

### FLORIDA CONSUMER J NEWSLETTER

**July 2024** 

A publication of the Florida Department of Agriculture and Consumer Services

### **SPOTTING SCAMS**

In 2023, about 332,000 people reported a business impersonation scam, far more than any other fraud type, and reported losses totaled over \$660 million. Government agencies, like the IRS, the Federal Trade Commission (FTC), or even local law enforcement agencies, are often impersonated as well. But the available data is not inclusive of all fraud because the vast majority of frauds are not reported, so these figures reflect just a small fraction of the public harm.

Scammers are all about spinning lies, but they operate in the real world. The data shows that many scammers are successful at pretending to be well-known businesses or government agencies to gain trust and make their stories seem more believable. And scammers use real-world methods to contact people and to get paid. Reports to the FTC's Consumer Sentinel Network point to some of their favorite methods.

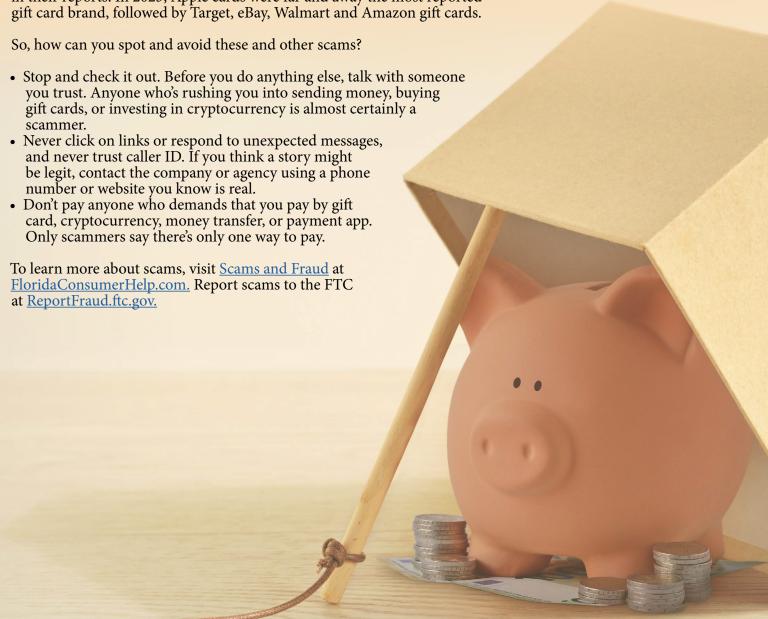
According to 2023 reports, the most-impersonated companies include Best Buy's Geek Squad, Amazon, and PayPal. But reported losses tell a different story: losses were highest when scammers impersonated Microsoft and Publishers Clearing House. The scammers impersonating these businesses work in very different ways. For example, phony Geek Squad emails tell you that a computer service you never signed up for is about to renew - to the tune of several hundred dollars. Microsoft impersonation scams start with a fake security pop-up warning on your computer with a number to call for "help." And calls from the fake Publishers Clearing House say you'll have to pay fees to collect your (fake) sweepstakes winnings.



Reports about all types of fraud also tell how scammers contact their targets. Last year, people shared that scammers were most often reaching out by email and phone calls. But people also told us that they lost the most money on scams that started on social media. As a matter of fact, more money was reported lost to fraud starting on social media than any other contact method in 2021, 2022, and 2023. In 2023, 51% of reports about fraud starting on social media identified Facebook as the social media platform, and 22% identified Instagram. These reports most often involved online shopping scams that started with ads on social media. However, the largest reported losses to scams starting on social media platforms were to investment scams.

How scammers get their money varies by the type of scam, too. For example, people who report investment scams most often say they "invested" with cryptocurrency or via bank transfer. Reported payments to scammers by these two methods added up to the highest losses in 2023, both per person and in total. And many people reported using payment apps and services, most often in connection with online shopping scams.[9] Most people who reported using a payment app or service named the company they used, with PayPal, Cash App, Zelle, Venmo, and Apple Pay most often reported in 2023.

Gift cards were the top reported payment method on several types of scams in 2023, including romance scams, tech support scams, government impersonation scams, and scams that impersonate people you know, like your boss or a grandchild. Reports show that scammers specify what gift card brand to buy, which most people named in their reports. In 2023, Apple cards were far and away the most reported gift card brand, followed by Target, eBay, Walmart and Amazon gift cards.



