FLORIDA CONSUMER
# NEWSLETTER
September 2026

A publication of the Florida Department of Agriculture and Consumer Services

# BE STORM READY – BUILD A DISASTER SUPPLY BUCKET

When a catastrophic storm is bearing down on you and your family, it is too late to wonder, "What do we need?" Assemble these essential items in a durable waterproof five-gallon bucket to keep at the ready your home or vehicle.

- Photos of family members and
- pets
- Pocket knife
- Portable phone charger
- Ponchos
- Rope/paracord
- Soap
- Special family needs (diapers,
- feminine hygiene items, etc.)
- Tarp
- Toilet paper
- Toothbrush
- Towel
- Water
- Waterproof bag with family
- documents, including driver's
- license, insurance information,
- out-of-area contact, medical
- Information
- Whistle
- Batteries
- Hand crank emergency radio
- Blanket
- Manual can opener
- Cash
- Change of clothing
- Duct tape
- Dust masks for each person
- First aid kit
- Flashlight
- Games and toys
- Gloves
- Hand sanitizer
- Keys (home and car)
- Large plastic trash bags
- Local map
- Medications
- Non-perishable food
- Permanent marker
- Pet supplies

# CONSUMER ALERT: BE CAUTIOUS WHEN HIRING FREELANCERS ONLINE

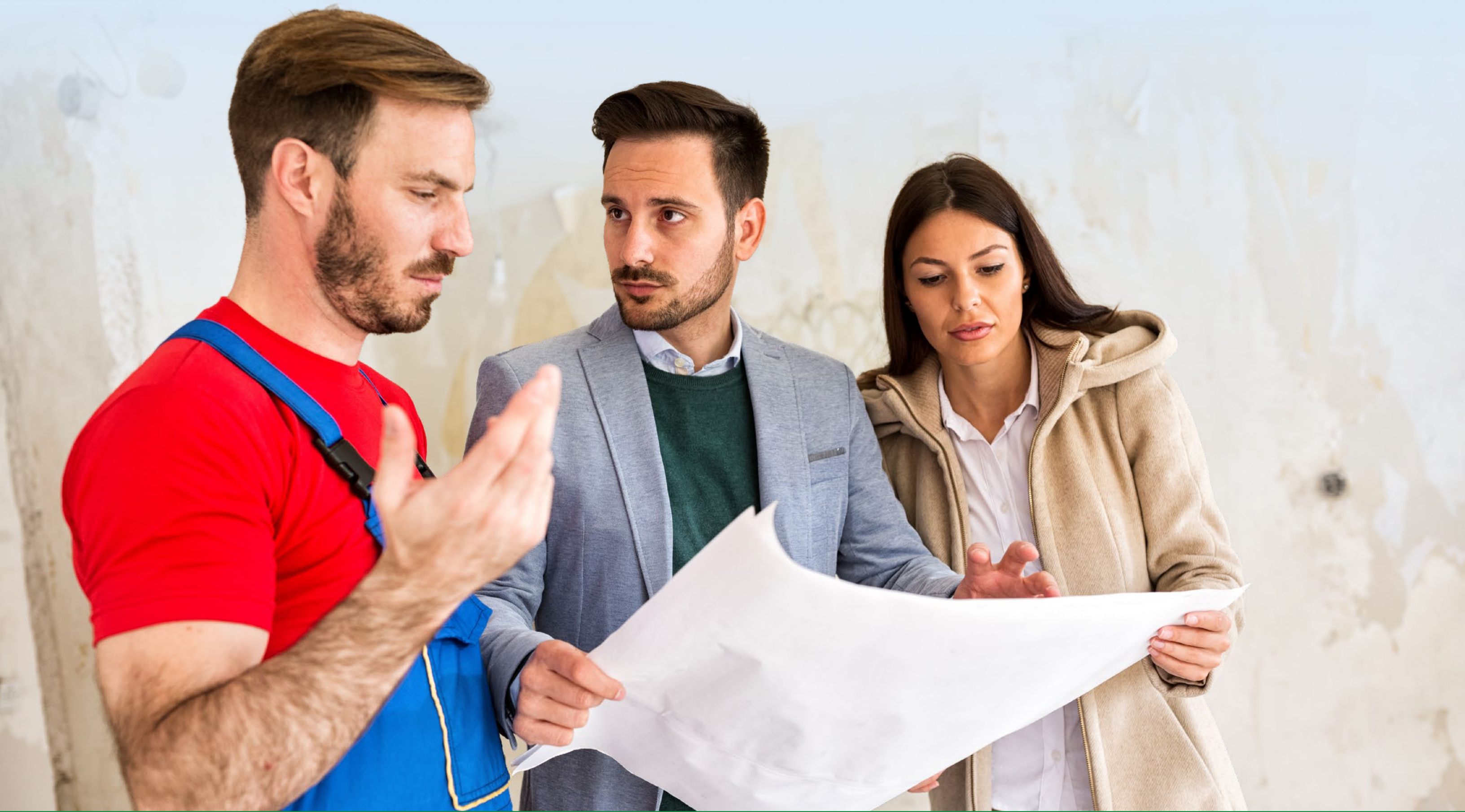
The Florida Board of Professional Surveyors and Mappers is warning consumers to be careful when using freelancing websites such as Upwork, Fiverr, and Freelancer to hire professional surveying services. These popular platforms allow anyone to advertise their services but may not verify if they are properly licensed.
In some cases, bad actors have falsely claimed to be licensed, fraudulently used professional seals and signatures to appear legitimate, and then delivered substandard work. When an unlicensed person uses someone else's professional seal, it becomes nearly impossible for homeowners, contractors, or local officials to verify who performed the work or whether it meets accepted standards.

