information Sharing and Analysis Center. Partners with US DHS, US-CERT, ICS-CERT, etc. <https://www.cisecurity.org/ms-isac/>



KEEPING OUR KUPUNA (SENIORS) SAFE

Baby boomers are the largest generation in our nation's history. Since 2011, baby boomers have been entering their senior years and the U.S. has seen increasing incidents of senior fraud perpetuated against them. It may be in part due to the sheer number of people and their vast cumulative wealth that make the baby boomers a prime 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.

As of 2018, baby boomers hold the majority of the country's wealth at approximately \$30 trillion, and across the nation continue to be the target of financial and Medicare fraud. Many seniors fall prey to con artists who think nothing of wiping out their savings leaving them little to survive on. On the rise across the continental U.S. and in Hawaii, are incidences where family members are committing fraud on their own kupuna. Statewide, our kupuna are victimized by various types of financial, consumer, Medicare, medical, and other types of fraud. Impacting them is the growing problem of financial exploitation due to age, failing health, and diminished capacity. This section will help seniors and caregivers address these issues and provide resources to get help.



**CHECK PROFESSIONAL LICENSES:
PHYSICIANS, DENTISTS, NURSES,
PHYSICAL THERAPISTS, AND
PHARMACISTS**

Individual doctors, dentists, nurses, physical therapists, and pharmacists must be licensed to practice in Hawaii. Having a license to practice means the State has vetted the healthcare professional for various qualifications, including accredited education and training.

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

For more information on how to check a license or complaint history or to report fraud, contact the DCCA Professional and Vocational Licensing Division at (808) 586-3000 or visit pvl.hawaii.gov/pvlsearch to check complaint history. To report suspected fraud, call DCCA RICO at (808) 587-4272 or visit businesscheck.hawaii.gov.

HEALTHCARE AND MEDICARE FRAUD

Healthcare fraud can take various forms, including scams, suspicious billing practices and/or abuse against Medicare and insurance companies. This section provides information about how to protect yourself by detecting irregularities within your medical services and billing statements. It also looks at specific scams, fraud and abuse against the Medicare system, healthcare providers and most importantly, against YOU!

\$60 BILLION LOST ANNUALLY

Medicare loses billions of dollars each year due to fraud, errors, and abuse. In 2014, the National Health Care Anti-Fraud Association placed these losses at approximately \$60 billion annually, though the exact figure is impossible to measure. The most commonly cited range for all health care fraud estimates is 3 to 10 percent of annual health care expenditures. According to the National Health Expenditure Data, in 2017, Medicare spending exceeded \$700 billion dollars. These numbers are expected to rise as the baby boomer population ages.



WHO COMMITS MEDICARE FRAUD?

Those who commit Medicare fraud don't look like the "bad guy." Scammers and fraudsters look like everyone else. They tend to be charming, dynamic, and friendly; personality traits that help them be successful at taking advantage of others.

Medicare fraud and scams can have an even greater likelihood of being lucrative to the scammers when healthcare professionals or service providers are involved. Why? This is because medical professionals have the credentials, knowledge, and experience working within healthcare and know how to "trick the system" from the inside-side out. For example, unscrupulous physicians who prescribe drugs, medical supplies, laboratory tests, or genetic tests to patients they've never seen in person have become more common. Those that prescribe drugs, tests, and supplies online or over the phone can be part of a ring of scammers who prey on seniors. While most healthcare providers are ethical, committed, and caring individuals, the warning is this: Do not trust anyone by virtue of their profession alone.

So, how do you spot a scammer? You can't; not by merely looking at a person, their profession, or their degree. You must guard against Medicare fraud and scam by protecting yourself.

MEDICARE FRAUD

Medicare is complicated. What may seem like an error may simply be the result of a misunderstanding about benefits. It may also be abuse, which involves billing Medicare for services that are not covered or are not correctly coded.

Medicare fraud assumes criminal intent. The Centers for Medicare and Medicaid Services (CMS) defines fraud as “the intentional deception or misrepresentation that the individual knows to be false or does not believe to be true,” and that is made “knowing that the deception could result in some unauthorized benefit to himself or herself or some other person.” Some common examples of suspected Medicare fraud or abuse are:

- Billing for services or supplies that were not provided
- Providing unsolicited supplies to beneficiaries
- Misrepresenting a diagnosis, a beneficiary's identity, the service provided or other facts to justify payment
- Prescribing or providing excessive or unnecessary tests and services
- Violating the participating provider agreement with Medicare by refusing to bill Medicare for covered services or items and billing the beneficiary instead
- Offering or receiving a kickback (bribe) in exchange for a beneficiary's Medicare number
- Requesting Medicare numbers at an educational presentation or in an unsolicited phone call
- Routinely waiving co-insurance or deductibles
- Waivers are only allowed on a case-by-case basis where there is financial hardship, not as an incentive to attract business

TYPES OF FRAUDULENT CLAIMS

Here are some of the different ways that fraudulent billing can be presented to Medicare. Keep in mind that this list doesn't include all types of fraudulent scams but provides examples of some of the more common ones.

Call Senior Medicare Patrol (SMP) Hawaii toll free at 1-800-296-9422 if a situation resembling any of those below happens to you or a loved one, or if you're unsure if your circumstances require further investigation.

GENETIC TESTING/ CLINICAL LABORATORIES	<ul style="list-style-type: none">» Enticing Medicare beneficiaries to take a “free” genetic diagnostic test for the detection of cancer and other diseases» Using “rolling labs” to visit senior centers, elderly housing projects, or malls to offer “free” or unnecessary diagnostic tests and obtaining Medicare numbers to bill Medicare
DURABLE MEDICAL EQUIPMENT (DME) AND SUPPLIES	<ul style="list-style-type: none">» Falsifying examination or lab test results, Certificates of Medical Necessity, or claims forms» Billing for more expensive equipment than what was delivered» Offering “free” supplies or equipment and obtaining Medicare numbers to bill Medicare
PHYSICIANS/ PRACTITIONERS	<ul style="list-style-type: none">» Upcoding to higher-level of service to obtain a higher payment» Billing for services not provided» Misrepresenting diagnoses to obtain payment

MENTAL HEALTH SERVICES	<ul style="list-style-type: none"> » Using unlicensed staff to provide services » Billing group therapy sessions and individual therapy » Billing for drugs or psychotherapy for patients that can't benefit (comatose patients or late stage Alzheimer's Disease)
HOSPITALS	<ul style="list-style-type: none"> » Billing for tests, therapy, or supplies not provided to the patient » Holding patients under observation status in order to obtain higher payment » Recruiting persons with Medicare to be admitted to the hospital when inpatient care isn't needed
NURSING FACILITIES	<ul style="list-style-type: none"> » Understaffing to reduce costs and neglecting necessary care » Falsifying documents to avoid liability (e.g. faking duty rosters and altering patient records)
HOSPICE	<ul style="list-style-type: none"> » Enrolling patients who don't meet the criteria of having a terminal illness with only 6 months to live » Refusing to discharge a patient no longer eligible for hospice care or who wants to stop receiving hospice care
AMBULANCES	<ul style="list-style-type: none"> » Billing non-emergency trips as "emergency" trips » Billing for advanced life support services that weren't provided
PHARMACIES	<ul style="list-style-type: none"> » Billing for brand-name drugs but dispensing generic drugs » Conspiring with Medicare beneficiaries and physicians to divert filled prescriptions to drug traffickers

MEDICAL IDENTITY THEFT

Medical identity theft occurs when a beneficiary's Medicare number is misused, either by a provider, supplier, or by someone posing as the real beneficiary in order to receive medical care. Such Medicare numbers are considered "compromised." With the introduction of the new Medicare cards in 2018, Medicare numbers are no longer tied to Social Security Numbers. One of the great benefits to consumers is that, as a result of this change, Medicare numbers can now be changed and reissued if stolen or misused. However, substantial financial and emotional damage can still occur in cases of medical identity theft.

HEALTH IMPACT

Receiving health care from a fraudulent provider can mean the quality of the care is poor, the intervention is not medically necessary, or worse, the intervention is harmful. A beneficiary can receive improper medical treatment from legitimate providers as a result of inaccurate medical records that contain:

- False diagnoses
- Records showing treatments that never occurred
- Misinformation about allergies
- Incorrect lab results

Additionally, because of inaccurate or fraudulent claims to Medicare, beneficiaries may be denied needed Medicare benefits. For example, some services have limits. If Medicare thinks such services were already provided, they will deny payment.

PERSONAL FINANCIAL LOSSES

Medicare fraud, errors, and abuse can all result in higher out-of-pocket costs for beneficiaries, such as copayments for health care services that were excessive, were medically unnecessary or were never provided. Beneficiaries may also find themselves stuck with bills for services from providers who should have billed Medicare but instead billed the beneficiary for the entire cost of that service.

THE CONSEQUENCES OF MEDICARE FRAUD

As noted earlier, the annual cost of money lost to Medicare fraud, waste and abuse is staggering! These funds could have been used to provide more services to beneficiaries, increase reimbursement rates for providers, or to reduce premiums and co-payments to members.

FUTURE GENERATIONS

In order to ensure that your children, grandchildren, and their grandchildren receive the benefits they are entitled to, everyone must work together to protect, detect and report potential healthcare scams, fraud, abuse and errors.



PREVENTIVE TIPS FOR MEDICARE FRAUD

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

PROTECT your Medicare and Medicaid cards and numbers:

- Your Medicare number is your personal information. It can be more important to thieves than a credit card or bank account number.
- You should only provide your Medicare number and information to the healthcare providers you know, trust and have an established relationship with. Never give your numbers to people trying to sell a “free” service to you.
- Beware of people whom you don’t know calling, mailing, approaching you in person, emailing, and requesting your personal information. Letters, postcards, emails and online advertisements can look very legitimate, sometimes even using the Medicare name or logo. Frequently they contain an urgent threat, “You’ll lose your benefits if you don’t respond right away”. Hang up the phone, shred all personal information, walk away, delete, and just say “NO!” Bottom line, be extremely careful to whom you give your personal information.



