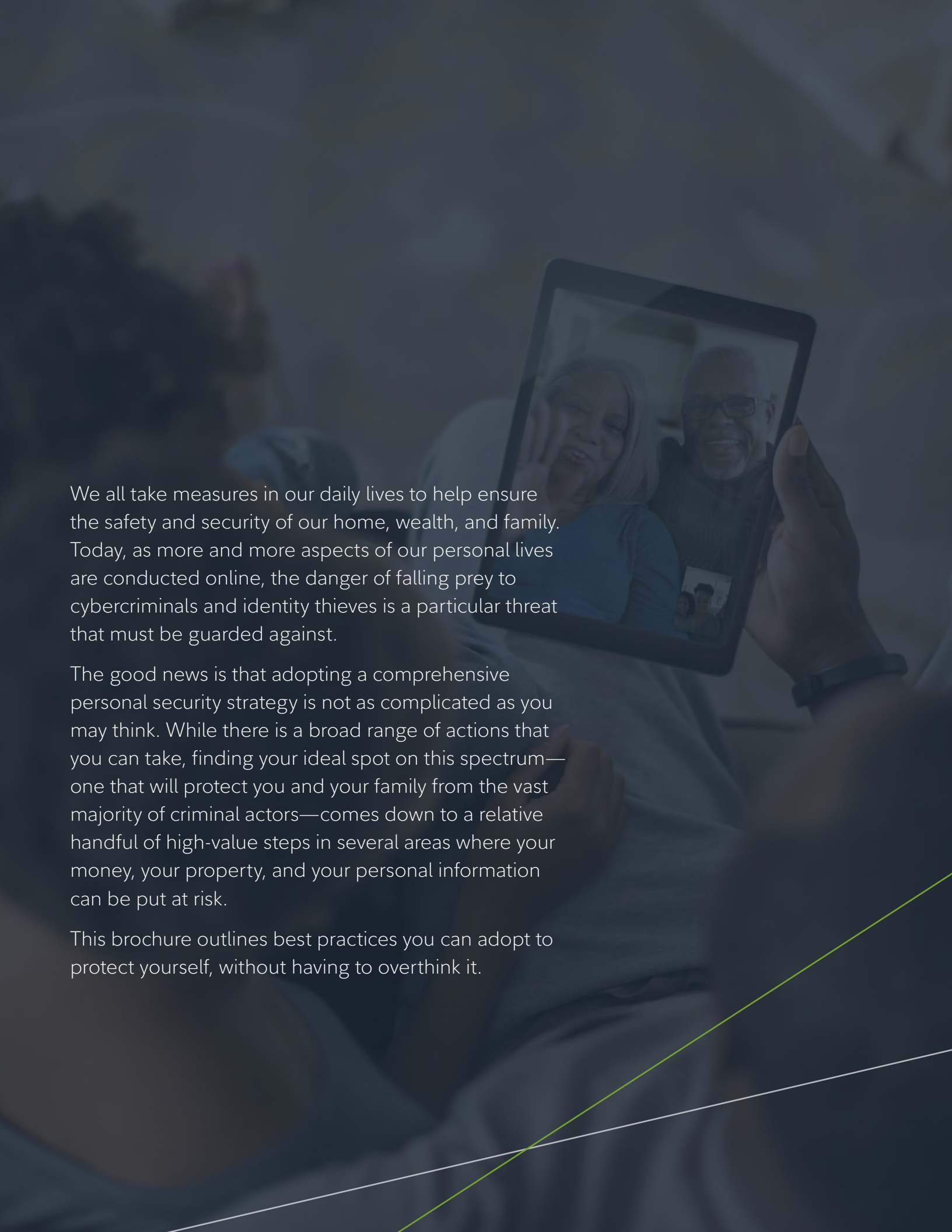
Personal Security Insights

Proven Strategies for Safeguarding Wealth & Family

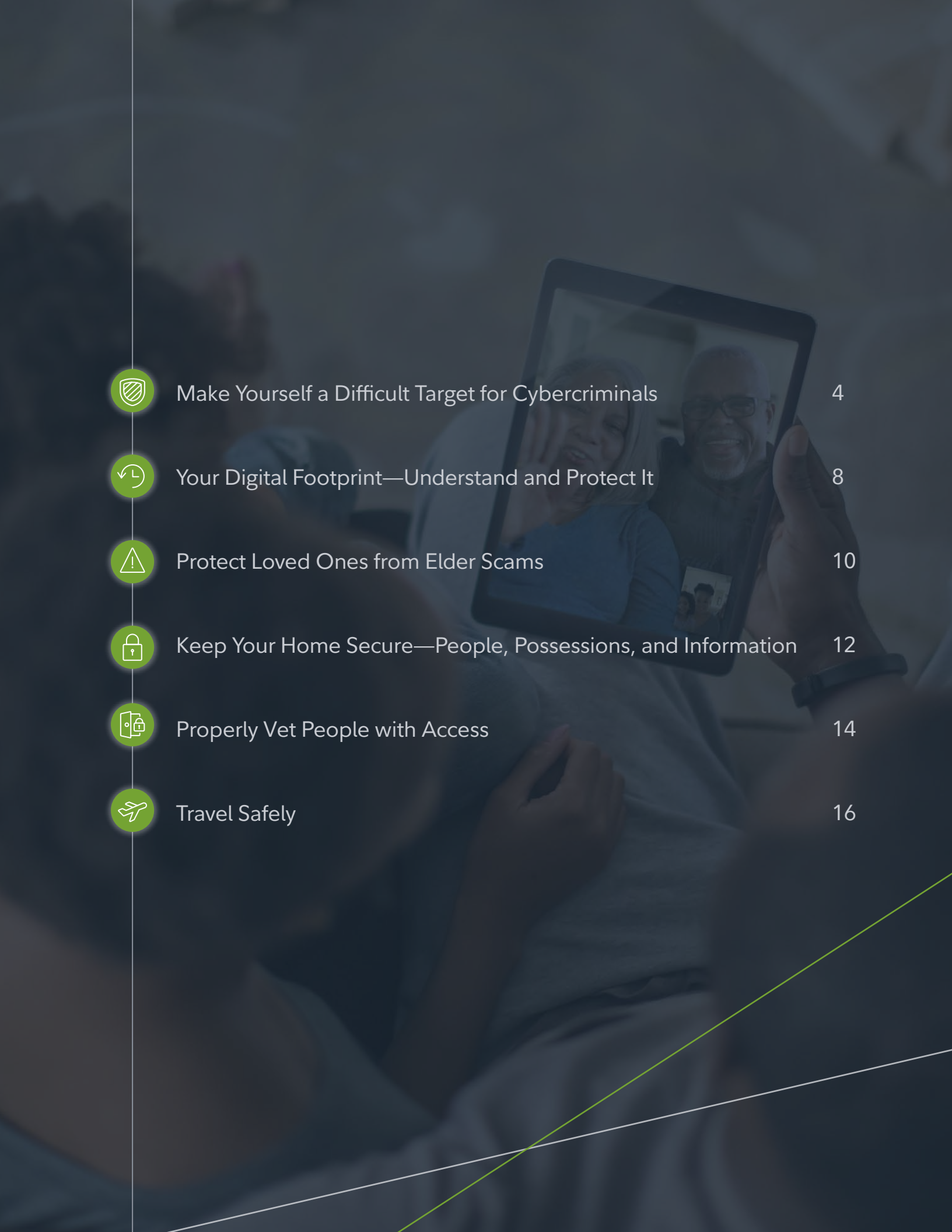
Fidelity INVESTMENTS



We all take measures in our daily lives to help ensure the safety and security of our home, wealth, and family. Today, as more and more aspects of our personal lives are conducted online, the danger of falling prey to cybercriminals and identity thieves is a particular threat that must be guarded against.

The good news is that adopting a comprehensive personal security strategy is not as complicated as you may think. While there is a broad range of actions that you can take, finding your ideal spot on this spectrum—one that will protect you and your family from the vast majority of criminal actors—comes down to a relative handful of high-value steps in several areas where your money, your property, and your personal information can be put at risk.

This brochure outlines best practices you can adopt to protect yourself, without having to overthink it.



Make Yourself a Difficult Target for Cybercriminals 4

Your Digital Footprint—Understand and Protect It 8

Protect Loved Ones from Elder Scams 10

Keep Your Home Secure—People, Possessions, and Information 12

Properly Vet People with Access 14

Travel Safely 16

Make Yourself a Difficult Target for Cybercriminals

Cybercriminals devise schemes to trick you into giving them an entry way into your digital world. They'll try to steal the log-in credentials to your financial accounts, your email, and/or your mobile phone, with the ultimate goal of moving money from your accounts to accounts they control. Taken as a group, these identity thieves are formidable adversaries: highly skilled and sophisticated, and employing time-honed techniques and technology tools to deceive you.

The most effective strategy for keeping them out is to lock down the most common entry points.

How cybercriminals operate

Most cybercriminals cast a wide net, hoping to catch enough victims from among a large group to make their efforts profitable. But in a concerning trend, a growing number also target specific individuals, quickly profiling and identifying worthwhile targets before attempting to steal their credentials, access their financial accounts, and in some cases impersonate them to open new accounts.

In both cases, the techniques are similar. The following page details how many of these scenarios play out.

Cyber Scam Scenarios: What to Watch for

In many of the cases we see, this is how cybercriminals go about trying to steal your money.

