STOP THE SCAMMERS

LEARN, PREVENT, & PROTECT

yourself with tips to spot scams and keep you safe.

IOWA | Department of Insurance and Financial Services

AARP Iowa

IOWA FRAUD FIGHTERS — SHIELD YOUR SAVINGS

IOWA DEPARTMENT OF JUSTICE — OFFICE OF THE ATTORNEY GENERAL

www.IowaFraudFighters.gov/stop-the-scammers-event/

INTRODUCTION

The Iowa Department of Insurance & Financial Services, The Office of the Iowa Attorney General, and AARP are here to help you learn and empower yourself against con artists.

This booklet provides ways to protect yourself with expert fraud prevention tips, reporting resources, and more to help you stay a step ahead of fraudsters.

TABLE OF CONTENTS

By attending this event you are entering an area where photography, audio, and video recording may occur. If you don't wish to be recorded, please see an event representative.

ABOUT US

Did you know there is a whole team dedicated to helping Iowans learn more about scams and ways to prevent fraud? The Iowa Department of Insurance & Financial Services, The Office of the Iowa Attorney General, and AARP are working together to help Iowans identify and avoid scammers' latest tactics.

About Fraud Fighters, a program of the Iowa Department of Insurance & Financial Services

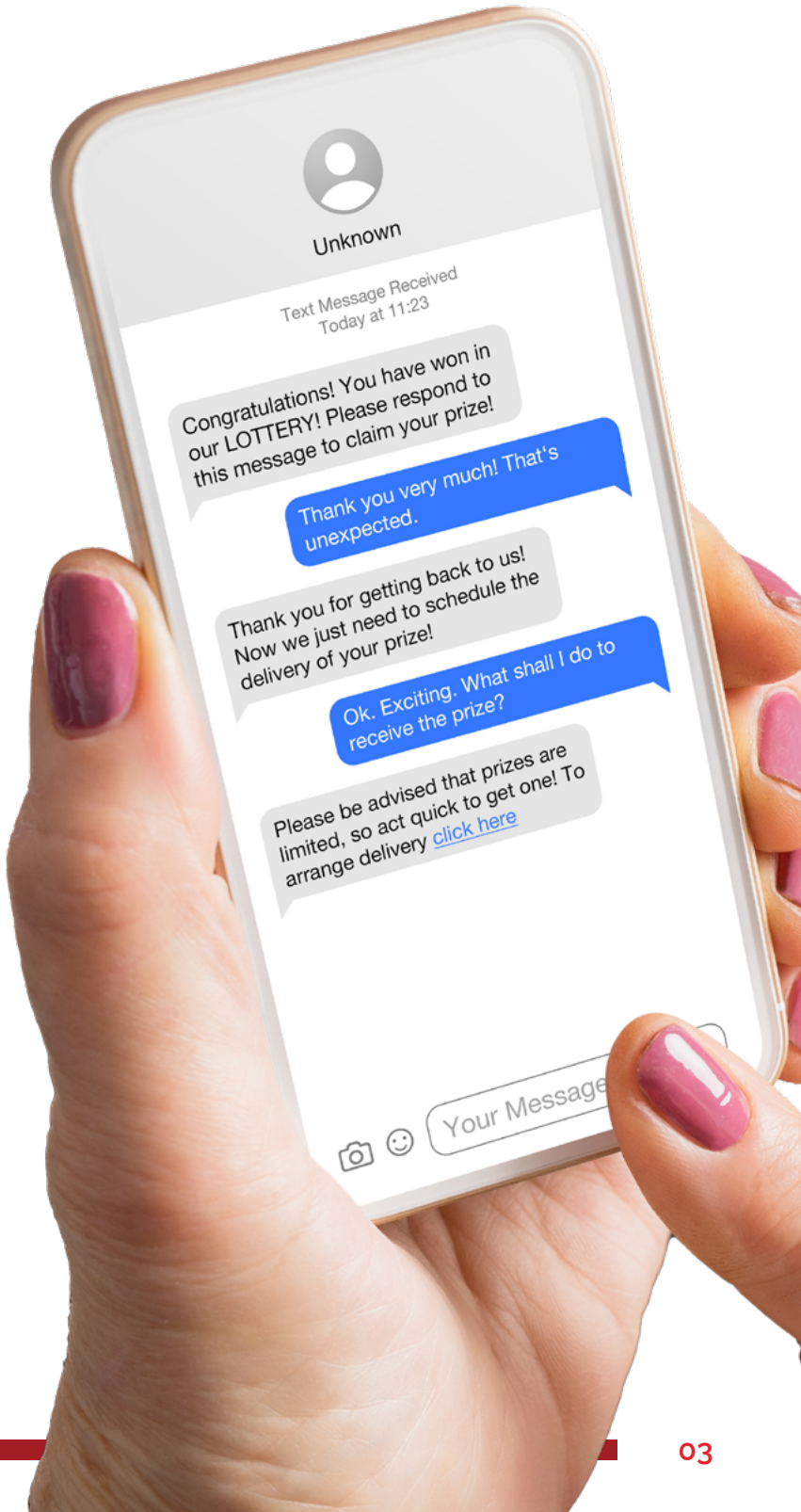
Iowa Fraud Fighters are Iowans who have pledged to be informed and careful investors. Iowa Fraud Fighters shield their savings from scammers and fraudulent investment, consumer, and Medicare insurance offers. Arm yourself with expert fraud prevention tips and learn how to avoid scams. It's time to take a stand and shield your savings. You can become an Iowa Fraud Fighter by empowering yourself to fight and report fraud. The Iowa Department of Insurance and Financial Services and other state agencies are here to help you. You can see more about us by visiting https://iowafraudfighters.gov.