PREVENTIVE TIPS FOR MEDICARE FRAUD (CONTINUED)

- Record doctor visits, tests, and procedures in your Personal Healthcare Journal (PHCJ) or on a calendar. Contact SMP Hawaii at (808) 586-7281 or toll free at 1-800-296-9422 for a free PHCJ.
- 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.
- Don't fall for solicitations via one-on-one interactions, in group settings, via postcards, emails, Internet, phone or infomercials. If something seems too good to be true, it probably is!
- Don't let those commercials fool you. Medicare will only pay for medical test and supplies if they are medically necessary and your personal physician orders it. If you need medical equipment, testing or services, go to your own physician who you know and trust.
- 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, letters or emails trying to get you to disclose your information. Medicare will not make an urgent demand of you, such as "failure to contact Medicare within three business days will result in your benefits being terminated."



Personal Health Care Journal

U.S. Administration on Aging



SMP Hawaii

Take an active role in your own health care!



PREVENTIVE TIPS FOR MEDICARE FRAUD (CONTINUED)

DETECT potential errors, abuse, and fraud:

- Always review your Medical Summary Notice (MSN) and Explanation of Benefits (EOB) for mistakes. Compare them with your PHCJ, prescription drug and other service provider receipts to make sure they are correct.
- Look for these three things in your billing statements to ensure accuracy:
 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 errors, abuse and fraud:

- If you find billing errors, or possible fraud, report it. You can avoid a negative financial impact, save your Medicare benefits for a time when you need them, and prevent others from becoming victims!
- If you're 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 for assistance.



OPEN ENROLLMENT

Each year the Annual Medicare Open Enrollment Period (October 15 through December 7) provides a unique opportunity for those who flourish on victimizing seniors about the Medicare Advantage and Prescription Drug programs. Scammers thrive on seniors' confusion and panic as they make critical choices. Understanding the choices can be very complicated and very individualized depending upon the beneficiary's healthcare needs, prescriptions and other factors. When faced with deadlines to choose a plan, beneficiaries may become nervous and seek the advice of "experts" who conveniently show up at the right place and time to alleviate their anxiety. Scammers can and will use confusion to mislead beneficiaries to join a health or drug plan that may not be right for them. Even worse, they may cause a beneficiary to lose health benefits that they may not be able to get back in the future, in order to make a lofty commission for themselves. Through a federal grant, the Hawaii State Health Insurance Assistance Program (SHIP), under the Hawaii State Department of Health, provides local, unbiased, one-on-one counseling to help Hawaii's Medicare beneficiaries to make informed decisions. Call the Hawaii SHIP Help Line at (808) 586-7299 or Toll Free at 1-888-875-9229.



VOLUNTEER

To help fight Medicare fraud and abuse, become a team member of SMP Hawaii and join our nationwide volunteer program numbering more than 6,000 members!

The SMP mission is to empower and assist Medicare beneficiaries, their families, and caregivers to

prevent, detect, and report health care fraud, errors, and abuse through outreach, counseling, and education. Contact us to learn about the role you can play in this important mission.

Also, contact SMP Hawaii if you have questions or concerns regarding potential healthcare scams, fraud, waste, abuse, or billing errors. Phone: (808) 586-7281 or toll free at 1-800-296-9422 or via our website: smphawaii.org. For more information, see the Resources section.



A Story About Medicare:

Tutu, remember your Medicare card number is sacred!

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, from free back braces to genetic tests that screen for cancer.

“They want to give me something for free and all they need is my Medicare number”, she said. Her brother, a SMP Hawaii Volunteer, stopped her and reminded her that her Medicare number has the same exposure to fraud as her credit card number.

“Scammers can use your number to commit all kinds of fraud that can leave you holding the bag for thousands of dollars or worse! That’s the result of Medical identity theft too!”, he told her.

Once Tutu understood that her Medicare number should only be given out to healthcare professionals and service providers that she has a history with, Tutu started saying “No!” to all the solicitations, and life became safer and simpler.



COMMON CONSUMER SCAMS AGAINST KUPUNA (SENIORS)

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 AND GRANDPARENT SCAM	<p>You get a call or email unexpectedly from someone who claims to be your grandchild or other relative. The callers says there is an emergency they need assistance with and you MUST send them money immediately, otherwise they will be a victim of something terrible that will happen.</p> <p>Example: A caller claiming to be the senior’s grandchild is arrested and attempts to get the senior to wire money to bail him out of jail.</p>
CHARITY APPEALS	<p>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.</p>
LOTTERY OR SWEEPSTAKES	<p>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.</p>

<p>HOME IMPROVEMENT</p>	<p>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.</p>
<p>FREE LUNCH SEMINARS OR WEALTH BUILDING WORKSHOPS</p>	<p>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.”</p>
<p>FREE TRIP</p>	<p>Scammers say you've won a free trip but they ask for a credit card number or advance cash to hold the reservation.</p>
<p>GOVERNMENT MONEY</p>	<p>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.</p>
<p>DRUG PLANS SCAMMERS</p>	<p>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.</p>
<p>FAKE “OFFICIAL” MAIL</p>	<p>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.</p>

ELDER FINANCIAL EXPLOITATION

This section addresses the factors that contribute to elder financial exploitation and how to suspect the occurrence of elder financial abuse, which is the misuse or taking of assets belonging to an elder that benefits the offender and deprives the elder of vital financial resources for his or her personal need. It often occurs without the elder's explicit knowledge or consent. The State of Hawaii defines an elder as someone who is 62 years or older.

Abuse is on the rise because of several factors:

- The elderly population is the largest growing age group.
- There is no known cure for dementia which is loss of cognitive functioning such as thinking, remembering, and reasoning.
- Victims often do not report out of shame.
- Home care is the third fastest growing occupation.
- Home care employment requires minimal background checks.
- High temptation, low risk factors.





WARNING SIGNS OF FINANCIAL ABUSE

- Unexplained disappearance of valuable possessions.
- Substandard care and unpaid bills despite adequate finances.
- Statements by the elder about suspected financial exploitation.
- Inclusion of additional names on bank signature cards.
- Unauthorized withdrawal using elder's accounts.
- Forged signature on financial transactions or titles of possessions.
- Sudden appearance of previously uninvolved relatives claiming rights to the elder's affairs and possessions.
- Abrupt changes in a will or other financial documents.
- Unexplained transfers of assets to family members or people outside of the family.
- Bank statements no longer go to the elder.
- Elder signing documents he or she cannot explain.
- Pension checks are cashed and all, or part does not go to the beneficiary.
- An individual, generally a caretaker, is designated power of attorney and withholds money to such a degree that the elder cannot buy food, pay bills or rent, etc.

FORMS OF ELDER EXPLOITATION

- **GENETIC TESTING AND MEDICARE SCAM**

Capitalizing on the growing popularity of genetic testing and fears of terminal illness, scammers are persuading seniors to take two types of genetic screenings that are covered by Medicare Part B.

Scammers will bill Medicare for these tests, that costs an average of \$8,000, and will likely not send the results to the senior. But more seriously, a senior's personal information and family medical history are at risk of being compromised. Before agreeing to genetic testing, be sure the test is ordered by a doctor and the test is medically necessary and covered by insurance.



- **INVESTMENT SCAM**

Investment scams are sometimes made with the victims' knowledge and consent. Email messages with “get-rich quick” schemes and offers of “guaranteed results” are often sent to seniors. Be cautious of emails that promise huge results with no risk.

- **LOTTERY SCAMS**

This is a type of advanced fee fraud which begins with an unexpected email, mailing (sometimes including a large check), or phone call claiming that “You have won!” a large sum of money in a lottery. The scammer will ask the senior to pay a “processing fee” so that the lottery payment can be distributed, but the victim will never receive any payment.

- **REAL ESTATE SCAMS**

- » **UNAUTHORIZED SALE OF PROPERTY OR TRANSFER OF PROPERTY TITLE**

– Vulnerable seniors are susceptible to being tricked into signing legal documents transferring the title of their property by people close to them such as a relative experiencing financial difficulty or a scammer posing as a trustworthy caretaker.

Trusted family members should look out for signs of unusual or large withdrawals or transfers from bank accounts the senior cannot explain, newly executed documents the senior cannot explain, and be wary of individuals who suddenly form a close relationship with the senior, gaining easy access to their home, money, and other property.

- » **ESCROW WIRE FRAUD** – A senior gets an email, phone call, or text from someone purporting to be from the title or escrow company with instructions on where to wire the escrow funds. Fraudsters set up fake websites that appear to be the title or lending company the senior is working with. Before sending money to a third party, always go back to the original documents received from the lender and call the phone number listed to verify the wiring instructions. Never click on email or text links, or send money online, without checking wire instructions with a live person on the phone from a number that you've called.

- » **FORECLOSURE RELIEF** - Homeowners who fall on hard times and get behind on their mortgage payments can become desperate to save their homes. That's when scammers, who have access to public records of homes in pre-foreclosure, swoop in with offers of foreclosure relief to capitalize on homeowners' vulnerability. The best way to avoid foreclosure is to work directly with a loan officer to modify an existing loan, request a forbearance, or make some other arrangement. A scammer will tell you not to talk to your lender, and that is a huge red flag!

- » **RENTAL SCAMS** – Scammers post ads of properties for rent on Craigslist or social media pages to lure in unsuspecting renters, sometimes using photos from other listings. The scammers, who have no connection to the property or its owner, will ask for upfront payment to let you see the property. Be suspicious of anyone who asks for a cash deposit upfront to see a property. Ensure you are dealing with the real property owner before negotiating rental terms or seeing a property in person. Avoid doing transactions via email or on the phone.





SCAM PREVENTION TIPS FOR KUPUNA (SENIORS)

- Keep personal information secure at home.
- Know who has access to your personal information.
- Get in the habit of shredding expired and unnecessary documents.
- Be suspicious of any emails or phone calls requesting passwords or personal information.
- Don't use your mother's maiden name, parts of your Social Security Number or phone numbers as passwords.
- Cut up old credit cards.
- Don't give out personal information over the phone unless you initiated contact or know who you are speaking with.

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



HOW TO SPOT A CON ARTIST

Investing in securities is risky enough without worrying about whether your salesperson is going to fleece you. To be an informed investor, you must know what danger signs to look for. Some are subtle, and some are easier to spot.



Sign #1: Con Artists Like To Blend In

Con artists like to blend in with others in your group whether that group be political, community (such as the local senior center), religious or other. They quickly get to know a lot of people in the group so they can count on this common bond to spread the word about their questionable investments and reel in unsuspecting investors. Effective con artists must disguise their true motives.

Sign #2: Con Artists Dress For Success

Even though con artists would like you to believe that they are “just plain folk,” they are smart enough to realize that this alone will not sway you to part with your money. They work very hard to come across as smooth, professional and successful. Con artists may dress like they are wealthy and work out of impressive looking offices. If your only contact is by mail, the office may bear a prestigious sounding address. Often, this is nothing more than a mail drop. Your best bet is to look behind the surface and do some serious investigating before you part with your money.