1 Step 1: Gaining Access

Cybercriminals will most often target your financial accounts because, as a famous bank robber once said, "That's where the money is." First, they need to capture your log-in credentials—your username and password. The cyberattack may come via any of several methods: you'll receive an email, text, or phone call from a fraudster pretending to be a trusted source, be it a company or person. The criminal will try to get you to provide personal information or to click on a web link that will install malicious software, or malware, on your computer or other device.

Most people have heard of these types of "phishing" schemes; some are obvious to detect, but criminals are becoming more and more cunning at getting their targets to click on a photo, or a document, or a link within an email, so constant vigilance is required.

2 Step 2: Account Takeover

Once the scammers have stolen the log-in credentials to one of your accounts, they will move quickly to take over that account. Once in, they'll oftentimes change the password to lock you out. And if you use the same username and password in multiple places, they will often exploit that too, and try to take over as many of your accounts as possible.

Also, if you know that one of your financial providers has been the victim of a corporate data breach, be sure to change the credentials for your account(s) with that provider. Otherwise, cybercriminals may try to use the stolen information to "play you" online and set up new accounts in your name. This is known as true name fraud.

3 Step 3: Moving the Money

Once the criminals have gained access and locked you out, they will look to move the money to a third-party account they control or attempt to open a new account in your name. Most often, they'll first move the money to a destination or fraud account here in the United States, and then will hop the money overseas to launder the funds.

Glossary of Common Scams

Malware/Spyware

A software program designed to damage or cause unwanted actions on a computer system, including viruses, worms, and Trojan horses. Once the malware has corrupted a device, it can install functions like "password capture" where your current username and password are recorded and made visible to the criminal when you log-in to your accounts.

Phishing

An attempt to obtain financial or other personal information from a user, typically by sending an email that appears to be from a legitimate source but contains malware.

Pharming

A type of cyberattack in which malware is installed that directs users to fake websites that look like real ones. The aim is to get the users to enter personal information on the fake sites.

Smishing

A version of phishing done by texting rather than email.

Spear phishing

A personalized, targeted form of phishing where an email appears to be from a trusted source—a close friend, financial institution, favorite charity, etc.—with an attachment or link to a site that downloads malware.

Ransomware

A type of malware that restricts access to computer systems until the target pays a ransom to the cybercriminal.

Top Tips

Here are the low-pain, high-impact strategies you can adopt to protect yourself from cyber fraud.

Strategy 1: Protect your financial accounts—employ extra layers of protection for accounts of value

- Use a strong and unique username and password
- Employ two-factor authentication (2FA) for all financial accounts and sites that store your financial information (debit card, credit card, bank account number, etc.). A 2FA is the addition of a second step (e.g., an extra, one-time password) to the log-in process; the feature is generally available, but must be enabled, on financial, social, and email accounts
- Leverage alerts on all financial accounts to warn you of suspicious activity
- Leverage voice biometrics (like Fidelity's MyVoice) that detect and verify your voice on a call
- Freeze your credit—this will make it more difficult for thieves to open new accounts in your name. Read more about how to do it at the U.S. Federal Trade Commission website (See web link below)

Strategy 2: Protect your email account(s)

- Use a strong and unique password
- Employ 2FA
- Don't keep sensitive data (like account numbers) in your email folders

Strategy 3: Protect your mobile account

- Use a strong and unique password
- Employ 2FA for online accounts whenever possible
- Manage "trusted devices" (see web link below)

Strategy 4: Protect your computer

- Keep operating system up to date (auto-update is recommended)
- Use anti-virus software and keep it up to date
- Be very cautious when clicking on email attachments or links
- If possible, use a dedicated device for financial transactions
- Be wary of Wi-Fi networks: All browsing that involves sensitive information should be on a network you trust
- Don't save passwords or credit card numbers in your web browser

Following these four strategies will make you a difficult target and protect you from the vast majority of cyber scams.

Learn more:

How to add two-factor authentication (2FA) on your Fidelity account, using Fidelity's free VIP Access: https://www.fidelity.com/security/soft-tokens/overview (1-800-FIDELITY)

Activate MyVoice verification on your Fidelity account: https://www.fidelity.com/security/fidelity-myvoice/overview

Setting up 2FA and "Trusted Devices" on Apple products: https://support.apple.com/en-us/HT204915

Adding 2FA to Samsung devices: https://account.samsung.com/membership/guide/2step/gate

Most email providers—Google, Microsoft, Yahoo, Verizon, AT&T, etc.—also offer two-factor authentication as a security option. A Web search of your provider plus "two-factor authentication" or "two-step verification" will lead you to instructions.

How to "freeze" your credit at the credit bureaus: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

Read about common scams at: fbi.gov/scams-and-safety

Your Digital Footprint—Understand and Protect It

Online personal information can invite unwanted attention—make sure you know what's "out there" about you and your family. And when it comes to sharing personal details on social media, be aware of the extent of your total household exposure, and understand that what you and your other family members put out on the internet for well-intended purposes can be used against you by criminals.

