Fight Telephone Fraud:

How To Identify, Prevent, and Report Phone Scams

"I added my phone number to the Do Not Call Registry so this incoming call from the IRS must be legit... right?"

Wrong.

While there are many legitimate calls, there are also many from criminals who commit fraud by phone. Through devious tricks and schemes, they not only steal your money but also your valuable personal information.

What Can Telephone Fraudsters Do?

Once your personal information is in their hands, identity thieves can:

- Apply for credit cards and car loans
- Submit for a mortgage
- Steal your healthcare benefits
- Takeover your email accounts
- Steal your tax refund
- Make posts on social media
- Contact your friends and family
- Share (or sell!) your information to other scammers

While financial institutions will often help you sort out what happened, victims of telephone fraud often have to spend enormous amounts of time, energy, and money trying to get their life back in order after falling prey to one of these schemes. It's better to strive for prevention or know how to identify the signs early.

How Pervasive Is Telephone Fraud in America?

- According to the <u>Truecaller Insights 2022 U.S. Spam and Scam Report</u>: In 2022, 26% of Americans (68.4 million people) lost money due to phone scams – up 23% (59.4 million) in 2021.
- 1 in 3 Americans (33%) have fallen victim to phone scams at some point in their lives, with 20% of Americans defrauded more than once.
- Enough money was stolen by phone scammers in 2021 (\$39.5 billion USD) that you could give every person in California \$1,000.

"It Won't Happen To Me."

Many believe phone scams target the elderly and that a "younger" person would never fall for one. In reality, Americans between the ages of 18 and 44 are the most common victims of phone scams, with men targeted more than women.

How To Identify Telephone Fraud

• While clever criminals are continually evolving their strategies to keep stealing, here are a few common scams to look out for:

Free gifts, cash prizes, rewards, travel and vacations: If it sounds too good to be true, it probably is — especially if you need to give them your credit card to pay the shipping and handling or some other modest fee first.

- **Charities and fundraisers**: Tactics include thanking you for a donation you don't recall giving or pressuring you to give right now. Be especially wary of organizations that call around the holidays or after a natural disaster and ask you to donate in cash, gift card, virtual currency, or wire transfer.
- **Family emergency scams:** Someone impersonates a family member or pleads that a family member is in trouble and money needs to be sent immediately. Often they'll involve an authority figure like a lawyer, police officer, the IRS, or a doctor to make the request sound more urgent. Sophisticated scam artists are even using <u>voice cloning technology</u> to impersonate loved ones.
- Imposter scams: The caller allegedly from a government agency, a utility company, PayPal, Apple, a shipping carrier, or a bank —says there is a problem with your account, your payment is late, or you owe back taxes. Whatever the issue, if you provide details like your social security information and your bank account number, they say it can be easily fixed.
- **One ring scams:** For illegal robocallers, the goal isn't always getting you to answer. Sometimes, it's getting you to call them back. The **Federal Trade Commission** advises that you never return or answer calls from numbers you don't recognize, even if they look like they are coming from a U.S. area code. You may end up connecting to an international call or adult hotline, prompting charges on your bill for which the scammer receives commission payments.
- **Banking scams**: According to <u>*Kiplinger*</u>, there's been a surge in scams targeting savings and checking accounts, especially during the holiday shopping seasons. The easiest way to become a victim of a scam is to share your personal info. Never give out account numbers, PIN codes, social security numbers, addresses, to someone or a company you don't know and trust.

How To Prevent Phone Scams

- Add your phone number on the FTC's <u>National Do Not Call Registry</u>. It won't stop spam calls, but it will make them easier to spot, as it stops telemarketing calls from legitimate companies.
- **Don't answer calls from unknown numbers.** Once you answer, you may be charged or deemed an "active number" worthy of future calls. If you pick up and realize it's a robocaller or scam, hang up immediately.

- **Don't give personal or financial data to callers you don't know**. Personal information includes your Social Security number, date of birth, pin numbers, or credit card account numbers.
- Slow down and ask questions of telemarketers. Legitimate businesses and charities will answer questions and give you time to consider a purchase or donation. Scam callers will pressure you to commit right away.
- Hang up and call the company directly. The scammer will fight, but if there is a legitimate issue from the company, any customer service rep will be able to address it from a general call center.
- Don't return one-ring calls from unknown numbers. These may be scams to get you to call hotlines in African and Caribbean countries that have U.S.-style three-digit area codes, and you could incur hefty connection and per-minute fees.
- **Don't follow instructions on a prerecorded message.** If you "Press 1" to speak to a live operator, it will probably lead to a phishing expedition. Or if you press any key to get taken off a call list, it will probably lead to more robocalls.
- **Don't pay registration or shipping charges to get a supposed free product or prize.** Such fees are ploys to get your payment information.
- **Don't make payments by <u>gift card</u>**, **prepaid debit card or wire transfer.** Fraudsters favor these methods because they are hard to trace.

How To Report Telephone Fraud

- If you encounter a suspected phone scam or an abusive telemarketer, file a complaint with the Federal Trade Commission <u>online</u> or at <u>877-382-4357</u>, and notify your <u>state consumer protection</u> <u>office</u>.
- Report caller-ID spoofing to the Federal Communications Commission <u>online</u> or at <u>888-225-5322</u>. The FCC also provides <u>consumer guides</u> to numerous phone scams and improper practices.
- Visit the Do Not Call Registry <u>website</u> or call <u>888-382-1222</u> to register your number or report illegal robocalls.

Wealthcare Advisory Partners LLC (Wealthcare) is an investment advisors registered with the SEC under the Investment Advisors Act of 1940. Additional Important Disclosures may be found in the Wealthcare Advisory Partners LLC ADV Part 2A. Request a copy at <u>compliance@wealthcarecapital.com</u>

This communication is for informational purposes only and is not to be considered advice or a recommendation of any specific investment product or strategy. Views and opinions are subject to change at any time based on market and other conditions.

©2023 Wealthcare Advisory Partners LLC. All Rights Reserved.