Sign #3: Con Artists Often Push Poorly Understood Or Little-Known Products

Today, a variety of institutions, from banks to brokerage firms to financial planners, offer a wide range of financial products. With such a confusing mix to choose from, it is no wonder that many people turn to financial advisers for guidance. Con artists know this and stand ready to assume full responsibility for your investment decisions. Don't let them! When it comes to your money, think things through for yourself after getting all the facts. Never give someone control over your purse strings just because you think you are too old, young or financially inexperienced. If you really need help, only deal with financial advisers, broker-dealers or financial institutions with proven track records.

Sign #4: Con Artists Bring Out The Worst In You

Skilled con artists can bring out your worst traits, particularly greed, fear, and insecurity. Con artists know that promises of huge returns with no risk will get your attention. They hope that it will get your money too. Fear comes into play when the con artist warns you that complaining about a failed investment to the government may result in your spoiling it for others or “rocking the boat.” Con artists try to make you feel inadequate if you don’t believe them or ask too many questions. If you find yourself making investment-related decisions based only on your emotions, watch out!

Sign #5: Con Artists Are Fair Weather Friends

They take a personal interest in you out of the blue. They call back when they promised they would and may pressure you into investing. Despite his or her kind words, the con artist will do anything in his or her power to make a sale. However, once you have invest your money, the con artist is gone. If you cannot get answers to your questions after handing over your cash, there is a good chance someone else is getting rich off of your investment.

Sign #6: For Every Silver Lining, There Is A Cloud

Every investment involves risk. But to hear the con artist explain it, the investment may be too good to be true. Trust your inner voice if you hear the following claims:

- “Your return is guaranteed. There’s no way you can lose money.”
- “Gotta get in on the ground floor now or you’ll be left out in the cold. In fact, we’ll send a messenger over tomorrow to pick up your check.” (Con artists often use this device to avoid federal mail fraud charges.)
- “This deal is so great, I invested in it myself.”
- “If this doesn’t perform as I just said, we’ll refund your money no questions asked.”
- “Everyone else that invested in this did very well.”
- Be especially careful if the salesperson downplays any downside or denies that risk exists. Con artists usually are not very good at answering important questions. Watch out if the salesperson is reluctant to provide information on the following:
- The background, educational history and work experience, track record of the deal’s promoters, principals or general partners;



- Information on whether your investment monies will be segregated from other funds available to the business;
- Written information on the business' financial condition, such as a balance sheet and bank references;
- The salesperson's name, where he or she is calling from, who he or she works for, his or her background and what commission or other compensation he or she will receive; and
- The salesperson's connection with the venture and any affiliates

In addition, be wary if the salesperson doesn't ask you questions about your past investment experience and your ability to withstand risk. Even if the salesperson does ask a few related questions, take heed if you get the sense that he or she is merely going through the motions.

Sign #7: Don't Be Afraid To "Sleep On It."

If you are promised high, guaranteed profits and given no written explanation concerning the investment or the risks involved, walk away. Never invest in anything based on the enthusiasm or charisma of the salesperson - they may have more to gain by taking your money than you know.

FINANCIAL DESIGNATIONS

These are the only **RECOGNIZED** financial expert designations under the state securities laws.

ABBREVIATION	DESIGNATION	ORGANIZATION
CFP	Certified Financial Planner	Certified Financial Planner Board of Standards, Inc.
ChFC	Chartered Financial Consultant	American College
PFS	Personal Financial Specialist	American Institute of Certified Public Accountants
CFA	Chartered Financial Analyst	Chartered Financial Analyst Institute
CIC	Chartered Investment Counselor	Investment Advisor Association

These are **NOT RECOGNIZED** as financial expert designations under the state securities laws.

ABBREVIATION	DESIGNATION	ORGANIZATION
CSA	Certified Senior Advisor	Whatever organization they say they are with.
SS	Senior Specialist	
SE	Senior Expert	
RA	Retirement Advisor	

A laundry list of credentials after someone's name does not give them the authority to sell securities. In most cases, a stockbroker or any other person who wants to sell securities (for example, stocks, bonds, mutual funds, etc.) or advise you on investments must be registered to do so. The Financial Industry Regulatory Authority (FINRA) has FREE BrokerCheck reports. Visit the website at www.finrabrokercheck.com or call toll free 1-800-289-9999, Monday through Friday 8am – 8pm EST.

Also, call the Office of the Securities Commissioner, Compliance Branch at (808) 586-2722 to verify the registration of your broker-dealer and the salespersons, or your investment adviser and their representatives. One call can make a difference!

ONLINE COMMUNICATION: SOCIAL NETWORKING

A social network is a group of individuals (or organizations) who are connected through common interests, hobbies, lifestyles, faith or other beliefs. Websites such as Facebook, Twitter, LinkedIn, eHarmony and other online social networks and communities have made it faster and easier for users to meet, interact and establish connections with other users anywhere in the world. Offline, social networking involves making these connections through membership in community organizations, associations, and other social groups. While social networking helps connect people with others who share similar interests or views, con artists infiltrate these social networks looking for victims. By joining and actively participating in a social network or community, the con artist builds credibility and gains the trust of other members of the group.



HOW DO CON ARTISTS EXPLOIT SOCIAL NETWORKS?

In traditional social networks, con artists use the weekly or monthly meetings to establish strong bonds through face-to-face contact and sharing of personal interests and lifestyles. In online social networks, a con artist can establish this trust and credibility more quickly. The scammer has immediate access to potential victims through their online profiles, which may contain sensitive personal information such as their dates or places of birth, phone numbers, home addresses, religious and political views, employment histories, and even personal photographs. The con artist takes advantage of how easily people share background and personal information online and uses it to make a skillful and highly targeted pitch. The scam can spread rapidly through a social network as the con artist gains access to the friends and colleagues of the initial target.



WARNING SIGNS OF AN ONLINE INVESTMENT SCAM?

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 con artists use them to cover up the money trail.
- **Recruit your friends.** Most cons will offer bonuses if you recruit your friends into the scheme.
- **Professional websites with little to no information.** These days anyone can put up a website. Scam sites may look professional, but 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.

HOW CAN I PROTECT MYSELF FROM FRAUD IN SOCIAL NETWORKING?

- Contact Hawaii Office of the Securities Commissioner. Before investing any money, contact their office to check registration of the salesperson and the investment product.
- Protect your personal information. Many sites will allow you to choose how much personal information you want to make publicly accessible, and how much you want to keep private. Adjust your privacy and security settings accordingly, and think twice before posting personal information online.
- Search the names of all persons and companies connected to the investment being offered. The Internet offers anonymity and scam artists take advantage of this. Do a search for the name of the person offering you the investment and the companies involved in the investment. If there are few results, or their name doesn't appear anywhere outside of the one investment program they're offering you, that's a red-flag that they may be using multiple aliases, or hiding behind a fake identity.
- Beware of the use of names or testimonials from other group members. Scam artists frequently pay out high returns to early investors using money from later arrivals. This type of scam is a Ponzi scheme. Fraud aimed at groups of people who share similar interests is called affinity fraud.
- Obtain a prospectus. Ask for written documentation that details the risks of the investment and procedures to get your money out.
- Do not take the word of a salesperson. Don't feel pressured to "act now." Take time to check out the investment yourself, and remember the old adage: "If it sounds too good to be true, it probably is."

Before you invest, evaluate every investment opportunity in the virtual world the same way you would in the real world. Visit the Hawaii Office of the Securities Commissioner website investing.hawaii.gov or North American Securities Administrators Association (NASAA) website nasaa.org for more tips on recognizing, avoiding and reporting investment fraud.



VARIABLE ANNUITIES

Before purchasing a variable annuity, you owe it to yourself to learn as much as possible - how they work, the benefits they provide, and the charges you will pay.

ASK QUESTIONS

Ask YOURSELF questions to ensure that you understand what you are investing in and if it suits your particular investment needs.

1. Will I use the variable annuity primarily to save for retirement or a similar long-term goal?
2. Do I understand all the features of the variable annuity?
3. Am I willing to take risk that my payout may be a lot less if the underlying investment options perform poorly?
4. Do I understand all of the charges and fees of the variable annuity?
5. Am I purchasing from a trusted salesperson and feel comfortable with all of the information he/she has provided?
6. Is this annuity investment right for me given my age, the lock-in time and my tolerance for risk?

Ask the SALESPERSON questions to protect yourself from being a victim of investment fraud.

1. Are you registered with the Hawaii Office of the Securities Commissioner to sell this product?
2. Did you disclose all commission, charges and fees associated with this transaction?
3. What is the total commission, charges and fees you will receive from this transaction?
4. What will it cost to withdraw my money early?
5. Is there a lock-in period and how long is it?

Give yourself time to think about the purchase. Variable annuity contracts typically have a “free look” period of ten or more days, during which you can terminate the contract without paying any surrender charges and get back your purchase payments. You can continue to ask questions during this period to make sure you understand your variable annuity before the “free look” period ends.

BEWARE OF FEES AND CHARGES

Several charges and fees will be incurred when you invest in a variable annuity. Be sure you understand all the charges before you invest and understand how much that takes away from your investment. It could be a lot. If you don't understand the charges, don't purchase the annuity.

- **Surrender Charge:** A type of sales charge or penalty you will be assessed if you withdraw money from a variable annuity within a certain period after purchase (typically within six to eight years).
- **Mortality and Expense Risk Charge:** This charges is equal to a percentage of your account value (typically in the range of 1.25% per year) and compensates the insurance company for risks it assumes under the annuity contract.
- **Administrative Fee:** The insurer may deduct charges to cover record-keeping and other administrative expenses. This may be charged as a flat account maintenance fee (perhaps \$25 or \$30 per year) or as a percentage of your account value (typically in the range of .15% per year).
- **Underlying Fund Expense:** You will also indirectly pay the fees and expenses imposed by the mutual funds that are the options for your variable annuity. These funds are taken annually as a percentage of your assets invested in the fund.
- **Management Fee:** A fee to manage the investment portfolio (can range from .10% or higher)
- **Distribution and Service Fees:** Also known as Rule 12b-1 fee to manage the investment portfolio.
- **Charges and Fees for other features:** Special features offered by some variable annuities, such as a stepped-up death benefit, a guaranteed minimum income benefit, or long-term care insurance, often carry additional fees and charges.