As more people turn to online platforms to hire professional services, scammers are taking advantage of the ease and anonymity to defraud. Consumers are encouraged to always do their research before paying for services and verify licenses and credentials to make sure they are hiring a professional.
Hiring an unlicensed person to perform a survey on your property puts you and your property at risk. Inaccurate surveys can lead to costly construction errors, unsafe conditions, violations of local permitting requirements, and potential civil liability.

Licensure exists to protect the public, and that protection breaks down when someone misuses another professional's seal. A professional license ensures that national and state minimum competency standards have been met. Before you hire someone you found online to survey a property, take a few minutes to verify if they are licensed. Verification is free, it's easy, and it could save you from a costly or dangerous mistake.

Verify a person's license through the License Lookup tool and contact them directly at a verified number or email address

If you believe you have been misled by someone advertising or performing licensed survey services, or if you suspect that someone is misusing a professional seal, report it to the Florida Department of Agriculture and Consumer Services.



# COULD SOMEONE REALLY BUY THE ROMAN EMPIRE?

Imagine being told that the Roman Empire was for sale. Not a piece of land or a palace, but the whole empire. Even though it sounds like the beginning of an obvious scam, in 193 CE, one wealthy Roman senator decided the offer was real and that he was willing to pay handsomely for it.

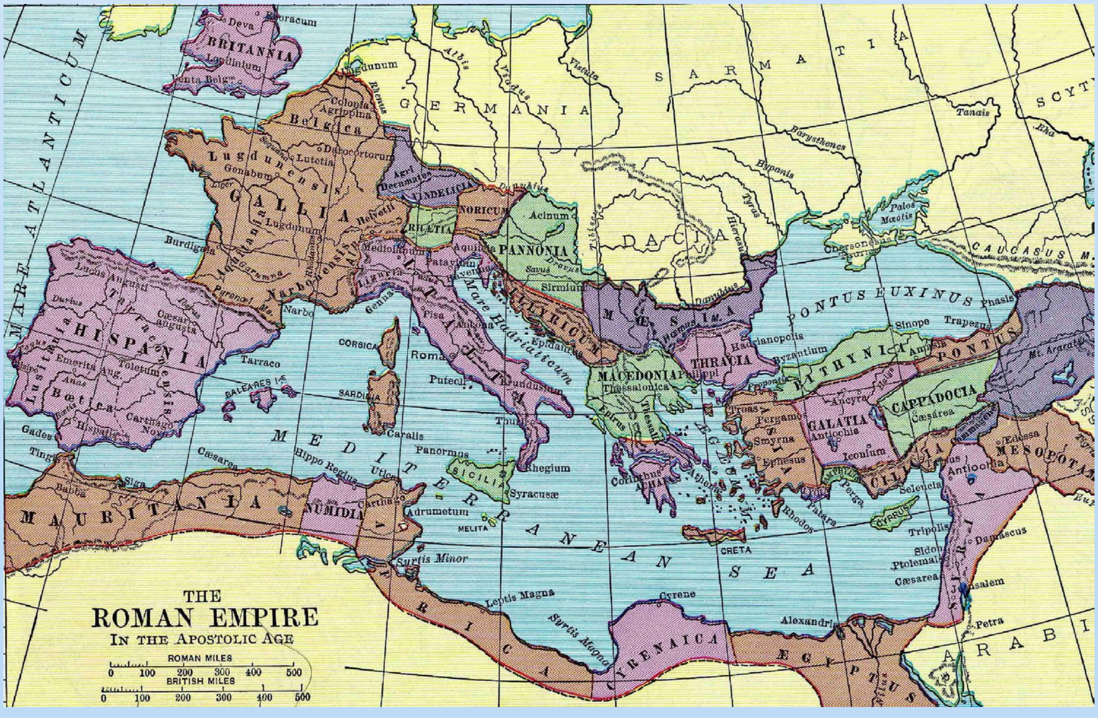
The story begins during one of the most chaotic moments in Roman history. Emperor Pertinax had been in power for less than three months when members of his own personal guard, the Praetorian Guard, assassinated him. After murdering the man it was sworn to protect, the Praetorian Guard was now in control of Rome with no clear successor standing in their way. And that was the moment when the Guard reportedly made an astonishing announcement: the imperial throne would go to whoever offered them the most money. In effect, the Roman Empire was being auctioned to the highest bidder.

A wealthy senator named Didius Julianus heard what was happening and hurried to the Guard's camp. Another prominent Roman, Sulpicianus, the late emperor's father-in-law, was already there trying to secure the throne. The two men began competing against each other, increasing the amount they promised to pay each soldier.