About AARP Fraud Watch

The AARP Fraud Watch Network™ is a free resource for all. With AARP as your partner, you'll learn how to proactively spot scams, get guidance from our fraud specialists if you've been targeted, and feel more secure knowing that we advocate at the federal, state, and local levels to protect consumers and enforce the law. To learn more, visit aarp.org/fraudwatchnetwork.

About Iowa Attorney General's Office

The Iowa Attorney General's office protects Iowans from fraud, ensures fair competition in the marketplace, and equips Iowans with the knowledge to recognize the red flags of a scam. All too often, scammers will manipulate Iowans' emotions and take advantage of "Iowa nice." But not on our watch. The Iowa Attorney General's office is committed to slamming the scam and holding scammers accountable. If Iowans are suspicious of a scam, they should contact the Iowa Attorney General's office at 888-777-4590 or www.iowaattorneygeneral.gov/for-consumers.



SCAM TACTICS:

How They Try to Convince Us

Criminals use a variety of persuasion tactics to convince us of an untruth to steal our money or sensitive information – and they are good at it. Scammers may try to go after our money through cash, wire transfers, money transfer apps, cryptocurrency, and gift cards. Here are some of the tactics common to today's scams:

Phantom Riches
The prospect of wealth is behind many common scams, and the criminal's goal is to pressure the target into believing that a large bounty awaits. Fake lottery winnings and surefire investment schemes commonly use the phantom riches technique to coerce targets. Criminals create legitimate-looking shopping sites online and even create faux versions of the online stores of well-known retailers. If you are told you've won a sweepstakes or a lottery, but you just need to pay some fees upfront to claim your winnings, it is a scam.