ALERT: BE SURE TO GET THE CHARGES AND FEES IN WRITING BEFORE YOU SIGN.



HOW TO PROTECT YOUR NEST EGG

As an older investor, you are a top target for con artists. State securities agencies are filled with tragic examples of senior investors who have been cheated out of savings, windfall insurance payments, and even the equity in their own homes.

You can avoid becoming a victim by following 10 self-defense tips:

- 1. *Don't be a courtesy victim.*** Con artists will not hesitate to exploit your good manners. Save your good manners for friends and family members, not strangers looking for a quick buck!
- 2. *Check out strangers touting strange deals.*** Trusting strangers is a mistake anyone can make when it comes to their personal finances. Say “no” to any investment professional who presses you to make an immediate decision, giving you no opportunity to check out the salesperson, firm and the investment opportunity itself. The Central Registration Depository (CRD) contains extensive background information on investment salespeople and firms and is available to your state or provincial regulatory agency.
- 3. *Always stay in charge of your money.*** Beware of anyone who suggests investing your money into something you don't understand or who urges that you leave everything in his or her hands.
- 4. *Don't judge a book by its cover.*** Successful con artists sound and look extremely professional and have the ability to make even the flimsiest investment deal sound as safe and sound as putting money in the bank. The sound of a voice, particularly on the phone, has no bearing on the soundness of an investment opportunity.
- 5. *Watch out for salespeople who prey on your fears.*** Con artists know that you worry about either outliving your savings or seeing all of your financial resources vanish overnight as the result of a catastrophic event, such as a costly hospitalization. Fear can cloud your good judgment. An investment that is right for you will make sense because you understand it and feel comfortable with the risk involved.
- 6. *Don't make a tragedy worse with rash financial decisions.*** The death or hospitalization of a spouse has many sad consequences - financial fraud shouldn't be one of them. Ask a con artist to describe his ideal victim and you are likely to hear the following two words: “elderly widow.” If you find yourself suddenly in charge of your own finances, get the facts before you make any decisions. Local libraries and universities may offer classes and information on investing. Talk to friends, family, trade organizations, and state or provincial securities regulators for advice on locating a financial professional and checking their background. An insurance settlement may help with expenses but it also makes you an ideal target for fraud. Arm yourself with information and your confidence will send con men running.

- 7. Monitor your investments and ask tough questions.** Don't compound the mistake of trusting an unscrupulous investment professional or outright con artist by failing to keep an eye on the progress of your investment. Insist on regular written reports. Look for signs of excessive or unauthorized trading of your funds. Don't let a false sense of friendship or trust keep you from demanding a routine statement of your accounts.
- 8. Look for trouble retrieving your principal or cashing out profits.** If a stockbroker, financial planner or other individual with whom you have invested stalls you when you want to pull out your principal or profits, you have uncovered someone who wants to cheat you. Some kinds of investments have certain periods when you cannot withdraw your funds, but you must be made aware of these kinds of restrictions before you invest.
- 9. Don't let embarrassment or fear keep you from reporting investment fraud or abuse.** Con artists know that you might hesitate to report that you have been victimized in financial schemes out of embarrassment or fear. Con artists prey on your sensitivities and, in fact, count on these fears preventing or delaying the point at which authorities are notified of a scam. Every day that you delay reporting fraud or abuse is one more day that the con artist is spending your money and finding new victims.
- 10. Beware of "reload" scams.** If you are already the victim of an investment scam, don't compound the damage by letting con artists "reload" and take a "second bite" of your assets. Con artists know you have a finite amount of money. Faced with a loss of funds, some seniors who have been victimized once will go along with another scheme in which the con artists promise to make good on the original funds lost and possibly even generate new returns beyond those originally promised. Though the desire to make up lost financial ground is understandable, all too often the result is that you lose whatever savings you had left in the wake of the initial scam.



CARING FOR OUR CAREGIVERS

Given the growing number of seniors in our community, caregiving is a huge responsibility, and sometimes, big business and people cross the line to elder exploitation. 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



PROTECTING OUR KUPUNA (SENIORS)

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.



REMINDERS

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



WARNING SIGNS FOR INDICATING 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 <http://www.agingwisely.com/scams-on-the-elderly-senior-care-tips-for-fraud-prevention/>

FAMILY CAREGIVER SUPPORT PROGRAM

The Family Caregiver Support program provides caregiver support services to enable care recipients to remain in their familiar environment. These caregiver support services are available to adult family members, or other individuals who are informal, unpaid providers of in-home and community care to older adults age 60 and older.

Caregiver support services are also available to grandparents or relatives (not parents) age 55 or older who are taking care of a child, age 18 and younger and/or a relative 18 and older with a disability. Please contact your county office on aging for more information about accessing these services.

CAREGIVER SUPPORT SERVICES

- **Access Assistance** – A service that assists caregivers in obtaining access to the services and resources that are available within their communities.
- **Counseling** – Counseling to caregivers to assist them in making decisions and solving problems relating to their caregiving roles. This includes counseling to individuals, support groups, and caregiving training.
- **Information Services** – A service for caregivers that provides the public and individuals with information on resources and services available to the individual within their communities.
- **Supplemental Services** – Services provided on a limited basis to complement the care provided by caregivers. Examples of supplemental services include, but are not limited to, home modifications, assistive technologies, emergency response systems, and incontinence supplies.
- **Respite Care** – Services which offer temporary, substitute supports or living arrangements for care recipients in order to provide a brief period of relief or rest for caregivers.



PREVENTIVE 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 loved 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 your loved ones 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 mailbox.
- It’s very important for you to seek support from other caregivers. You are not alone! Accept offers of help.



KUPUNA ALERT PARTNERS

Kupuna Alert Partners (KAP) is a multi-agency partnership that offers presentations to the community. KAP was formed as a partnership between the Department of the Attorney General, Crime Prevention and Justice Assistance Division, Community and Crime Prevention Branch; Department of Commerce and Consumer Affairs, Office of the Securities Commissioner; Department of Health, Executive Office on Aging, Senior Medicare Patrol (SMP) Hawaii; and Department of Public Safety, Narcotics Enforcement Division.

Kupuna Alert Partners (KAP) are FREE presentations statewide available to community groups of 20 or more individuals. The presentation includes information on:

- Prescription drug misuse and medication take back
- Medicare fraud
- Identity theft and top scams in Hawaii
- Securities fraud

For more information or to request a presentation, contact:
Department of the Attorney General, Crime Prevention and Justice Assistance Division, Community and Crime Prevention Branch at (808) 586-1487

Hawaii Medication Drop Box Program

Hawaii residents can bring their unused or expired medication for safe, anonymous disposal at the KAP presentations or go to: hawaiiopioid.org to locate a drop box near you. This service is free and anonymous – no questions asked. Tablets, capsules, liquids, and other forms of medication will be accepted. New or used syringes will not be accepted.

Unused or expired medicine should be disposed of properly when it is no longer needed for the illness for which it was prescribed.

- Medicines may lose their effectiveness after the expiration date.
- Improper use of prescription drugs can be as dangerous as illegal drug use.

Having unused or expired medicine in your home increases the risk of accidental poisoning.

- Homes where children or the elderly live are especially vulnerable to this danger.
- People may mistake one type of medicine for another type; children may mistake medicine for candy.

Expired medicine should not be thrown in the trash or flushed down the toilet. Proper disposal helps reduce the risk of prescription drugs entering the human water supply or potentially harming aquatic life.



METHODS OF COMMON FRAUDS AND SCAMS

The following section covers the method, and a vast range of frauds and scams from Affinity Fraud to Utility Company Scam. We will discuss the method of Advance Fee Fraud, red flags, tips, and where to go for help. Additionally, we will discuss the importance of checking the professional license and consumer complaint history for more than 50 industries before engaging in any transaction.

ADVANCE FEE FRAUD

Advance Fee Fraud is a scam where the victim believes that paying an advance 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.
- The 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.



WARNING SIGNS FOR ADVANCE FEE FRAUD

- 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.”



PREVENTIVE TIPS FOR 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.





CHECK A PROFESSIONAL LICENSE AND CONSUMER COMPLAINT HISTORY

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 50 different professional or vocational industries. These industries are the kind that affect the health, safety, and welfare of Hawaii's residents. The Regulated Industries Complaints Office (RICO) of the DCCA investigates and can prosecute complaints alleging professional misconduct by licensees, and complaints that concern unlicensed activity. RICO offers the licensing information and complaint history for professionals in the industries, listed on the following page.

Go to BusinessCheck.hawaii.gov. To report suspected fraud in any of these areas, call (808) 587-4272.

Licensed Professionals Regulated by DCCA PVL and RICO

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



TYPE OF FRAUDS AND SCAMS

- Affinity Fraud
- Car Repairs and Sales Fraud
- Charity Fraud
- Computer Repair Scam
- Construction and Home Repair Fraud
- Credit Card Fraud
- Diploma Mill Scam
- Foreign Money Transfer Scam
- Genetic Testing (Medical) Fraud
- Hearing Aid Dealers and Fitters Fraud
- Home Loan Fraud
- Inheritance Scam
- Insurance Fraud
- Investment (Securities) Fraud
- Lottery or Sweepstakes Scam
- Mortgage Reduction/Servicing or Debt Relief Fraud
- Obituary Scam
- Overpayment, Fake Refund, and Fake Check Fraud
- Ponzi Schemes
- Purchasing Online Scam
- Rental Scam
- Romance Scam
- Security Alarm System Fraud
- Solar Panels/ Photovoltaic (PV) Panels or Other Distributed Energy Resources (DER)
- Tax Fraud and Scams
- Utility Company Scam



AFFINITY FRAUD (also known as Friendly 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 “family” and “friends” to buy into fake investments, often Ponzi schemes. Victims of Affinity Fraud have stated that they let their guard down because the promotor was a “friend” when in reality, the promotor had embedded his or herself into the group, often times befriending those in well-regarded or prominent positions first to then gain the trust of others in the group.

COMMON TARGET GROUPS OF AFFINITY FRAUD:

- Athletic Groups
- Church Groups/Members
- Elderly/Senior and Pre-Retiree Groups
- Ethnic Groups
- Military Groups
- Professional Groups
- Union Groups/Members

The results of Affinity Fraud can be devastating and life-changing. In many cases, the fraud involves what turns out to be a Ponzi scheme or some other fraud. Remember - Investigate before you invest, no matter who is selling the financial product.