Online venue		May reveal your ...
Facebook, Twitter, Instagram, TikTok, WhatsApp, and other social media sites		Personal and family information, photos, location, travel
LinkedIn and other business networking sites		Location, professional history, personal information
Ancestry/genealogy sites		Family history, names of relatives, etc.
Professional biographies on corporate websites, or profiles related to other affiliations		Professional and personal history
Real estate records (sale records, listings, videos, photo tours)		Purchase price, tax information, photos of interior and exterior of home
Family foundations/charities		Information on your specific charitable donations, including dates and amounts

Top Tips

- **Limit disclosure.** Don't share unnecessary personal details on social media.
- **Enable security features.** Find the security settings (like two-factor authentication) on social media sites, and use them to protect your accounts.
- **Leverage privacy settings** to distinguish between accounts and posts you want to be public and ones you want to be private.
- **Don't share information as it happens.** Example: "We are boarding our flight to Europe!"
- **Get everyone on the same page.** Ensure that other family members know the risks and act accordingly—remember, a chain is only as strong as its weakest link. Decide as a family what your preferred level of privacy/discretion is, and be consistent among all family members.
- **Periodically "audit" your digital footprint.** In addition to checking yourself, consider hiring a third party to assess your online exposure; these professionals know how to look deeper and wider to see what information is available.

Don't let bad guys keep you from doing what you want to do. It's fine to use social media for communicating with friends and for professional networking. But take advantage of security settings, be selective about what information you share, and be aware of what's out there on public sites—and how it may be used by bad actors.

Learn more:

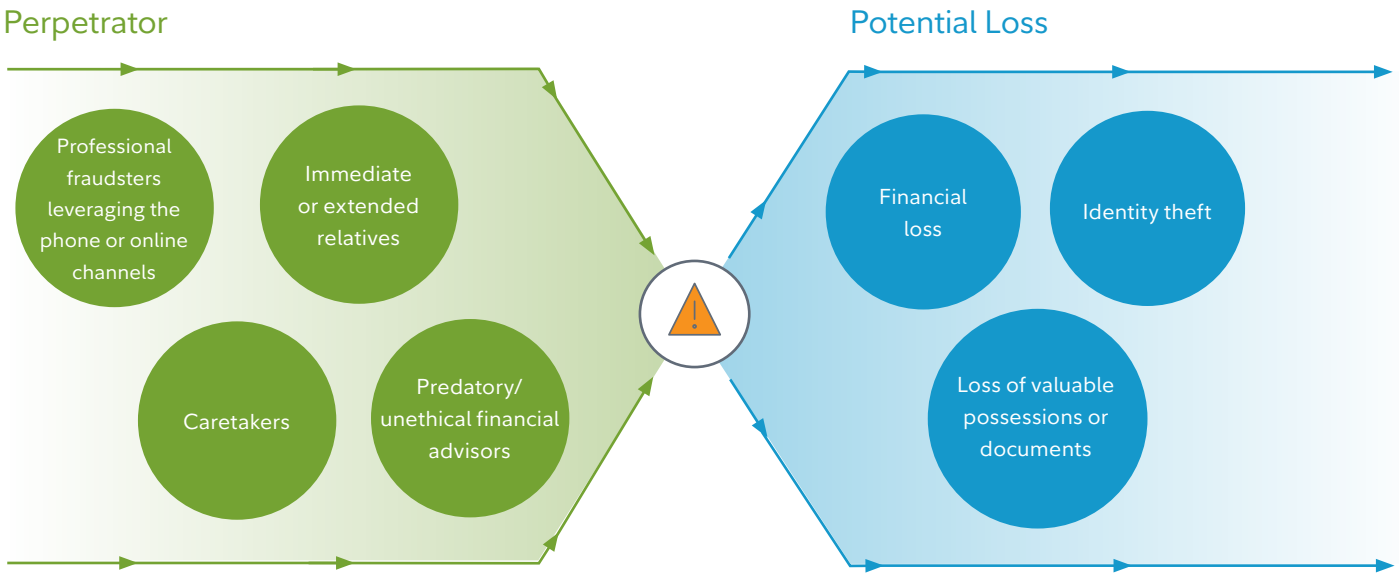
Operated by the Federal Trade Commission (FTC), this site provides tips and technical guidance on cybersecurity issues as well as a guide for talking to children about internet use: www.OnGuardOnline.gov

Parents of young children and teens may also check out: https://www.consumer.ftc.gov/topics/protecting-kids-online

Resources on a variety of cybersecurity issues, including information on adjusting privacy settings on a number of popular platforms: www.StaySafeOnline.org

Protect Loved Ones from Elder Scams

Unfortunately, one of the fastest-growing areas of fraud is the exploitation of our senior population and those with some form of diminished capacity/dementia. Perpetrators include professional fraudsters and cybercriminals but also individuals known to, and trusted by, the victim. Extra vigilance in monitoring financial accounts within this demographic is highly recommended, especially after the loss of a spouse.