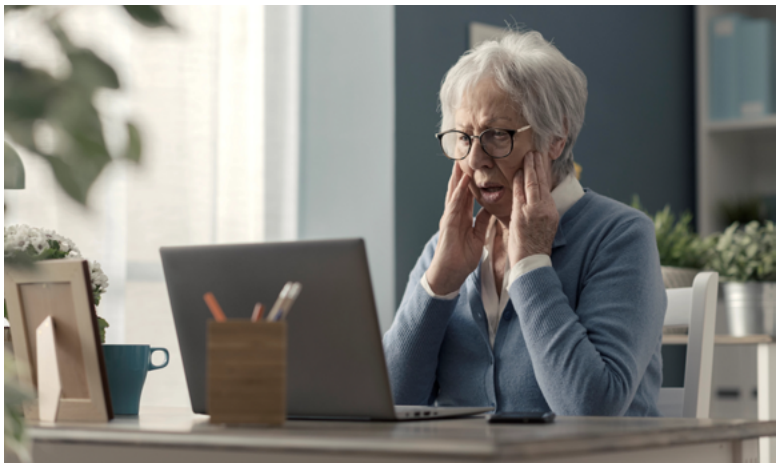
Profiling
The profiling tactic involves the criminal gathering key pieces of information about the target and using that information to establish credibility and elicit an emotional response. The goal is to get the target to act quickly to address an "urgent" situation. For example, today's scammer may peruse social media accounts to gather enough information to impersonate a family member in trouble. Be careful what you are sharing on social media and don't give out any personal information to someone you don't know!

Fear and Intimidation
Criminals commonly use fear and intimidation to get their targets. Many cases we hear about begin with inducing immediate fear, such as telling you your grandson is in danger, the police have a warrant for your arrest, or your computer has a deadly virus. And we've heard from victims that criminals will harass them, calling dozens of times a day and leaving threats on their voicemails.

Secrecy and Urgency
Scammers will create a sense of secrecy and urgency to get you to act without seeking outside support. Victims are often instructed to keep interactions secret from family members and banks. A scammer will create urgency by demanding immediate action to avoid negative consequences.

Imposter Scams
Imposter scams rely on getting the target to believe the contact is coming from a credible source — often a government agency such as Medicare or the IRS. Common social media scams involve fake profiles that appear to be celebrities, or new "friends" with profiles that are a mix of invented and stolen information.

Unusual Payment Methods
Be wary of unusual payment methods. A scammer may instruct victims to buy cryptocurrency, gold, gift cards, or mail cash. If someone asks you to send money in one of these ways, it's likely a scam.



INVESTMENT SCAMS

Ponzi or pyramid schemes promise high returns, often "guaranteed" for investors, but collapse when new investors can't be found. These schemes use funds from new investors to pay off the initial investors. Each group of new investors is used to pay off an earlier, smaller group of investors, while the majority of the money disappears into the scammer's pocket at the top of the pyramid.

Promissory notes are used by companies to raise money by selling debt, typically paying a high interest rate, to an investor. Con artists often sell promissory notes for companies that do not exist, so always check that a company is legitimate before purchasing these.

Affinity fraud targets groups, such as religious or ethnic communities, by using trusting relationships with influential or respected members of the group to attract more investors in a pyramid-type scheme.

Private placement offerings, or Regulation D, Rule 506 offerings can be used by small companies to raise funds. These offerings are unregulated and are often very risky investments or scams.

Oil and gas drilling programs are always high risk and should be researched carefully to avoid scams, especially those claiming a particular well is guaranteed to produce high returns or have attractive tax advantages.

Gold and precious metals are always risky investments. It may be a scam if the seller wants you to invest in gold mining or to purchase gold or other precious metals that will be delivered to a secured facility. Be sure the company is genuine and ensure the gold or precious metal you purchase does exist.

Free dinner seminars are often advertised in local newspapers, on websites, or through mass-mailed invitations or emails. Many of these seminars are used to sell investment products at the seminar or through later communications. Be wary if guilt, fear, or high-pressure tactics are used to try to sell products.

High-yield investment products are peddled by scammers claiming to have access to the world's leading financial institutions or banks. The scammers promise high returns at little or no risk to you by enrolling you in an elite or secret investment venture, often called a prime bank investment.

Cryptocurrency is a decentralized digital asset that operates outside the regulation of traditional banks or financial institutions. While it can be used for legitimate purchases and investments, its nature makes it a primary tool for financial exploitation. Scammers often direct victims to send funds via cryptocurrency trading platforms, P2P apps, or bank wires, favoring these methods because they allow for the rapid, international movement of illicit funds. In many cases, victims are coached to make legitimate cryptocurrency purchases on reputable exchanges, only to unknowingly transfer those assets directly into a scammer's control.