WARNING SIGNS TO WATCH OUT FOR:

- The investment is an exclusive deal for “only” a select group of people.
- Information on the investment product and the business is poorly written and often times contains spelling and/or grammatical errors.
- Explanations of how the business runs and how money is made are vague or overly complicated.
- The investment is promoted as having no risk or downside.
- You are pressured to sign the documents now and get the information later.
- You are promised high or unrealistic returns in a short period of time.
- The person selling the investment is not registered with the DCCA - Securities Compliance Branch.



PREVENTIVE TIPS FOR AVOIDING AFFINITY FRAUD

- Remember, you have the right to say “no” even if it is a friend or family 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.

CAR REPAIRS AND SALES FRAUD

A motor vehicle repair shop must be licensed by the 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. To check a license or complaint history, go to BusinessCheck.hawaii.gov 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.

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 hurricane 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) 586-1454. 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. Some scammers use names that sound similar to real charity names.
- 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?

- Consider donating by check or credit card, never with cash.
- Check for fundraising reports on the charity on the Attorney General’s website and with charity watchdogs such as:
 - » Charity Watch (charitywatch.org)
 - » Better Business Bureau’s Wise Giving Alliance (give.org)
 - » Charity Navigator (charitynavigator.org)
 - » GuideStar (guidestar.org)
- Be aware some scammers can change caller ID to make a call look like it is from a local area code.
- 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) 586-1454.
3. Call the Federal Bureau of Investigation (808) 566-4300.
4. Report the scams to [FTC.gov/complaint](https://www.ftc.gov/complaint) (<https://www.ftc.gov/complaint>).

COMPUTER REPAIR SCAM

Someone calls pretending to be from a computer repair center, Internet security firm, technician who monitors “your” computer, or from Microsoft and says the senior consumer’s computer needs to be repaired. The scammer would then take control of the senior’s/consumer’s computer accessing sensitive files containing personally identifiable data that could be used to steal the senior’s/consumer’s identity. To report fraud, contact your local police department and/or the DCCA Office of Consumer Protection at (808) 586-2630.



CONSTRUCTION AND HOME REPAIR FRAUD

Construction and Home Repair Fraud could involve 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). To search whether a contractor is licensed, please visit pvl.hawaii.gov/pvlsearch or contact (808) 586-3000. The Regulated Industries Complaints Office (RICO) of the DCCA takes complaints regarding licensed and unlicensed contractors, including complaints that may involve fraud. RICO also provides the public with a searchable database of prior complaints. Go to BusinessCheck.hawaii.gov 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 decrease the chances of being taken by fraud through hiring a licensed contractor.



WARNING SIGNS OF POSSIBLE 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, search pvl.hawaii.gov/pvlsearch or contact (808) 586-3000 or DCCA Consumer Resource Center (808) 587-4272 to check their complaint history.

In Hawaii, a licensed contractor is required to perform certain remodeling, repair, electrical and plumbing, or painting over \$1,500, and whenever a building permit is required for a home project. Remember, three bids or estimates, preferably from licensed contractors, may help you decide if the work they're proposing is really necessary.





PREVENTIVE TIPS FOR HIRING LICENSED CONTRACTORS

- Ask to see a picture ID 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 Professional and Vocational Licensing Division at (808) 586-3000 or visit their website at pvl.ehawaii.gov/pvlsearch, or the DCCA Consumer Resource Center at (808) 587-4272 or by going online 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 complies with city and county building 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.

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 inputted.



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

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>



PREVENTIVE 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 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.

DIPLOMA MILL SCAM

Avoiding Deceptive Post-Secondary Education Degrees

Continuing your education and pursuing a degree to further your career is becoming more accessible with growing online options, however, students should do their due diligence when selecting a school. Beware of “diploma mills” that offer degrees for a flat fee with minimal or no course work. Do not get duped by a professionally designed website or catalog. An “.edu” in the website address does not necessarily mean that it is a legitimate school. What may look like a shortcut to success will end up as a complete waste of money as most employers and accredited schools will not recognize a degree or credits from a diploma mill.

While not foolproof, checking if an institution is properly accredited by an agency recognized by the U.S. Department of Education can help you avoid enrolling in a diploma mill. Be careful of schools attempting to deceive prospective students by advertising accreditation from an agency with a professional sounding name or one named similarly after a legitimate accreditor.

Never be afraid to ask too many questions. What is the school’s success rate? Get information about job placement and average salaries for graduates in the program you plan to pursue. Are the school’s loan default rates high? That may be a sign graduates are having difficulty obtaining desired jobs. It is important to also ensure that if your planned profession requires a license, the school’s program that leads to licensure will meet your own state’s licensing requirements. Different states may have different requirements to obtain a license.

Please review the resources below for more tips and information on avoiding diploma mills and choosing a school that is right for you:

<https://cca.hawaii.gov/hpeap/>

<https://cca.hawaii.gov/ocp/udgi/>

<https://nces.ed.gov/collegenavigator/>

<https://studentaid.ed.gov/sa/prepare-for-college/choosing-schools>

<https://www.consumer.ftc.gov/education>

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.

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

We are top officials of the Federal Government contract review panel who are interested in importation of goods into our country with funds which are presently trapped in Nigeria. In order to commence this business we solicit your assistance to enable us to transfer info your account the said tapped funds...

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.

GENETIC TESTING (MEDICAL) FRAUD

Across the nation genetic testing company representatives are offering “free” genetic tests to Medicare beneficiaries. These tests can also be referred to as DNA screenings, cancer screenings, and hereditary testing, to name a few. The representatives go to senior centers, senior housing, health fairs, and even parking lots to convince people to let them take a cheek swab for testing. They advertise on TV and online. They promise that the results will help recipients avoid diseases like cancer, Parkinson’s and even dementia. All they ask for in return is the person’s Medicare number. Giving out your Medicare number can put you at risk, compromise your Medicare benefits and cost you a lot of money.

HEARING AID DEALERS AND FITTERS FRAUD

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. To check a license or complaint history, go to BusinessCheck.hawaii.gov or to report suspected fraud, call DCCA RICO at (808) 587-4272.

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:** 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 the victim 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.
- **Flipping Fraud:** In this reverse mortgage scam, smooth-talking realtors seek out seniors and get them to take out a reverse mortgage to buy a lower-cost house, without having to put any money down. These homes are often distressed properties that have been given a facelift but are really in poor condition. The scammers help the homeowners obtain a special type of reverse mortgage called a "Home Equity Conversion Mortgage (HECM) for purchase" to pay for the house, then find a way to divert some or all of the proceeds to themselves. The seniors think they're receiving housing through a Housing and Urban Development program.



PREVENTIVE 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.
- If you have a reverse mortgage, remember that you are responsible for the insurance and taxes.



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.

To report fraud, contact your local police department and/or the DCCA Office of Consumer Protection at (808) 586-2630.

INSURANCE FRAUD

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

SELECTING AN AGENT

Whether looking for an agent or thinking about switching agents or companies, it's a good idea to have several to choose from. Get referrals from family, friends, neighbors and colleagues. When asking around, find out why they like the agent. Is the agent friendly and knowledgeable? Did the company do a particularly good job handling a claim? Small business owners can talk with local trade associations or other similar business owners, which might have related insurance needs. Search the line of coverage on the Internet. The largest companies writing that type of insurance will typically be the first listings. Many companies also post a list of agents online.

When evaluating the list of options, consider these things:

- **Licensing:** Make sure the agent and the insurance company are licensed in Hawaii. Consumers can check company licensing information online on the National Association of Insurance Commissioner's Consumer Information Search (NAIC's CIS) at naic-cms.org/consumer.htm. Agent and company licensing information is also available on the DCCA Hawaii Insurance Division website at insurance.ehawaii.gov/hils.
- **Complaints:** Check the NAIC's CIS or call the Hawaii Insurance Division at (808) 586-2790 for complaints filed against the company. The Insurance Division can also check for complaints filed against agents.
- **Financial Strength of the Company:** Evaluate the company's financial rating. There are five major rating services. Each has their own criteria for rating that uses a combination of qualitative and quantitative numbers to assess the company. Generally, a letter rating from A to F is assigned to the company. Be sure to review how the rating agency assesses the company and understand the rating system.
- **Ask Questions:** Have conversations with prospective agents. Explain the situation and ask for a quote. If consumers had a particularly interesting insurance experience, ask how the agent and the company they represent would have dealt with the circumstances. This is an opportunity to see how the agent works.

WHAT TO EXPECT

With a short list of potential agents, what should consumers expect when visiting the office to purchase coverage?

- **Answers to Questions:** If consumers have questions about the quote or coverages needed, this is the time to ask. If the agent can't answer the questions, they should offer to find out the answer. An agent should never leave a question unanswered prior to purchase.
- **Choices:** Evaluate the options to ensure the selected company and policy best suits the situation. 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 to secure coverage with one insurance agent or company.
- **Company Explanation:** If the agent doesn't state the company where coverage will be placed with and why that company has the best coverage, ask why they chose that company.
- **Honest Sales:** Don't feel pressured to choose an agent, a company or a quote. If an offer seems too good to be true, it probably is.

PROTECT YOURSELF

Insurance fraud can happen to anyone, anywhere. Consider these tips during the purchasing process.

- Don't give out any personal information such as your Social Security Number or bank information over the phone until the legitimacy of the insurance company and agent is confirmed with the Hawaii Insurance Division.
- Ask for copies of all signed paperwork and keep a copy of the payment receipt or check for the initial premium paid to the agent for the policy.
- Call the insurance company if a copy of the insurance policy outlining coverage and its limitations is not received within 30 days of purchase.

The best way consumers can protect themselves is to research the agent and company they're considering. Always stop before writing a check or signing the contract. Confirm both the agent and company are licensed to write insurance in Hawaii.

WHERE TO GET HELP

Consumers who feel that they have been taken advantage of should contact the Hawaii Insurance Division's Investigations Branch at (808) 586-2790. For more information about Hawaii's insurance industry, visit insurance.hawaii.gov.

INSURANCE FRAUD AFFECTS EVERYONE

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 Hotline at (808) 587-7416.

INVESTMENT (SECURITIES) FRAUD

In Hawaii, we have been seeing an increase in investment fraud. This type of fraud involves the sale or solicitation of securities, Ponzi schemes and other investment schemes. Sometimes the person soliciting an investment is not properly registered to do so, while in other instances, the fraud involves a registered professional who pressures or persuades an investor to make an inappropriate investment 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. Invest wisely by doing your research, getting all the details, and understanding the terms of the investment before signing any documents and before making any payments.