Top Tips

- **Prioritize appropriately.** Whether for yourself or on behalf of your elder loved ones, make this subject a regular topic of financial and estate planning efforts.
- **Create oversight to monitor financial accounts.** At least one, or ideally two, trusted individuals should have insight into the financial activity of a senior individual or couple. Create clear accounting and transparency.
- **Know the common scams.** Sign up for AARP's Fraud Watch Network, become aware of the most common scams, and get alerts on new ones.
- **Set up alerts.** Set up automatic alerts with financial institutions that are triggered when significant transactions are requested, or when profile changes are made.
- **Act quickly.** If you are concerned about potential fraud, **seek help right away** by contacting banks, financial institutions, or credit bureaus as appropriate. (Your financial representative can connect you with a specialist in the area of elder fraud.)
- **Remain vigilant.** The World Health Organization (WHO) estimates that 15.7% of people 60 years and older are subjected to some form of abuse.[1] So stay continuously engaged and vigilant, and incorporate this topic into a broader family conversation.

Many seniors feel embarrassed or ashamed when they are scammed and have difficulty talking about it: Only one in 44 cases of financial abuse is ever reported.[2] So initiate the conversation, be empathetic, and have a strategy. It may be the most important thing you can do for your senior loved ones.

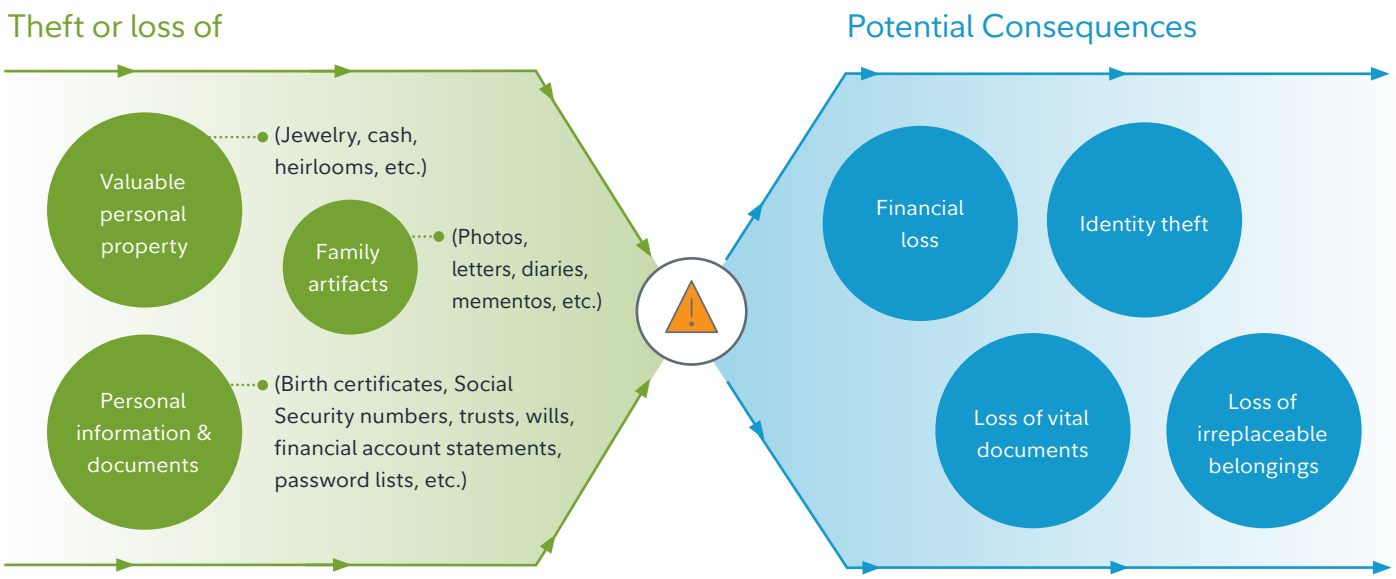
Learn more:

Information from the National Adult Protective Services Association: www.napsa-now.org.
Information from the World Health Organization: https://www.who.int/ageing/projects/elder_abuse/en/.
AARP Fraud Watch Network: https://www.aarp.org/money/scams-fraud/fraud-watch-network/.

Keep Your Home Secure—People, Possessions, and Information

While many scammers work through the online realm, other criminals still operate the old-fashioned way: for instance, by attempting to break into your home. And, of course, there are other emergencies, both natural and human-made. Most of us take common-sense measures for emergency preparedness but a systematic approach to securing your home—being ready for unplanned events, break-ins, or natural disasters, and taking steps to minimize loss—will help protect your family, your personal property, and your personal information.