Online investment scams (aka pig butchering) are sophisticated schemes that involve criminals who build long-term trust with victims via text, dating apps, or social media. By posing as romantic interests or investment advisors, scammers lure individuals into fake opportunities—typically involving cryptocurrency or precious metals. While the platforms may look legitimate and even show "false profits," the money is never actually invested. Victims eventually find themselves unable to withdraw funds and are required to pay endless fees, leading to devastating financial losses. Always exercise caution with unsolicited contacts or offers promising "guaranteed" high returns.

DOUBLE-CHECK BEFORE YOU INVEST

Use this form to collect the information you will need to verify any investment seller or company before you make an investment. (Additional copies can be downloaded from www.IowaFraudFighters.gov.)

Seller/Agent and Company Information

Seller/Agent Name _____

Company/Business Name _____

Company/Business Address _____

Phone Number _____ Email _____

What Services Are Being Offered?

Investment:

- ☐ Stocks and Bonds
- ☐ Mutual Funds
- ☐ IRAs
- ☐ Private Placements
- ☐ Oil & Gas/Minerals

Insurance:

- ☐ Life
- ☐ Annuities
- ☐ Viaticals

Financial Planning:

- ☐ Investment Advice
- ☐ Financial Planning
- ☐ Wealth Creation

What written information will be provided? _____

Is seller/agent required to act in my best interest? Yes____ No____

Potential conflicts of interest _____

Explain commissions or fees charged _____

Licensing Information

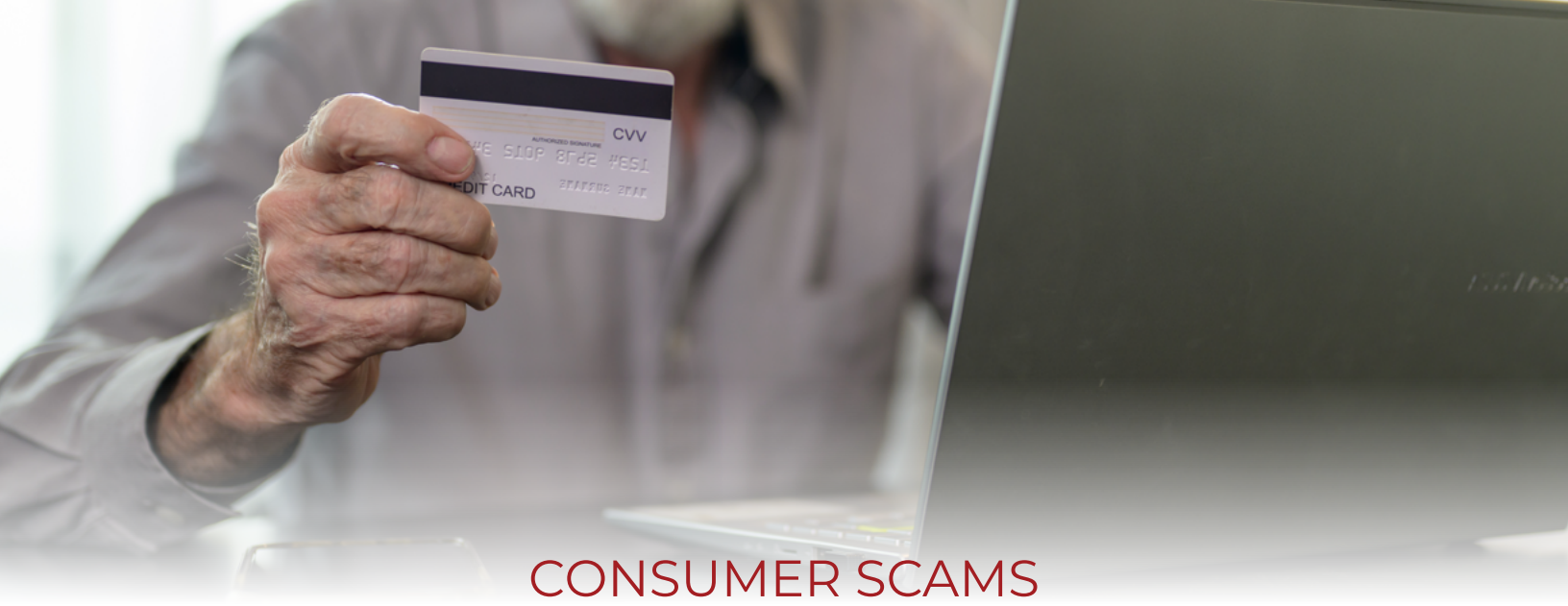
(Call to check names and/or license numbers with Iowa Insurance Division at 877-955-1212.)