PREVENTIVE TIPS AGAINST SECURITIES 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.
- Check registration information and view background and complaint history of the person you are dealing with. Here are a few website you can use:
 - » The U.S. Securities and Exchange Commission (SEC) – investor.gov
 - » The U.S. Commodity Futures Trading Commission (CFTC) – smartcheck.gov
 - » The Financial Industry Regulatory Authority (FINRA) – brokercheck.org
- Call the DCCA Office of the Securities Commissioner at (808) 587-2267 to see if the investment adviser, representative, broker-dealer, agent or the investment is properly registered in Hawaii.

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.

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 (signature)
Mr. John Doe



REMINDERS

- 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 thieves 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. Type 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 department, the DCCA Office of Consumer Protection at (808) 586-2630 and the FBI at (808) 566-4300.

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 such as 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 DCCA 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 DCCA Consumer Resource Center at (808) 587-4272 or visit the DCCA OCP website at cca.hawaii.gov/ocp/ for more information about filing a complaint.

If you have been victimized by a mortgage servicer or mortgage lender, contact the Division of Financial Institutions at (808) 586-2820 or visit the DCCA DFI website at <http://cca.hawaii.gov/dfi/> and file a complaint.



PREVENTIVE 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.

OBITUARY SCAM

Scammers read obituaries from the local paper and call the deceased relative's family and demand money for a supposed outstanding debt that the deceased left behind. To report fraud, contact your local police department and/or the DCCA Office of Consumer Protection at (808) 586-2630.

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 (for example, legal services). For example, you want to sell your phone for \$500. The scammer pretends to be a buyer from out of the country. 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 U.S. 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.



PREVENTIVE TIPS ON OVERPAYMENT, FAKE REFUND, AND FAKE CHECK FRAUD

- Do not deposit a check for more than the agreed amount. If the purchaser overpaid, they need to send 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 Northwest + Pacific 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 the DCCA Office of Consumer Protection at (808) 586-2630.
3. Call the Federal Bureau of Investigation (808) 566-4300.



PONZI SCHEMES

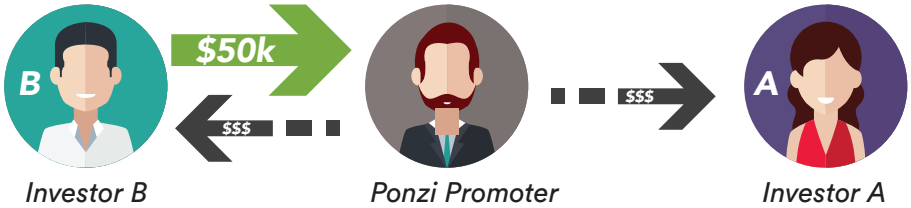
The “Ponzi scheme,” named after the 1920’s swindler Charles Ponzi, is a ploy where earlier investors are paid with funds of subsequent investors. In a Ponzi scheme, claims of underlying investments are bogus; the whole scheme depends on the money coming in from new investors. Very few, if any, actual 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. A con artist lures investors by offering investments with no risk and high returns. Earlier investors are paid with funds given by later investors rather than from actual profits earned. Since investors have received payouts, they believe the investment is real and invest more money or encourage others, often times friends and family, to invest too. The scheme collapses when the con artist cannot keep up with the required payments. In many cases, the Ponzi promotor will try to run off with the money.

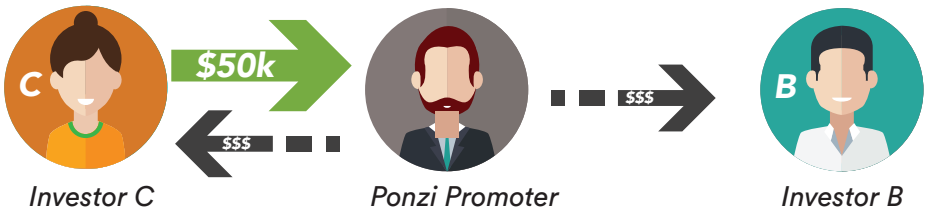
UNDERSTANDING A PONZI SCHEME



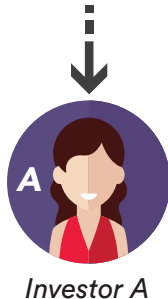
- Investor A invests \$50,000.
- To keep Investor A fooled, the Ponzi promoter pays Investor A a little bit of money each month in so-called “interest.”



- Investor B invests in \$50,000.
- Investor A is paid more fake interest with Investor B’s money
- Investor B is paid a little bit of “interest” to make him think that there really is an investment



- Investor C invests \$50,000.
- Investor A and B are paid “interest” with Investor C’s money.
- Investor C is paid “interest” with her own investment
- The Ponzi Promoter keeps most of the money.





PREVENTIVE 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.
- **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.
- **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. In many cases, the victims are part of a trusted network and may rely on prominent or influential leaders in their community. Be alert to any sales pitch that plays on your emotions, including your feelings of trust, common affiliations and friendship.
- **Understand the investment.** Ask detailed questions about the investments and those selling the investment, and get clear and direct answers before you invest. Don't let an "inside tip" override careful judgment. If the investment is 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 can 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.

- **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 Securities Compliance Branch at (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.



PURCHASING ONLINE SCAM

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.

To report fraud, contact your local police department and/or the DCCA Office of Consumer Protection at (808) 586-2630.



PREVENTIVE TIPS WHEN PURCHASING ONLINE

- Do not wire money.
- Avoid doing business with anyone who wants to operate outside of a monitored website.
- Check history, and 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, PayPal or Cash on Delivery (C.O.D.).
- Be cautious if the seller insists on payment by wire transfer, cashier's check or money order.

RENTAL SCAMS

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.

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.



PREVENTIVE TIPS FOR AVOIDING RENTAL SCAMS

For Renters:

- Before renting, you or 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 they say he they are 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.

ROMANCE SCAM

Scammers are using dating sites and apps (phone calls too) to scout for lovesick men and women. Before they know it, these men and women are being romanced and forging a long distance relationship. What happens next is the scammer is saying they are in need of money to get out of a debt, bad financial investment, medical bills, etc. And, can't be with them until they are bailed out. Or, the scammer will convince the victim to open the account in their name or register a limited liability company and allow money transfers to flow into the account. In reality, the fraudsters transfer stolen money into the account and instruct their unsuspecting crime accomplices into forwarding the money to accounts controlled by the fraudsters.

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 that a contractor's license is required in Hawaii to install low-voltage alarms and to perform electrical work. To check a license or complaint history, go to BusinessCheck.hawaii.gov or to report suspected fraud, call DCCA RICO at (808) 587-4272.

SOLAR PANELS/PHOTOVOLTAIC (PV) PANELS OR OTHER DISTRIBUTED ENERGY RESOURCES (DER) SCAM

Installing photovoltaic (PV) panels on rooftops or other distributed energy resources (DER), such as energy storage batteries, to reduce 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 double check with your utility company to verify that everything is in line with proper procedure. For more information, contact your utility company.



PREVENTIVE TIPS WHEN INSTALLING PV PANELS AND AVOIDING SCAMS

- **Do Your Research and Get Multiple Quotes.** There are different PV technologies and they are improving. Doing some research will help you understand what will be added to your home and whether you are getting a quote that makes sense. Doing research on the vendor on DCCA's BusinessCheck.hawaii.gov will provide information about whether the company is registered and also allow you to see any complaints about a vendor. 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 receive the contract, make sure you understand all the terms before you sign. What's being guaranteed? With so many components in a PV system or energy 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 or energy system, such as a combined PV and battery system. Leasing, power purchase agreements, and loans can look attractive on paper, but make sure you understand the costs and risks involved. It is important to understand the responsibilities that system owners may have under the DER program so do not feel pressured to sign any agreement until you are comfortable. If necessary, have the vendor come back at a later date to allow the time you need to read and understand what you are signing.
- **Ask About Necessary Upgrades and Updates.** Once you sign an agreement with the vendor and utility, you will be responsible to uphold the agreement's terms and conditions. This may include the need to make equipment upgrades and/or software updates in the future. Ask your vendor upfront whether they will agree to provide these future upgrades and updates as part



of your system installation. If they say no, you may have to incur additional costs to remain connected to the electrical grid or to participate in certain DER and demand response (“DR”) programs in the future. If they say yes, make sure your contract with the vendor reflects this commitment as well as any charges. This will allow you to follow up with your vendor to make sure they honor their commitments.

- **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/). The vendor may provide estimates of how much you might save on your bill but take the time to evaluate whether the system makes sense for you if the actual savings vary significantly from or even end up lower than the estimate.
- **Hire a Licensed Contractor.** Trying to cut costs by taking up an offer from an unlicensed worker is playing with fire. Do it right and hire a reputable licensed contractor to avoid headaches. The DCCA Regulated Industries Complaints Office (RICO) is a great resource to check on contractor businesses and individuals. Go to BusinessCheck.hawaii.gov or give RICO a call at (808) 587-4272.
- **Solar Maps.** 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.

- **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. Oahu customers can check their area's circuit to see if it is full by looking for the Oahu Locational Value Map on Hawaiian Electric's website:



[https://www.hawaiielectric.com/clean-energy-hawaii/integration-tools-and-resources/locational-value-maps/oahu-locational-value-map-\(lvm\)](https://www.hawaiielectric.com/clean-energy-hawaii/integration-tools-and-resources/locational-value-maps/oahu-locational-value-map-(lvm)).

Other customers should contact their electric utility company directly for the most up-to-date information. With the growing popularity of PV installations, it is still possible that changes in penetration may occur while preparing your application. Contacting the utility company or submitting an application does not reserve your spot to interconnect.

- » Hawaiian Electric Company:
(808) 543-4760, connect@hawaiielectric.com
 - » Maui Electric Company:
(808) 871-8461 ext. 2455, connect@mauielectric.com
 - » Hawaii Electric Light Company:
(808) 969-0358, connect@hawaiielectriclight.com
 - » Kauai Island Utility Cooperative:
(808) 246-4300, info@kiuc.coop
- **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 utility company to jump the queue. Customers given information along these lines should be aware 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 DER 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 DER agreement. Customers in violation risk disconnection of electric service.



