

The bond between a grandparent and grandchild is unique. Unfortunately, fraudsters may exploit this loving, trusting relationship to trick you and steal your money.

# **How Grandparent Scams Work**

Out of the blue you get an email from your granddaughter who is studying abroad. She mentions the country where she's living and says she's in distress — her credit cards, passport and phone have all been stolen and she needs you to wire money to her international bank account right away.



### **Details and Signs of a Grandparent Scam**



 Takes place via phone, email, text message or even social media.



 Typically involves the fraudster posing as your grandchild or an authority figure (like a police officer, doctor or lawyer).



 The fraudster concocts an urgent, troubling situation.



• The scammer pleads with you to keep the situation a secret.



 Personal details found online are incorporated to make the scenario seem realistic. In the unfortunate event that you fall victim to what you believe to be a scam, responding quickly can help limit the damage.

## **Action Steps**

1

If you provided financial account information, immediately contact your financial institutions and discuss cancelling fraudulent charges, obtaining a new credit/debit card or opening a new account.

2

Seek help or advice from a trusted contact, such as your Morgan Stanley Financial Advisor.



Contact local law enforcement to report the scam, or if you believe your grandchild may be in danger.



Report the incident and file a complaint with the Federal Trade Commission (FTC).



Visit IdentityTheft.gov for more information and specific actions to take based on your situation.

#### Sources:

https://www.aarp.org/money/scams-fraud/info-2019/grandparent.html

https://www.fcc.gov/watch-out-grandparent-scams

https://www.consumer.ftc.gov/blog/2021/04/dont-open-your-door-grandparent-scams

This material may provide the addresses of, or contain hyperlinks to, websites. Except to the extent to which the material refers to website material of Morgan Stanley Wealth Management, the firm has not reviewed the linked site. Equally, except to the extent to which the material refers to website material of Morgan Stanley Wealth Management, the firm takes no responsibility for, and makes no representations or warranties whatsoever as to, the data and information contained therein. Such address or hyperlink (including addresses or hyperlinks to website material of Morgan Stanley Wealth Management) is provided solely for your convenience and information and the content of the linked site does not in any way form part of this document. Accessing such website or following such link through the material or the website of the firm shall be at your own risk and we shall have no liability arising out of, or in connection with, any such referenced website. Morgan Stanley Wealth Management is a business of Morgan Stanley Smith Barney LLC.

# **Tips and Best Practices**



**DO** confirm details with others, such as your grandchild's parents or friends to verify the story you're being told. If you speak to someone who claims to be a police officer, call the relevant law enforcement agency to confirm their identity.



**DON'T** panic, no matter how dire your grandchild's situation sounds. Scam artists try their hardest to make you distraught and distract you from recognizing the scam.



**DO** say you'll call right back and then call the phone number that your grandchild usually uses. If they answer, then you will know the other call was a scam.



**DON'T** transfer money or provide financial information without confirming the identity of the receiver. Ensure the story you are hearing on the phone or reading via email is true, and call law enforcement to decide next steps.



**DO** ask questions that only your grandchild would be able to answer and that couldn't be gleaned from your social media presence.



**DON'T** volunteer any information. For example, if the scammer calls you pretending to be your grandchild, do not say their name; allow the caller to identify it.



**DO** set the privacy settings on your social media accounts so only people whom you know and approve of can access your posts. Scammers will use your social media presence to gather information to better persuade you.



**DON'T** let your guard down because the number on the caller ID looks familiar or the email is coming from the account your grandchild typically uses. Scammers may be spoofing your grandchild's phone number or may have compromised their email account.