Insurance License No: _____ State _____

Securities License CRD No: _____

Other License: _____ No: _____

Always request a CRD report to learn of disciplinary actions taken against the company/business, criminal convictions, settlements, bankruptcies, civil proceedings and customer complaints.



CONSUMER SCAMS

Investment schemes shouldn't be the only thing you need to guard yourself against. Fraudsters are always looking for ways to get access to your personal or financial information and money.

Tech support scams typically begin with a fraudulent charge or virus alert on a victim's device. Con artists posing as technical support, customer service, or government officials then gain contact to request fees for 'repairs.' In some instances, they use the false pretense of an investigation to pressure victims into liquidating assets and moving their funds to the scammer for 'safekeeping.'

Grandparent scams are used to coerce money from older Iowans by con artists who pretend to be a grandchild calling from a foreign country in desperate need of money to get out of jail or some other urgent trouble.

Romance scams occur when con artists strike up romantic relationships, often through social media or online dating sites, to coerce money from victims, often for travel expenses to visit the victim or for hardships the perpetrators claim they are going through.

Home repair scams are common when there has been a damaging weather event, such as a flood or tornado. Scammers pretend to be contractors or home repair specialists selling home evaluations and repairs in affected areas before disappearing without providing the services that were paid for.

Identity theft occurs when someone uses your personal information to open accounts, file taxes, or make purchases. As of July 2018, you can now freeze your credit. Refer to iowa.gov/difs for more information.

Imposter calls are robocalls that claim the IRS, other government entity, or a business is filing suit against you for owed taxes or threatening to send police to your residence if you don't pay a specific amount using prepaid cards. Remember, the IRS and other government entities will notify you by mail if it is transferring an outstanding debt to a private collection agency.

Lottery and sweepstakes scams occur when fraudsters charge an entry fee for sweepstakes or contests, or con artists sell international or out-of-state lottery tickets to Iowans. They typically seek advance payment of taxes or fees before they send a prize that never arrives or a check that bounces. If you have to pay a fee to receive your winnings, it's a scam.

Job scams occur when con artists pose as potential employers. Scammers may send you a job offer via text or email describing a job that allows you to work from home and requires little effort. These unsolicitied offers are many times too good to be true. Scammers will send what looks like an official job offer that comes with paperwork that requires your personal and financial information.

MEDICARE FRAUD

Tips to Prevent Medicare Fraud

1. Stay informed about enrollment — Get the enrollment dates and plan information from an official source, make an appointment with a SHIIP representative to review plan options, and remember that Medicare plans cannot be sold door-to-door.
2. Don't carry your Medicare card — Unless you're going to the doctor's office, it is best to leave your card at home in a safe place.
3. Protect your personal information — Medicare will never call to ask for your personal financial information or Medicare number because they already have it.
4. Review your statements — Check your statements each month for unfamiliar charges or charges for services/products you did not receive.
5. Confirm suspicious mailings — If a Medicare mailing looks suspicious, SHIIP and Senior Medicare Patrol can review and confirm if it is an official mailing or a scam.

About Senior Health Insurance Information Program (SHIIP) and the Senior Medicare Patrol (SMP)

Medicare loses an estimated $60 billion each year due to fraud, errors, and abuse, though that number is impossible to measure. Every day, issues related to these problems affect people across the country, often costing them time, money, and well-being.