COMMUNITY-BASED RENEWABLE ENERGY (CBRE)

A community-based renewable energy (CBRE) program allows electric utility customers to purchase shares in a renewable energy facility and receive utility bill credits for energy production. Customers who may be unable to install a DER system, such as renters those two, live in a high-rise condominium or those who are subject to other limiting factors, may be interested in CBRE.

Customers should again do their research to understand the agreement with a subscriber organization. Make sure that any party trying to get you to sign the agreement explains the terms and conditions and risks associated with the agreement. Contact your utility company for a list of approved subscriber organizations that are authorized to participate in the CBRE program. Hawaiian Electric customers can visit the following website for more details:



<https://www.hawaiianelectric.com/products-and-services/customer-renewable-programs/community-solar>

TAX FRAUD AND SCAMS

Taxpayers should be aware of not just the scams in obtaining your personal information via phishing, phone, and identity theft, but should also be vigilant of the following frauds and scams that will impact your tax credit.

- **Return Preparer Fraud:** Be on the lookout for unscrupulous return preparers. The vast majority of tax professionals provide honest, high-quality service. There are some dishonest preparers who operate each filing season to scam clients, perpetuate refund fraud, identity theft and other scams that hurt taxpayers. (IR-2019-32)
- **Inflated Refund Claims:** Taxpayers should take note of anyone promising inflated tax refunds. Those preparers who ask clients to sign a blank return, promise a big refund before looking at taxpayer records or charge fees based on a percentage of the refund are probably up to no good. To find victims, fraudsters may use flyers, phony storefronts or word of mouth via community groups where trust is high. (IR-2019-33)
- **Offshore Tax Avoidance:** Successful enforcement actions against offshore cheating show it's a bad bet to hide money and income offshore. People involved in offshore tax avoidance are best served by coming in voluntarily and getting caught up on their tax-filing responsibilities. (IR-2019-43)

UTILITY COMPANY SCAM

Utility company scams involve scammers impersonating utility company employees threatening to disconnect service unless the victim pays or provides personal information over the phone, email, or in-person. When in doubt, contact the utility company (such as electric, water, gas, phone, cable, etc.) directly to verify the request. Contact information for your utility company should be on the bill you received or included in your electronic monthly billing statement. Make payments directly to the utility company and keep a receipt as proof of payment.

Source: <https://www.irs.gov/newsroom/irs-concludes-dirty-dozen-list-of-tax-scams-for-2019-agency-encourages-taxpayers-to-remain-vigilant-year-round>

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.

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

COUNTY RESOURCES

CITY and COUNTY OF HONOLULU

DEPARTMENT OF COMMUNITY SERVICES

Elderly Affairs Division Information and Assistance

925 Dillingham Blvd., 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) 768-6471

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: (808) 723-3609 or 9-1-1

Fax: (808) 768-1680

Website: honolulu.hawaii.gov/police

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 OF HAWAII

HAWAII COUNTY OFFICE OF AGING

Website: hcoahawaii.org

Email: hcoa@hawaiiantel.net

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

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

HILO: (808) 961-2251

KONA: (808) 326-4646 ext. 268

Fax: (808) 961-2376

Website: hawaiipolice.com

Email: rwagner@hawaiiicounty.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, Kealahou, 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/departments/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 OF KAUAI

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

INVESTIGATIVE SERVICES: (808) 241-1633

COMMUNITY RELATIONS: (808) 241-1647

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 OF MAUI

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) 270-7774

Website: Mauicountyadrc.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 NORTHWEST + PACIFIC

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

425 Queen Street, Honolulu, HI 96813

Phone: (808) 586-1500

Fax: (808) 586-1239

Website: ag.hawaii.gov

Description: The mission of the Department is to provide excellent legal and public services in a timely manner. The Attorney General is the chief legal officer and chief law enforcement of the State of Hawaii. 180 attorneys and over 500 professional and support personnel assist the Attorney General in fulfilling the responsibilities of the office.

CRIME PREVENTION and JUSTICE ASSISTANCE (CPJA) DIVISION Community and Crime Prevention Branch

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

Phone: (808) 586-1150

Fax: (808) 586-1097

Website: ag.hawaii.gov/cpja/ccp/

Email: hawaiiag@hawaii.gov

Description: The Community and 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 and 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; maintains a computerized juvenile offender information system.

CRIMINAL JUSTICE DIVISION (CJD)

Website: ag.hawaii.gov/cjd

Description: The Criminal Justice Division is the criminal prosecution arm of the Attorney General. The mission of the Division includes to enforce the laws of the State of Hawaii, to ensure public safety, and to advocate for the passage of laws that protect the people of Hawaii.

HAWAII INTERNET CRIMES AGAINST CHILDREN (ICAC)

235 S. Beretania Street, 16th Floor, Honolulu, HI 96813

Phone: (808) 587-4114

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 using 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).

MEDICAID FRAUD CONTROL UNIT (MFCU)

707 Richards Street, Suite 402, Honolulu, HI 96813

Phone: (808) 586-1058

Fax: (808) 586-1077

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.

TAX AND CHARITIES DIVISION

425 Queen Street, Honolulu, HI 96813

Phone: (808) 586-1454

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 and other state departments and agencies relating to tax matters. The division also represents the Attorney General in her capacity as *parens patriae* in the oversight and enforcement of laws pertaining to charitable trusts, public charities, public benefit corporations, and private foundations. The division is responsible for the registration and oversight of charities fundraising in the State, as well as professional solicitors and professional fundraising counsels under the States' charitable solicitation laws codified at Chapter 467B, Hawaii Revised Statutes ("HRS"). The division is also the custodian of certifications by charities that issue charitable gift annuities under HRS § 431:1-204.

DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (DCCA)

DIRECTOR'S OFFICE

CONSUMER EDUCATION PROGRAM

Description: Provides consumer education information statewide to Hawaii residents to help them make wise choices in today's ever-changing marketplace. Distributes fraud prevention information and sponsors the Consumer Education Fair (March), Military Consumer Fair (July), and participates in senior fairs and community events throughout the state.

Website: cca.hawaii.gov

Email: dcca@dcca.hawaii.gov

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

Phone: (808) 587-DCCA / (808) 587-3222

NEIGHBOR ISLANDS: 1-800-394-1902

BusinessCheck.hawaii.gov

This website will allow consumers to check out businesses, individuals or licensed professionals that you intend to hire or do business with. It offers a number of online resources for consumers including licensee status and licensing complaints, tax and business registration, and other educational materials. As the search functions for licensee and business status is separate from complaints history, users are encouraged to use all of the available options below.

Business Name Search

Check on a business registered to do business in the Hawaii. Find out when the business was established, the names of the people involved, and any other previous names of the entity.

Business Complaint History

The Office of Consumer Protection enforces general consumer protection laws and investigates unfair or deceptive practices. Find out if a business has general consumer complaints. Please also consider using the Licensee Complaint History Search, which covers infractions relating to professional or vocational licenses.

Licensee Name Search

Certain services require the use of a professional licensed by the Professional and Vocational Licensing Division. Use this function to find out if a license is up to date or valid.

This website allows you to search for information about professionals licensed by DCCA. The Department is responsible for 25 professional boards and 26 licensing programs, for a total of 51 different professions and vocations which can be found at: cca.hawaii.gov/pvl. If a professional is not listed, it may be licensed by other Federal, State, or local government agencies.

Licensee Complaint History Search

Licensed professionals may have had prior complaints filed with the Regulated Industries Complaints Office. Find out if your licensed professional has any prior complaints or disciplinary actions.

This site provides information about complaints involving professions licensed by the Professional and Vocational Licensing Division as well as unlicensed activity investigations related to those professions. For complaints against Cable Franchises, Financial Institutions, Securities Dealers, Insurance Entities, and Utilities please check with the appropriate DCCA agency. Please also use the Business Complaint History function for consumer complaints, which are classified differently than license violations.

General Excise Tax License Search

Check on whether a business or individual has a general excise tax license with the State of Hawaii Department of Taxation.

Final Orders and Disciplinary Actions

These actions include dispositions based upon either the results of contested case hearings or settlement agreements. Respondents enter into settlement agreements as a compromise of claims and to conserve on the expenses of proceeding with an administrative hearing.

Consumer Education Materials

Find a Frequently Asked Questions (FAQ) and educational materials including informational brochures, a military consumer guide, and guides to preparing for natural disasters.

CONSUMER INFORMATION LINE

Description: 24-hour, automated system that contains prerecorded consumer messages.

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 and MOLOKAI

Toll Free 1-800-468-4644.

DCCA ONLINE SERVICES

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.

Website: cca.hawaii.gov/resources/

MILITARY CONSUMER FRAUD GUIDE

Description: Hawaii is home to 47,000 active duty service members and 5,500 National Guard personnel – many of whom face unique challenges due to permanent change of stations. To assist in consumer education for the military and their families, a Military Consumer Fraud Guide is available for download or order at <http://cca.hawaii.gov/militaryconsumer/>.

This booklet offers comprehensive guidelines to protect oneself from fraudulent activities and provide the necessary information to live and work in the State of Hawaii. Information about various issues and consumer topics that often affect our military community are highlighted within including housing, buying a car, payday lending, identity theft, and more. It also provides insight into laws and regulations that are important to know such as attaining a professional license or starting your own business.

Website: cca.hawaii.gov/militaryconsumer/

BUSINESS REGISTRATION DIVISION (BREG)

BUSINESS REGISTRATION BRANCH

Description: Maintains the business registry for all corporations, limited liability companies, general partnerships, limited partnerships, limited liability partnerships and limited liability limited partnerships conducting business activities in the State. In addition, the registry contains trade names, trademarks, service marks and publicity name rights.

335 Merchant Street, Suite 201, Honolulu, HI 96813

Website: cca.hawaii.gov/breg

Email: breg@dcca.hawaii.gov

Phone: (808) 586-2727

BUSINESS ACTION CENTER (BAC)

Description: Provides one-on-one personal assistance to the public to facilitate state business and employer registration and tax licensing application processes. Accepts business registration filings and fees, and serves as an information clearinghouse that provides general information on county, state and federal licensing, permitting and filing requirements, and assistance programs related to business or commercial activities. Offers free educational presentations and participates in business resource events in Hawaii.

Website: cca.hawaii.gov/bac

Email: bac@dcca.hawaii.gov

OAHU: 335 Merchant Street, Suite 201, Honolulu, HI 96813
Phone: (808) 586-2545
Fax: (808) 586-2733

HILO: 25 Aupuni Street, Suite 1301, Hilo, HI 96720
Phone: (808) 961-8947
Fax: (808) 935-1205

MAUI: 2145 Wells Street, Suite 106, Wailuku, HI 96793
Phone: (808) 243-8679
Fax: (808)- 243-5807

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 and MOLOKAI 1-800-4684644 (toll free).