Consider the consequences in the event of:



Top Tips

- **Have a plan for emergencies.** Obviously, protecting family members is a foremost concern. Do you have proper backups? Do you know what to take with you in the event of an emergency or natural disaster? Have a plan in place for events such as a break-in, fire, medical emergency, weather emergency, etc.
- **Protect personal information.** Don't leave important documents in readily accessible places in your home. Consider an online document storage service—like Fidelity's FidSafe—that allows you to store your vital information in encrypted, password-protected files.
- **Secure your home network.** Backup data on your devices regularly, and use a strong, unique password and two-factor authentication (2FA) to protect your router from being hacked.
- **Be aware of the "Internet of Things."** Many consumer products—from thermostats to coffee machines—are now Web-enabled. These products can provide thieves a back way into your home network (for example, if you use a common password for multiple products and devices).
- **Control physical access.** Keep careful track of who has keys to your house, and if you have an alarm system, everyone in the house should know how to use it.
- **Call for help as needed.** Get to know your local police and emergency personnel and don't hesitate to contact them. They are there to help and are trained and experienced to handle emergency situations, large or small.

The wave of technology products available now tends to favor convenience over security. As with social media, the idea is not to avoid these products but rather to be aware of potential vulnerabilities and take necessary precautions. **Convenience has a place in our lives—just make sure you understand the pros and cons ... and the risks.**

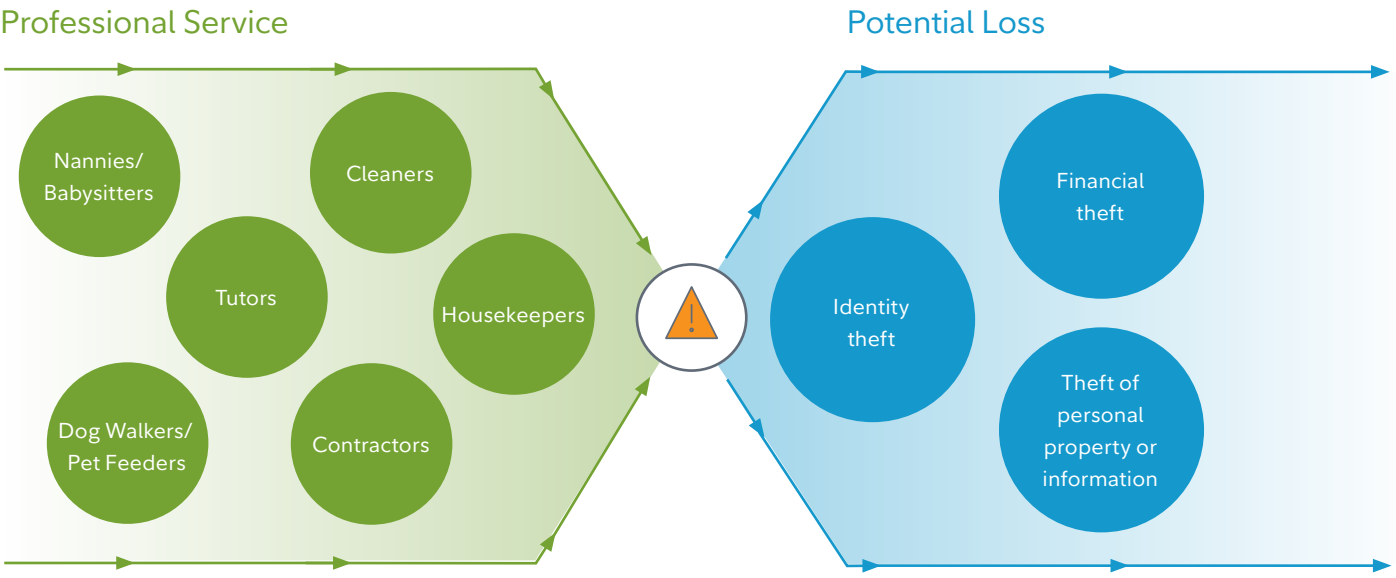
If you think you need help, consider a professional "all hazards" risk assessment. Similar to a comprehensive home inspection, the finished product should provide a roadmap, with action steps, to reduce risk.

Learn more:

Storing critical documents in a secure digital repository: www.fidsafe.com.
Emergency preparedness for home and family: www.fema.gov.

Properly Vet People with Access

Millions of Americans employ professional service providers to help with household tasks. Many develop close and long-term relationships with these individuals. But anyone with the keys to your home has potential access to your possessions and/or personal information, so you should carefully vet these providers prior to hiring.