You can PROTECT yourself from Medicare fraud, errors, and abuse; DETECT potential fraud, errors, and abuse; and REPORT your concerns. The Iowa Senior Medicare Patrol (SMP) and our trained volunteers educate and empower Medicare beneficiaries in the fight against health care fraud. If you suspect Medicare fraud, errors or abuse please report it by calling Medicare at 1-800-MEDICARE (1-800-633-4227), or your Iowa SHIIP-SMP at 1-800-351-4664 (TTY 1-800-735-294).

If you need assistance to report Medicare fraud, learn more about your Medicare coverage options, or review your statements, please contact a SHIIP representative or your local Senior Medicare Patrol.

SHIP
State Health Insurance Assistance Program

SMP
Senior Medicare Patrol
Preventing Medicare Fraud

OUR TOP 10

Fraud Prevention Tips

1. Don't be a courtesy victim. You don't owe your time to anyone. It's OK to just say no and hang up.
2. Check out anyone you don't recognize. Always contact the Department of Insurance and Financial Services at 877-955-1212 to double check that the financial professional and the investment offer are legitimate.
3. Monitor your money. Insist on receiving regular reports on your investments and financial accounts, check your credit score reports every year, and freeze your credit.
4. Never judge a person's integrity by the sound of his or her voice. Scammers know how to sound professional and friendly to gain your trust.
5. Watch out for anyone who pressures you by playing on fear, urgency, or strong emotions. Scammers often try to rush decisions by making situations sound scary or time-sensitive, hoping you won't stop to think. Take your time — pause, verify the information, and talk with someone you trust before taking action.
6. Be wary of unsolicited offers. Stop if you can't find current information about their company. If it sounds too good to be true, it is probably neither good nor true.
7. Always ask questions. Question everything. Your financial advisor or stockbroker is required to explain any restrictions before you invest.
8. Be leery of unusual payment methods. If someone is asking for payment in gift cards, cryptocurrency, gold, prepaid debit cards, or cash in the mail, it's probably a scam.
9. Watch out for "reload" scams. If you lost money once, you may be contacted by scammers pretending to be fund recovery firms or federal investigators.
10. Don't be embarrassed to report fraud. Reporting fraud is a responsible step in handling your finances, so don't be afraid or embarrassed to report it if you are victimized. You can save another person from becoming a victim.

HOW TO FREEZE YOUR CREDIT

Who Should Do This?

Everyone, regardless of age, income, or credit history.

A credit freeze provides maximum protection for your credit file. And it's free.

How to Freeze Your Credit

To freeze your credit, you must contact each of the three major credit bureaus.

Equifax
800-685-1111
www.Equifax.com

Experian
888-397-3742
www.Experian.com

Transunion
888-909-8872
www.TransUnion.com

Provide your name, address, date of birth, Social Security number, and other requested information. Each credit bureau will give you a password or personal identification number (PIN).

IMPORTANT: Keep the PIN or password in a safe place where you can access it. You cannot lift the freeze without it. If you lose this information, the credit bureaus cannot look it up for you.

How to Lift a Credit Freeze?

If you need to lift a credit freeze — when you're taking out a bank loan, for example, or financing a car — ask your creditor which bureau they use for credit applications. Then contact only that credit bureau to arrange a lift on the credit freeze. There's no need to unfreeze all three credit bureaus.

Select a temporary lift of the freeze, and at the end of a time limit you choose, your credit is automatically frozen again. Or you may choose to unfreeze your credit without a time limit. Just don't forget to freeze your credit again once your credit application is reviewed.

If you make the request by phone or online, the freeze must be lifted within an hour. If the request is made by mail, the credit bureau has three business days after recieving the request.

A Credit Freeze Won't...

- Prevent you from getting a free annual credit report
- Prevent you from opening a new account (Follow the steps to unfreeze your credit, above).
- Prevent a thief from making changes to your existing accounts. Keep monitoring all bank, credit card, and insurance statements for fraudulent transactions.