# IGNORE TEXT MESSAGES FROM STRANGERS

By Gema de las Heras, Consumer Education Specialist, FTC

A text message from an unknown number that simply says: hi, how are you? seems harmless. Your first instinct might be to respond to see if it's someone you know. Or maybe tell them they made a mistake. But it's best to ignore these type of text messages. Scammers are using this tactic as a conversation starter, so don't text back. If you do, here's what happens next.

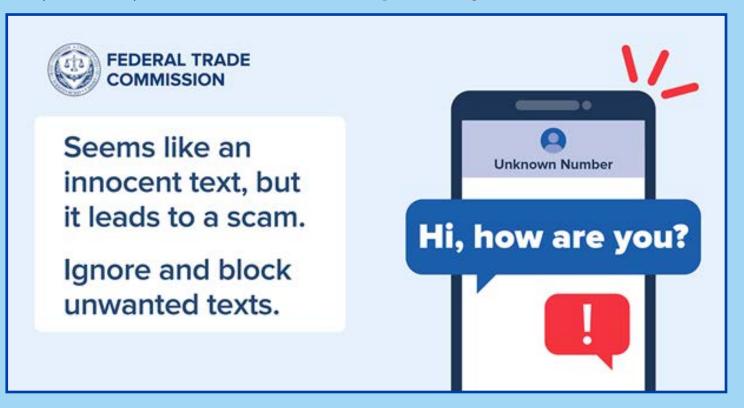
The person (a scammer) on the other end of the text will probably apologize...and find a way to keep the conversation going to be friend you. Then, once they have your trust, they'll try to offer you advice on investing in cryptocurrency or claim they can teach you the secrets to making big money in the crypto markets. For a fee, of course. But it's all a scam and they'll just steal your money.

Even if you just reply to the text but don't engage in conversation, you've still confirmed they reached a working telephone number. Which could lead to more calls and texts from scammers.

What's the best way to avoid scams if you're getting messages from numbers you don't recognize?

- Don't reply to text messages from unknown numbers. It could lead to a scam. Delete and report them using your phone's "report junk" option or forwarding unwanted texts to <a href="7726">7726 (SPAM)</a> and unwanted emails to your email provider.
- Never click links in an unexpected message. Some links might steal your information, or install <u>malware</u> that gives scammers access to your device.
- Don't trust anyone who says you can quickly and easily make money. Every investment has risks. Only scammers guarantee you'll make lots of money in a short time with zero risk.

Have you lost money to a scam like this? Tell the FTC at ReportFraud.ftc.gov.



#### FINDING ROMANCE ONLINE

By Cristina Miranda, Consumer Education Specialist, FTC

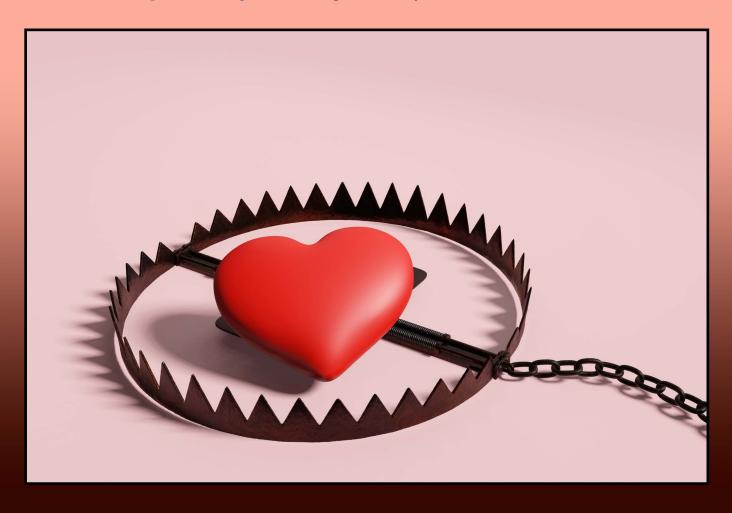
If you meet someone on social media or a dating website or app, how can you tell if their profile is real? They say they're in the military — but scammers especially like to pose as military servicemembers stationed overseas. What's the best way to spot a fake?

The short answer is this: if your online friend asks for money, for any reason, they're a scammer. Everything about their posts and profile is designed to seem real. These scammers often steal real military servicemembers' names and photos for their fake profiles. Their online chats can feel real and quickly turn to talk of love or even marriage. But they have reasons they can't meet in person or on video. And the story ends with needing your "help" (= money) urgently. Which, you know, means this is a scammer.