Top Tips

- **Do basic research.** A simple online search will often highlight obvious areas of concern.
- **Don't rely on third parties.** Many service providers work through agencies or employers. Sometimes these third parties conduct proper background checks; sometimes they don't. Don't automatically assume they will.
- **Consider a professional background check.** With the individual's consent, online providers can perform criminal checks.
- **Consider monitoring and key management.** Use separate alarm codes for household helpers/contractors, keep careful track of keys, and consider basic camera surveillance in your home.

The most important thing to remember is that it's perfectly reasonable to carefully vet individuals who will have access to your home. So don't feel awkward or uncomfortable about it. The vast majority of prospective employees will accept it as a condition of employment.

Learn more:

Choosing a vendor for background checks or internet analysis: https://thepbsa.org/.

Travel Safely

You put a lot of time and effort into planning a great family vacation, but don't forget to take the appropriate measures to keep you and/or your loved ones safe.

If you are journeying abroad, being prepared for issues that may arise can be the difference between safe and smooth sailing and an unpleasant travel experience.

Areas to consider include:

Unplanned events/ medical safety	• Register with the U.S. Department of State—or your home country's embassy, if possible—before traveling abroad • Ensure health coverage while abroad • Know where to go in the event of an emergency
Financial safety	• Notify credit card companies and banks of travel plans • Have phone number of financial institutions if needed
Communication safety	• Ensure you have a working cell phone with you at all times
Document safety	• Carry backup copies of vital documents
Home safety	• Stop mail delivery • Don't post real-time travel photos on social media

8 Safety Tips to Help You Travel Smart

Travel can be a memorable experience to share with family and friends. But there are some important things to consider when planning any trip—especially when traveling to an international destination. The following tips fill in the blanks on what you need to do to ensure a *bon voyage*.

1. Register your international trip with the U.S. Department of State—or your home country's embassy, if possible—and perform basic research.

U.S. citizens can register at the State Department's Smart Traveler Enrollment Program (STEP). Also, check the State Department's website for information regarding your international travel destination before you leave. Understand the following for all areas visited: hospitals near you, known crime areas, planned major events/protests, etc.

2. Obtain dedicated travel medical insurance to cover you and your family abroad.

Check with your health insurance provider to understand your coverage abroad and find out what your policy will and will not cover. Oftentimes, there are gaps in coverage and the best step is to consider purchasing dedicated travel medical insurance. Particularly, to assist in events requiring emergency medical treatment and evacuation, it's prudent to hire a provider specifically skilled in this area.

3. Activate international calling on your cell phone.

When traveling internationally, verify that your phone will work in the country you are visiting and activate the appropriate international service with your provider or rent a phone as needed. When you arrive, make a test call to ensure the phone is working. Don't forget to pack a charger that will work where you're going.

4. Program emergency numbers into your phone.

Ensure that your phone has contact information for your local embassy, health insurance provider, credit card company, and for the people you're traveling with. All travelers in the group should leverage geo-location services on their mobile phones (e.g., "Find your phone" functionality or family safety applications), so in the event of an emergency individuals may be located or contacted quickly.

5. Receive all recommended vaccines.

Before your trip, plan to meet with your health care provider, who can suggest what steps to take to help protect yourself against potential health risks. Schedule appointments in advance to allow for multiple doses, if necessary.

6. Notify your personal credit card provider of your international travel plans.

Many credit card companies will suspect fraud and put a freeze on your account if they see charges from a foreign country.

7. Be prepared if your passport and/or travel documents are lost or stolen.

Photocopy or scan your passport and carry a copy with you. Also, carry a printed copy of your travel itinerary and electronic ticket receipts. Consider leveraging secure online storage solutions like Fidelity's free FidSafe for access to important documents as needed while away.

8. Protect your home while you're away.

Take the necessary steps to avoid tipping off thieves. Before you leave, either have a trusted party retrieve your mail or contact the postal service to stop delivery. Avoid posting your travel plans on social media, and don't tag your location while on your trip.

Remember to secure cash, credit cards, and other valuables

- Petty crime (such as pickpocketing and bag snatching) is the primary risk to travelers globally. Always remain vigilant in public spaces and crowded areas.
- Try not to carry large amounts of cash.
- If you can, avoid using ATMs on the street and use one inside a bank or hotel. Set up alerts to monitor transactions at all your financial institutions.
- Never leave belongings unattended. Keep valuables in your carry-on luggage (not checked baggage) during the flight.
- Keep passports, travel documents, and valuables in your hotel safe when you don't need them. Unless the country requires you to carry your actual passport, carry a copy of the photo page for ID purposes. Retain copies of all important documents in a secure and accessible online repository like Fidelity's free FidSafe.
- Take any necessary medications with you in their original containers and keep them in your carry-on luggage during the flight.