Don't Give Out Personal Information

- For help with questions or concerns about freezing your credit, visit the Iowa Insurance Division at iid.iowa.gov/security-freeze-for-credit-reports
- To report a suspected theft of your identity, contact the Federal Trade Commission (FTC) at www.IdentityTheft.gov
- For more information on identity theft, visit the FTC at consumer.ftc.gov/topics/identity-theft

WHAT IS A TRUSTED CONTACT?

Naming a Trusted Contact on your financial accounts is a simple way to add an extra layer of protection for you and your money. A Trusted Contact is someone your financial institution can reach if there are concerns about potential fraud or if they are unable to contact you. This person does not have access to your accounts or control over your money. Understanding what a Trusted Contact can — and cannot — do can help you decide if this added safeguard is right for you.

What's a Trusted Contact?

A Trusted Contact is an individual chosen by the account holder and authorized to receive information regarding the financial activities of the client, in certain limited circumstances, particularly in the event of suspected financial exploitation.

What they can do:

A Trusted Contact can confirm a client's contact information, share current health status, and discuss unusual account activity with you, the financial representative.

What they can't do:

- A Trusted Contact cannot act on your behalf or make decisions for you.
- They cannot execute transactions, such as withdrawals, transfers, or changes to your account.
- They do not have access to your account information, balances, or statements.
- Naming a Trusted Contact does not give them control over your money in any way.

Why it's important:

Federal rules allow brokerage firms to share limited information with a Trusted Contact if there is a temporary pause on transactions due to concerns about possible financial exploitation. Experience has shown that involving a Trusted Contact early can be critical when fraud or exploitation is suspected, helping prevent money from being lost. Choosing a Trusted Contact ahead of time — and talking with them about this role — adds an important layer of protection and makes it easier to act quickly if a problem arises.

Anyone who works with or supports older adults or dependent adults is encouraged to help them consider naming a Trusted Contact on their financial accounts. If you have questions or need help adding a Trusted Contact, call (515) 654-6600 or (877) 955-1212, or refer to the information provided by your brokerage firm.

SCAM VICTIM CHECKLIST

I am the victim of a scam, now what?

1. **Remember — you are the victim of a crime, and you are not alone**
    A. Give yourself grace. You're understandably in pain and feel exhausted. Rest and regroup. When you're ready, we strongly encourage you to reach out to any of our trauma-informed resource partners.

2. **Collect all available evidence and report the scam *as soon as possible:***
    A. Report to your local law enforcement, the Iowa Insurance Division's Senior Financial Exploitation Investigator (515-654-6464) or the Iowa Attorney General's Office (515-281-5164) — you only need to report to one of these agencies.
    B. We also encourage you to report the scam to IC3.gov for reporting/tracking.
    C. You can also report the scam to FTC.gov for reporting/tracking.

3. **Contact all your financial institutions to inform them you were a victim of a scam**
    A. Ask them to place a fraud alert on your accounts for added protection.
    B. Ask about the ability to reverse/cancel any fraudulent transactions/charges.
    C. Discuss with them the potential need to create new accounts.
    D. Change your passwords on all online banking/investment accounts.
    E. If your credit/debit cards were compromised, ask to be issued new cards.
    F. Continue to monitor all your financial statements closely and report any fraudulent activity to your financial institution right away.

4. **If scammers have had access to your computer, phone, or other device:**
    A. Disconnect your device from the internet.
    B. Update your computer's security software, run a scan, and delete anything that identifies as a problem. Then take other steps to protect your personal information.
    C. If you need assistance, contact a local computer repair business.

5. **Scammers share victim information!**
    A. Contact your phone provider and get a new phone number.
    B. Get a new email address if a scammer ever communicated with you via email or had any access to your devices/information.
    C. Delete any apps the scammer used to communicate with you.
    D. Monitor any social media or online profiles for private information that may be shared publicly. Review your privacy settings and be cautious of connecting with unknown individuals online.
    E. **BEWARE** of secondary scams — scammers will attempt to present themselves as trusted contacts — when in doubt, contact one of the above reporting agencies! Do not answer calls, texts, or emails from individuals you do not know.