OFFICE OF THE SECURITIES COMMISSIONER (Part of BREG)

Description: The Office of the Securities Commissioner (OSC) regulates the registration of securities, broker-dealers and their sales agents, investment advisers and their representatives, and franchises. Investigates and prosecutes securities fraud and other state securities and franchise law violations. Provides free investor education materials, presentations, and informational displays.

335 Merchant Street, Suite 205, Honolulu, HI 96813

SECURITIES COMPLIANCE BRANCH (SEC)

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

Website: investing.hawaii.gov

Email: sc@dcca.hawaii.gov

Phone: (808) 586-2722

SECURITIES ENFORCEMENT BRANCH (SEB)

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

Website: investing.hawaii.gov

Email: seb@dcca.hawaii.gov

Phone: (808) 586-2740

Fraud Hotline: (808) 587-2267

Toll Free: 1-877-447-2267

INVESTOR EDUCATION PROGRAM (IEP)

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 Hawaii LifeSmarts Program and Competitions. Hosts Annual Financial Literacy Fair (April) and a partner with the annual Celebrating Safe Communities Event (Oct), offers free investor education presentations and participates in statewide community fairs and events.

Website: investing.hawaii.gov

Email: iep@dcca.hawaii.gov

Phone: (808) 587-7400

CABLE TELEVISION (CATV)

Description: Issues franchises to Hawaii cable companies, monitors the quality of service, and assists in facilitating a resolution of consumer complaints regarding cable matters. Advocates for and supports activities for the establishment of affordable, accessible broadband services and its use throughout the State.

335 Merchant Street, Suite 101, Honolulu, HI 96813

Website: cca.hawaii.gov/catv

Email for cable matters: cabletv@dcca.hawaii.gov

Email for broadband matters: broadband@dcca.hawaii.gov

Phone: (808) 586-2620

DIVISION OF CONSUMER ADVOCACY (DCA)

Description: Protects and advances the interests of Hawaii's consumers of regulated public utilities and transportation services.

335 Merchant Street, Suite 326, Honolulu, HI 96813

Website: cca.hawaii.gov/dca

Email: dca@dcca.hawaii.gov

Phone: (808) 586-2800

Fax: (808) 586-2780

DIVISION OF FINANCIAL INSTITUTIONS (DFI)

Description: Ensures the financial soundness of state-chartered and state-licensed financial institutions, and ensures regulatory compliance by state-licensed banks and credit unions, trusts, escrow depositories, money transmitters, mortgage servicers, mortgage loan originators and mortgage loan originator companies.

335 Merchant Street, Suite 221, Honolulu, HI 96813

Website: cca.hawaii.gov/dfi

Email: dfi@dcca.hawaii.gov

Phone: (808) 586-2820

HAWAII POST-SECONDARY EDUCATION AUTHORIZATION PROGRAM (HPEAP)

Description: Provides regulatory oversight of accredited, degree-granting post-secondary educational institutions that have a physical presence in the state.

335 Merchant Street, Suite 310, Honolulu, HI 96813

Website: cca.hawaii.gov/hpeap

Email: hpeap@dcca.hawaii.gov

Phone: (808) 586-7327

INSURANCE DIVISION (INS)

INSURANCE FRAUD INVESTIGATIONS BRANCH

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.

335 Merchant Street, Suite 213, Honolulu, HI 96813

Website: cca.hawaii.gov/ins

Email: insurance@dcca.hawaii.gov

Phone: (808) 586-2790

Fax: (808) 587-6714

INSURANCE FRAUD HOTLINE

Description: Call to report actual or suspected insurance fraud.

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 and MOLOKAI **Toll Free** 1-800-468-4644.

Website: cca.hawaii.gov/ins

Email: insurance@dcca.hawaii.gov

OFFICE OF CONSUMER PROTECTION DIVISION (OCP)

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

Website: cca.hawaii.gov/ocp

Email: ocp@dcca.hawaii.gov

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 and MOLOKAI

Toll Free 1-800-4684644.

LANDLORD-TENANT CODE INFORMATION LINE

Description: Call for information on landlord-tenant matters.

Website: cca.hawaii.gov/ocp/landlord_tenant

Email: ocp@dcca.hawaii.gov

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 and MOLOKAI

Toll Free 1-800-468-4644.

PROFESSIONAL AND VOCATIONAL LICENSING DIVISION (PVL)

Description: The Professional and Vocational Licensing Division (PVL) is responsible for licensing 52 different professions and vocations. This service assists consumers in deciding whether to use the services of that person or entity and to check whether individuals or entities are appropriately licensed. 335 Merchant Street, Suite 301, Honolulu, HI 96813

Website: pvl.ehawaii.gov/pvlsearch

Email: pvl@dcca.hawaii.gov

Phone: (808) 586-3000

REGULATED INDUSTRIES COMPLAINTS OFFICE DIVISION (RICO)

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

Website: cca.hawaii.gov/rico

Email: rico@dcca.hawaii.gov

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) 241-3300

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) 9842400, LANAI and MOLOKAI 1-800-468-4644.

CONSUMER RESOURCE CENTER (Part of RICO)

Description: The Consumer Resource Center (CRC) is part of the Regulated Industries Complaints Office (RICO). 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.

Website: cca.hawaii.gov/resources/

Phone: (808) 587-4272

Toll Free: 1-800-394-1902

LICENSE, BUSINESS, AND INFORMATION SECTION (LBIS) (Part of RICO)

Description: The License, Business and Information Section (LBIS) is part of RICO's Consumer Resource Center (CRC). The public can get basic business registration information, find out if a business or individual has a professional or vocational license, and get information about complaints filed with RICO and OCP from the LBIS.

Website: BusinessCheck.hawaii.gov

Phone: (808) 587-4272, Press 2

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: eo@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: 643-ADRC (808-643-2372)

TTY Line: 808-643-0889

Website: hawaiiadrc.org

Email: ADRC@doh.hawaii.gov

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

Description: Since 1997, SMP Hawaii has been providing outreach, education and one-on-one counseling to Hawaii's Medicare members and Medicaid recipients, their families, and their caregivers teaching them about prevention of fraud and abuse in the Medicare/Medicaid programs. To arrange for a presentation, or learn about volunteering for SMP, call 586-7319.

DEPARTMENT OF HUMAN SERVICES (DHS)

Adult Protective and Community Services Branch (APCSB)

OAHU: 1010 Richards Street, #710, Honolulu, HI 96813

Phone: (808) 832-5115

Fax: (808) 832-5670

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: 3056 Umi Street, Bsmt #1, 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 is a mandated service of APCS B providing 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: hawaiiicsreg@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 ensuring 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

64 New York Avenue, N. E., 4th Floor, Washington, DC 20002

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.

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)

Office for The Older American

General correspondence: 1700 G Street, N.W., Washington DC 20552;

Complaints: P.O. Box 2900, Clinton, IA 52733;

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

225 Reinekers Lane, Suite 325, Alexandria, VA 22314

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)

Website: fbi.gov/scams-safety/e-scams

OAHU: 91-1300 Enterprise Street, Kapolei, HI 96707

Phone: (808) 566-4300

Website: fbi.gov/honolulu

KONA: 75-5591 Palani Road, Suite 2008A, Kailua-Kona, HI 96740

Phone: (808) 329-5016

MAUI: 2200 Main Street, Wailuku, HI 96793

Phone: (808) 242-4849

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 **TTY** 1-866-653-4261

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, N.W., 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. 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) 842-3600

Fax: (816) 783-8175

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)

2614 Chapel Lake Drive, Suite B, Gambrills, MD 21054

Phone: (443) 292-4565

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 **TTY:** 1-866-290-4236

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

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 530201, Atlanta, GA 30353

Toll Free: 1-888-567-8688

Website: optoutprescreen.com

Description: The official Consumer Credit Reporting Industry Website to accept and process requests from consumers to Opt-In or Opt-Out of firms offers of credit or insurance.

UNITED STATES AIR FORCE

Office of Special Investigations

Detachment 601 Joint Fraud Program

655 Vickers Avenue, Bldg. 1105, Joint Base Pearl Harbor Hickam, HI 96853

Phone: (808) 449-7704

Fax: (808) 449-7759

Email: afosidet601.all@us.af.mil

Description: The mission of the United States Air Force Office of Special Investigations (AFOSI) 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 prosecutes cases that are referred by a federal law enforcement agency and supports training for law enforcement to improve identification of and response to elder fraud victims.

UNITED STATES CENTERS FOR MEDICAID AND MEDICARE SERVICES

Medicare

Contact Center Operations; P.O. Box 1270 Lawrence, KS 66044

Toll Free: 1-800-633-4227 or **TTY:** 1-877-486-2048

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 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 (HHS)

Office of The Inspector General (OIG)

P.O. Box 23489, Washington, DC 20026

Toll Free: 1-800-447-8477 or **TTY:** 1-800-377-4950

Website: oig.hhs.gov

Description: The OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse and mismanagement of U.S. Department of Health and Human Services' programs, including Medicare.

UNITED STATES DEPARTMENT OF JUSTICE

Office of the Inspector General (OIG)

Investigations Division

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

Toll Free: 1-800-869-4499

Fax (202) 616-9881 **OIG PUBLIC COMMENT LINE:** (202) 353-1555

Website: oig.justice.gov/hotline

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.

Office for Victims of Crime

National Elder Fraud Hotline

Toll Free: 1-833-372-8311

Website: stopelderfraud.ovc.ojp.gov/

Description: This toll-free call center helps combat fraud against older Americans and provides support for victims who have been robbed of their hard-earned savings. The National Elder Fraud Hotline is staffed by caring professionals who can provide personalized support to callers. Use this call center to report incidences of fraud; obtain a case manager who will help you through the reporting process at the federal, state, and local levels; and connect with other helpful resources on a case-by-case basis.

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

433 W. Harrison Street, Room 3255, Chicago, IL 60699-3255

Phone: (877) 876-2455

PRESS 3: For Mail Theft

PRESS 4: For Mail Fraud

Website: 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 Kalanianaʻole 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 Kalanianaʻole Federal Building, 300 Ala Moana Boulevard, Suite 1-114, Honolulu, HI 96850

Toll Free: 1-800-772-1213 or **TTY:** 1-800-325-0778

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.

