Tips to help you recover from scam calls...

Watch out for scam calls!

Have you given out your personal information over the phone? In the future, it's best not to answer the phone unless you know who's calling. If it's important, they'll leave a message. In the meantime, follow these steps immediately:

- **Call your bank if you gave out your account information.** You may want to consider changing your accounts altogether.
- **Call SHIBA at 1-800-562-6900 to report health care fraud, waste or abuse.** SHIBA shares the scam details with seniors across the state, and with programs in other states, to help warn people before they can become a victim.
- **Call 1-800-MEDICARE and let them know your Medicare number has been compromised if you gave it out.** With the new cards it'll be as simple as cancelling one and getting a new one. You'll also need to inform your providers so they don't use the old number.
- **Contact the Federal Trade Commission**
  - **Identity Theft Helpline:** 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261
  - **Email:** spam@uce.gov to forward unsolicited commercial email (spam), including phishing messages. These messages will be stored in a database that law enforcement agencies use in their investigations.

  Note: the FTC does not resolve individual consumer complaints.
- **File a police report.** You only need to make a report if you gave out your personal information such as your credit card, social security number, or routing numbers OR you experienced a money loss by sending a check or wiring money through Money Gram or Western Union.

  The police report contains specific details of the identity theft and is considered an Identity Theft Report under section 605B of the Fair Credit Reporting Act (FCRA). It entitles an identity theft victim to certain important protections that can help yourecover more quickly from identity theft down the road.
- Place a fraud alert or a freeze on your credit reports, and review your credit reports. A fraud alert or a freeze can help prevent an identity thief from opening any more accounts in your name. If you gave out your social security number, contact the toll-free fraud number for any of the following three consumer reporting companies to place a fraud alert on your credit report. The company you call is required to contact the other two companies. A fraud alert will last 90 days, while a freeze lasts until you lift it.

Continued on back

Consumer reporting agencies

TransUnion
Phone: 1-800-680-7289
Web: www.transunion.com
US Mail: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Equifax
Phone: 1-800-525-6285
Web: www.equifax.com
US Mail: P.O. Box 740241, Atlanta, GA 30374-0241

Experian
Phone: 1-888-EXPERIAN (397-3742)
Web: www.experian.com
US Mail: P.O. Box 9554, Allen, TX 75013

You can receive a free credit report from each of the three companies once a year. Requesting from one of the companies every four months allows you to look at your reports three times a year for free. Once you get your credit reports, look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information is correct, like your Social Security number, addresses, name or initials, and employers. If you find fraudulent or inaccurate information, get it removed. If you just gave out your information, likely it will not show up right away. Often times the information is kept for a year or two before it's used, so people are likely to quit worrying about it and let their guard down. Always check your credit report.

What to do if you did NOT give out personal information, but received a scam call

You do not need to call your bank, etc. However, follow these steps any time you receive a robocall or other telemarketing call and have answered the phone:

- **Hang up.** The longer you stay on the line the more attractive you are to them to call again and to sell your number to other lists. If you can, don't pick up the phone when you don't know who is calling. By answering, you're telling them you're a live line and they'll keep you on rotation. By not answering the phone you'll eventually drop off their call lists.
- **Block the number.** Most cell phones make this easy, and though telemarketers change their caller ID information often, blocking numbers will still help stop some of the calls.
- **Sign up for the Do Not Call list.** Since only reputable businesses will follow the law, this will tell you that those who continue to call are out to scam you. If you get a sales call after your number has been on the list for 31 days, complain to www.donotcall.gov or call 1-888-382-1222.
- **Report your experience to the FTC.** Go online at www.ftccomplaintassistant.gov or call 1-888-382-1222.

For more information, go to: https://dojmt.gov/consumer/identity-theft/

SHIBA OFFICE of the INSURANCE COMMISSIONER WASHINGTON STATE

SMP Empowering Seniors To Prevent Healthcare Fraud
WASHINGTON STATE SMP
Paid for by AoA and is hosted by the Washington State Office of the Insurance Commissioner
1-800-562-6900
www.insurance.wa.gov/shiba

SHP872 - 06/2019