FREQUENTLY ASKED QUESTIONS

How can I avoid telemarketing calls?

Don't answer your phone to unknown numbers, let them leave a voicemail. The more you answer your phone to telemarketers and scammers the more calls you will receive. Add your number to the National Do Not Call Registry. Register your phone number by calling 888-382-1222 or visiting www.DoNotCall.gov.

How can I deal with pushy callers?

Don't feel that you have to be nice or polite. You don't have to talk to these people. You can just say no and hang up, or better yet, don't answer your phone to unknown callers.

What if I'm asked for personal information?

Never send money, give out credit card numbers and expiration dates, bank account numbers, dates of birth, personal identification numbers, or Social Security numbers to unfamiliar companies or people you don't know, or if you have not initiated the conversation.

What terms should raise concern about a proposed investment?

Be wary of these terms: high rate of return, risk-free investment, or guaranteed or insured against loss. High rates of return are usually accompanied by high risk and legitimate investments are not guaranteed against loss. If it's too good to be true, it is!

What if I'm pressured into making an immediate decision?

Don't let anyone pressure you into a quick decision. Do your own research and call the Department of Insurance and Financial Services at 877-955-1212 and consult with someone you trust before making any purchase or investment.

What protects me from losses associated with my investment?

Securities regulators make sure companies abide by securities laws and rules, but they do not insure investments. You should determine what degree of risk you are willing to take and be prepared to experience possible losses.

Can I trust that professional promotional materials and websites are reliable indicators of legitimate investment opportunities?

Promotional materials, websites, company addresses, and testimonials from investors can all be part of a fraudulent scheme to lure you into a scam. Do your homework before you part with your money.

How can I make sure the people trying to sell me investments or insurance are reliable?

One way is to ask for written materials and then verify the information they provide with the Department of Insurance and Financial Services.

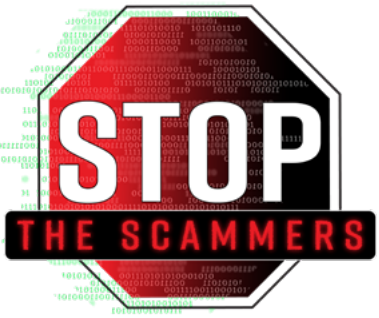
Should I report fraud?

Yes. Don't let embarrassment over your loss stop you from reporting fraud or suspicious activity and protecting others from the same scheme. It is a brave and responsible step to report fraud. Use the contact information in this booklet if you need assistance in reporting fraud.

Still have more questions?
Check out iowafraudfighters.gov or aarp.org/fraudwatchnetwork. You may also call 515-654-6464, and we will help you answer any questions you may have!

NOTES

NOTES



REPORT SUSPICIOUS ACTIVITY

If you or a loved one has fallen victim to scams or fraud, you are not alone. Thankfully, you have a whole team of people who are here to help you report and learn more about fraud. Reporting scams can help prevent fraud for others in the future. Call or visit the below organizations' websites to report fraudulent activity and learn more.

Iowa Department of Insurance and Financial Services
Check with the Iowa Department of Insurance and Financial Services if you suspect investment fraud.
(515) 654-6464 / www.iowa.gov/difs

Iowa Attorney General
You can file a complaint with the Iowa Attorney General.
(888) 777–4590 / www.iowaattorneygeneral.gov

Senior Medicare Patrol
If you suspect Medicare fraud or to schedule a presentation, call Senior Medicare Patrol (SMP).
(800) 351–4664 / www.shiip.iowa.gov

AARP Fraud Watch Network™
Visit AARP for more free resources about scams and fraud.
For scam alerts, text FWN to 50757.
(877) 908-3360 / www.aarp.org/fraudwatchnetwork

IOWA | Department of Insurance and Financial Services

AARP Iowa

IOWA FRAUD FIGHTERS — BUILD YOUR SAVINGS

IOWA DEPARTMENT OF JUSTICE — OFFICE OF THE ATTORNEY GENERAL