Learn more:

Register with the Smart Traveler Enrollment Program, a service of the U.S. Department of State: https://step.state.gov/step/
Research your destination at the U.S. Department of State: https://travel.state.gov/content/travel.html
Storing critical documents in a secure digital repository: www.fidsafe.com

Further Resources:

If you believe your identity has been stolen, go immediately to: www.identitytheft.gov

Fidelity Security Overview: https://www.fidelity.com/security/overview

Fidelity Customer Protection Guarantee: https://www.fidelity.com/security/customer-protection-guarantee

How to add alerts on your Fidelity account: http://www.fidelity.com/security/monitor-your-accounts

How to add voice biometrics on your Fidelity account: https://www.fidelity.com/security/fidelity-myvoice/overview

1-800-FIDELITY

Authors

Gary F. Rossi

Vice President, Fidelity Security Services

Gary Rossi has more than 30 years of experience as a private sector and law enforcement security professional with deep expertise in investigations, cyber fraud, risk mitigation, and strategic planning. Gary joined Fidelity Investments in 2003 and served as Fidelity's Head of Corporate Investigations for nearly a decade, leading all customer fraud/identity theft matters, anti–money laundering cases, and cyber-related investigations. Gary and his team created a comprehensive anti-fraud program to protect Fidelity's customers from sophisticated cyber criminals. Gary now leads the Fidelity Security Services group, working directly with many clients to assist them in better understanding current security threats and with building appropriate mitigation strategies.

Prior to Fidelity, Gary served for 14 years as a special agent for the Federal Bureau of Investigation (FBI). He specialized in a wide variety of white-collar crime investigations, which included sophisticated financial frauds, cybercrimes, and public corruption matters. Gary functioned as the Chief of the FBI's Undercover and Sensitive Operations unit at FBI Headquarters in Washington, DC. This unit was responsible for overseeing many of the FBI's most sensitive and complex cases. Prior to the FBI, Gary worked as a CPA for Arthur Andersen & Co., and as a consultant for the cybersecurity consulting firm @Stake (now Symantec). Gary holds a degree in accountancy and management from Bentley University.

Jon Dougherty

Managing Director, Personal Security Education Program

A Fidelity veteran of 25 years, Jon has worked in a variety of roles within the Global Risk and Security functions. He currently serves as managing director for Fidelity's Personal Security Education Program, focusing on educating customers on a broad range of security threats and assisting them in developing effective mitigation strategies.

Prior to his current role, Jon served as vice president of Risk Technology within Corporate Security, where he was responsible for the firm's Global Security Operations Center, Fidelity's 24/7/365 life safety, alert monitoring, and crisis management center. In addition, he led the enterprise physical security system engineering, architecture, software development, and infrastructure support functions across the Global Enterprise portfolio.

Before that, Jon was a member of the Corporate Investigations division, where he served as the program manager for Fidelity's primary financial fraud detection system.

Jon received his bachelor's degree from Westfield State University and is a certified fraud examiner, as well as an active member of a variety of security industry forums.

Fidelity INVESTMENTS

Views unless otherwise noted are as of Sept. 21, 2020.

Endnotes

[1] World Health Organization news release, June 14, 2017. https://www.who.int/en/news-room/detail/14-06-2017-abuse-of-older-people-on-the-rise-1-in-6-affected

[2] National Adult Protective Services Association, as of May 2020.

Information provided in this document is for informational and educational purposes only. To the extent any investment information in this material is deemed to be a recommendation, it is not meant to be impartial investment advice or advice in a fiduciary capacity and is not intended to be used as a primary basis for you or your client's investment decisions. Fidelity, and its representatives may have a conflict of interest in the products or services mentioned in this material because they have a financial interest in, and receive compensation, directly or indirectly, in connection with the management, distribution and/or servicing of these products or services including Fidelity funds, certain third-party funds and products, and certain investment services.

Information presented herein is for discussion and illustrative purposes only and is not a recommendation or an offer or solicitation to buy or sell any securities. Views expressed are as of the date indicated, based on the information available at that time, and may change based on market and other conditions. Unless otherwise noted, the opinions provided are those of the author and not necessarily those of Fidelity Investments or its affiliates. Fidelity does not assume any duty to update any of the information.

Third-party marks are the property of their respective owners; all other marks are the property of FMR LLC.

Fidelity Institutional℠ provides investment products through Fidelity Distributors Company LLC; clearing, custody, or other brokerage services through National Financial Services LLC or Fidelity Brokerage Services LLC (Members NYSE, SIPC); and institutional advisory services through Fidelity Institutional Wealth Adviser LLC.

Personal and workplace investment products are provided by Fidelity Brokerage Services LLC, Member NYSE, SIPC.

Institutional asset management is provided by FIAM LLC and Fidelity Institutional Asset Management Trust Company.

© 2020 FMR LLC. All rights reserved.

941922.1.0

1.9878766.104