**Recovering from a scam call**

*Have you given your personal information out over the phone? In the future, it’s best to not answer the phone unless you know who is 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 your local Montana SMP or 1-800-551-3191 to report it if it is regarding healthcare fraud, waste or abuse.** SMP shares the scam details with seniors across the state and with SMP’s in other states, to help warn people before they can become a victim.

*Note: SMP can help resolve an issue if someone billed for services in your name. Always read your Medicare Summary Notices or Medicare Advantage Explanation of Benefits and if you see something suspicious, call SMP.*

* **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 issued. If it was the old card containing a social security number, see below for additional steps. 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](mailto:spam@uce.gov) to forward unsolicited commercial email (spam), including phishing messages. These messages will be stored in a database law enforcement agencies use in their investigations.

*Note: the FTC does not resolve individual consumer complaints.*

* **File a police report.**

**The report only needs to be made if personal information, such as credit card, social security number, or routing numbers have been given out OR there has been a loss of money through the sending of a check or wiring money through Money Gram or Western Union.**

*The police report contains specific details of an 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 him or her recover 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 of any of the three consumer reporting companies below to place a fraud alert on your credit report. The company you call is required to contact the other two. A fraud alert will last 90 days, while a freeze will last until you lift it. Freezes cost $3 for each agency in Montana, a total of $9.

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

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

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

*You are able to receive a free credit report from each of the three companies once a year. Requesting from one of the companies every four months enables 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, like your Social Security number, addresses, name or initials, and employers are correct. 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 using so people are likely to quit worrying about it and let their guard down. Always check your credit report.*

**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 are telling them you are a live line and they will keep you on rotation. By not answering the phone you will eventually drop off their call lists.
* Block the number if you can. 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](http://www.donotcall.gov) or call 1-888-382-1222.
* Report your experience to the FTC online at [www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov) or by calling 1-888-382-1222.