Spot these signs of a <u>scammer</u> posing as a military servicemember:

- Their photo is in several profiles in different platforms. Check out who you're talking to. Do a reverse image search of the profile picture. Search the name online with the words "scam" and "imposter" to see what comes up. If the details don't line up, it's a scam.
- They ask you for money. As soon as an online love interest asks for money, the scam bell rings. And if they ask for money through <u>gift cards</u>, a <u>wire transfer</u>, <u>payment apps</u> like Apple Pay, CashApp, PayPal, and Zelle, or <u>cryptocurrency</u>, all the scam bells ring.

If you think someone is a scammer, cut off contact. Tell the social media platform, dating website or app, and then tell the FTC at ReportFraud.ftc.gov. Share this post to alert your friends and followers to this scam.



### FOOD FRAUD AND PRODUCT PACKAGING

Food fraud takes several different forms but is generally defined as the deliberate and intentional substitution, addition, tampering, or misrepresentation of food ingredients or packaging. FDACS inspectors are responsible for checking the packaging and net contents of food products to assure that consumers are getting the full measure of the product they pay for. The department has adopted national standards established by the National Institute of Standards and Technology to insure consistency and accuracy in measurements.

Information on package labeling must be displayed plainly and clearly, and the lettering color must conspicuously contrast with the background color. The required information falls into the following three categories:

1. Identity of the commodity in the package. The product identity must appear on the principal display panel of the package and must be the name required by federal or state regulation or the common or usual name or the generic name or other appropriate description including a statement of function.

2. The name and place of the business that will be responsible for the product and the package. If the responsible party is not the manufacturer, then the label should reveal the responsible party's connection to the package,

i.e. "Manufactured for and packed by," or "Distributed by."

3. How much of the product is in the package in terms of weight, measure or count. This must appear on the principal display panel of the product package. Net contents must be declared in the largest whole unit, properly rounded to overstate the quantity, contain only decimal fractions, and expressed in terms of weight, measure, volume, or count. Statements about net contents may not include "when packed," "minimum," "not less than," etc.

Proper packaging and consumer awareness can play a major role in fighting food fraud. Consumers can reach the Consumer Assistance Center Monday through Friday from 8:00 am to 5:00 p, ET, at 1-800-HELP-FLA (435-7352) or, for Spanish speakers, 1-800-FL-AYUDA (352-9832). Visit FloridaConsumerHelp.com to file a complaint, find information on scams, or check out the A to Z Resource Guide.



# CONSUMER PROTECTION SPEAKER REQUEST

Does your organization need a guest speaker for an event or meeting? An educated consumer is the best protection against fraud and deception, so let a member of our consumer outreach team share the latest information about scams and fraud with your group.

Visit our <u>Consumer Protection Speaker Request</u> page for more information and to request that a consumer protection representative present at your next virtual or in-person meeting. You may also contact our consumer assistance team at 1-800-HELP-FLA (1-800-435-7352), 1-800-FL-AYUDA (1-800-352-9832) en Español, or by sending correspondence to: Consumer Services Outreach, Florida Department of Agriculture and Consumer Services, 2005 Apalachee Parkway, Tallahassee, FL 32399.

Information submitted to the department is a public record unless exempted by Florida law.



# ABOUT THE FDACS DIVISION OF CONSUMER SERVICES

FDACS is Florida's state consumer protection agency responsible for regulating charities and handling consumer complaints. FDACS handles more than 400,000 consumer complaints and inquiries, oversees more than 500,000 regulated devices, entities, and products like gas pumps and grocery scales, performs over 61,000 lab analyses on products like gasoline and brake fluid, performs nearly 9,000 fair ride inspections, and returned over \$2.8 million to consumers through mediations with businesses.





The Division of Food Safety monitors food from the point of manufacturing and distribution through wholesale and retail sales to ensure the public of safe, wholesome and properly represented food products.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.



The Consumer Product Safety Commission provides consumer product recall information as part of the agency's mission to protect consumers and families from hazardous products.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection and information. Consumers who would like information about filing a complaint against a business or who believe fraud has taken place can visit us online at <u>FloridaConsumerHelp.com</u> or contact the department's consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) for Spanish speakers.