## Chances are good that the caller will hang up if you challenge him.

**Example:**
The senior answers his phone and a young voice says, "Hey, Grandpa, it's your favorite grandson, and I'm in trouble."

**Do not fill in any "blanks" for the scammer:**
"John, is that you?" It will be easy for the caller to then respond, "Yes, it's John…"

**Best way to get the scammer to hang up the phone:**
"Do you know who this is?" "No, I don't. Who is this?"

"It's your granddaughter." "Really? Which one?"

## What can you do if you have been scammed?

Contact the money transfer service immediately to report the scam. If the money hasn't been picked up yet, you can retrieve it, but if it has, unlike a check that you can stop payment on—the money is gone.

Contact your local authorities or state consumer protection agency if you think you have been victimized.

File a complaint with the FBI's Internet Crime Complaint Center (www.ic3.gov), which not only forwards complaints to the appropriate agencies, but also collates and analyzes the data—looking for common threads that link complaints and help identify the culprits.

If you have questions, please contact the Massachusetts Securities Division:
800-269-5428 or 617-727-3548

Email: MSD@sec.state.ma.us

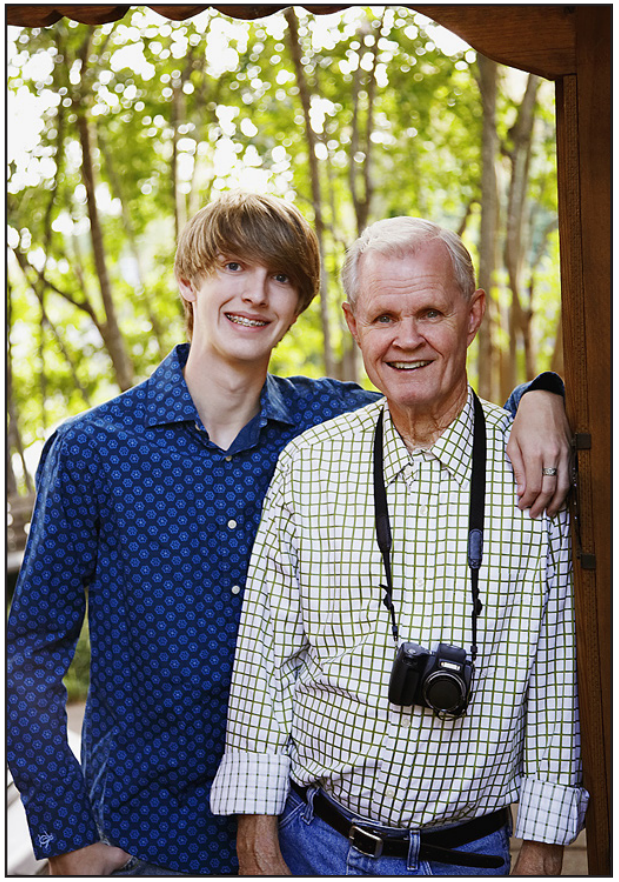
Published by:

**William Francis Galvin**
Secretary of the Commonwealth
Securities Division
One Ashburton Place, Room 1701
Boston, MA 02108
1-800-269-5428
www.sec.state.ma.us/sct

*Rev. 1/2023*

**Tips for Older Investors**

# *Protect Yourself from the "Grandparent Scam"*



**William Francis Galvin**
Secretary of the Commonwealth
Securities Division

## What is a Grandparent Scam?

It is a fraud that preys on the elderly by taking advantage of their love and concern for their grandchildren.

In the typical scenario, a grandparent receives a phone call late at night from a scam artist claiming to be one of his or her grandchildren. The phony grandchild is in a panic, saying that it's an emergency situation and he/she needs money immediately. The sense of urgency that the scam artist creates make concerned grandparents act quickly, without verifying who is calling.

While this scam has been around for years, it has become more sophisticated due to the Internet and social networking sites which allow a scam artist to uncover personal information about their targets and makes the impersonations more believable.

## Common scenarios include:

### "The Grandparents Scheme"

The grandparent scam is possibly the most widespread senior scam, where the victim receives a call supposedly from a grandchild in trouble. The "grandchild" claims to be calling from a friend's cell phone and he's gotten into a bad situation, like being arrested for drugs, getting in a car accident, or being mugged. He's out of state or in a foreign country and needs his grandparent to wire some money as soon as possible. The "grandchild" begs that his parents not be told.

### "The Fake Accident Ploy"

The scam artist gets the victim to wire or send money on the pretext that the victim's child or another relative is in the hospital and needs the money. Sometimes the scam artist will call and pretend to be an arresting police officer, a lawyer, or a doctor at a hospital. The phony grandchild may talk first and then had the phone over to an accomplice of the impersonator...to further spin the fake scenario.

### Kidnapping and Ransom

The scam artist tells the victim that his/her grandchild has been kidnapped and that the victim has to pay a ransom.

In some cases, the scam artist will have phoned the actual grandchild earlier, pretending to be from a cell phone company, with a fabricated story about why the grandchild's phone must be turned off, thus preventing the grandparent from calling the grandchild and checking the story.

## What are the Red Flags?

- Caller specifically asks the grandparent not to let other relatives know what has happened by saying "Can you please help me? I'm in jail (or in the hospital/or in some type of financial need). But don't tell Dad. He would kill me if he found out, please send the money ASAP. I'm scared."
- Caller asks that the money be sent by a money transfer company such as Money Gram or Western Union. Wire transfers allow scammers to retrieve money anywhere using a reference number and phony ID. Once the money is sent, it is gone.

## What should you do to protect yourself and avoid being victimized in the first place:

- **Resist the pressure to act quickly.**
- **Tell the caller you'll call them back at a known number, not a number that they give you.**
- **Contact your grandchild or another family member to determine whether or not the call is legitimate, and confirm the whereabouts of the grandchild.**
- **Never volunteer names or other personal information to "grandkids" that don't immediately identify themselves. Ask some questions that would be hard for an imposter to answer correctly – the name of the person's pet or the date of their mother's birthday.**
- **Develop a secret code or password with family members that can be used to verify a true emergency.**
- **Limit personal information, such as vacation plans, shared on social media sites.**
- **Never wire money based on a request made over the phone or in an e-mail... especially overseas. Wiring money is like giving cash—once you send it, you can't get it back.**