According to the ancient historian Cassius Dio, Julianus finally won by dramatically raising his offer. The guards accepted his bid, proclaimed him emperor, escorted him to the palace, and surrounded the Senate with armed soldiers while the senators confirmed his new position. For a moment, the unbelievable plan appeared to have worked. Julianus had the title, the palace and the Guard standing behind him. He even had the Senate's official approval. However, he did not have the support of the Roman people, and he certainly did not have the loyalty of the powerful Roman armies stationed outside the city walls.

It is important to be fair about Julianus' role in this story. He was not an innocent man who was tricked into handing over his life savings. He knowingly participated in a corrupt bargain following the murder of an emperor. He saw an opportunity to purchase political power, and he chose to take it. Still, his decision reveals something surprisingly familiar. Julianus appears to have believed that his money could buy more than a title. He trusted that the Guard could give him real, lasting control of the Empire.

Similarly, scammers often sell people an outcome they cannot guarantee: a high-return investment, a dream job, protection from arrest, the perfect home, or even a loving relationship. The details vary, but the promise is designed to make the target picture a future they desperately want, or urgently need, to believe is possible. Once that belief takes hold, warning signs become easier to overlook.



The same is true when a proposal appears to have the backing of a trusted authority: a call that seems to come from a bank, or a message that appears to be from a government agency, or an investment adviser that displays official-looking documents. The appearance of authority can make an extraordinary request seem safe, legitimate, and even routine. The Praetorian Guard did not merely pretend to hold power. Its members had real military authority, and they used it to make a corrupt transaction appear enforceable. Their weapons, position, and influence gave Julianus reason to believe that the bargain could succeed. However, their power had limits, and Julianus discovered those limits too late.

News of the imperial auction spread across the Empire, and several powerful generals refused to recognize the new emperor. One of them, Septimius Severus, marched toward Rome with his army. As he approached, support for Julianus collapsed and the same Guard that had helped place Julianus on the throne was unable, or unwilling, to keep him there. The Senate declared Julianus a public enemy and condemned him to death and, after a short reign of about two months, he was killed in the palace.

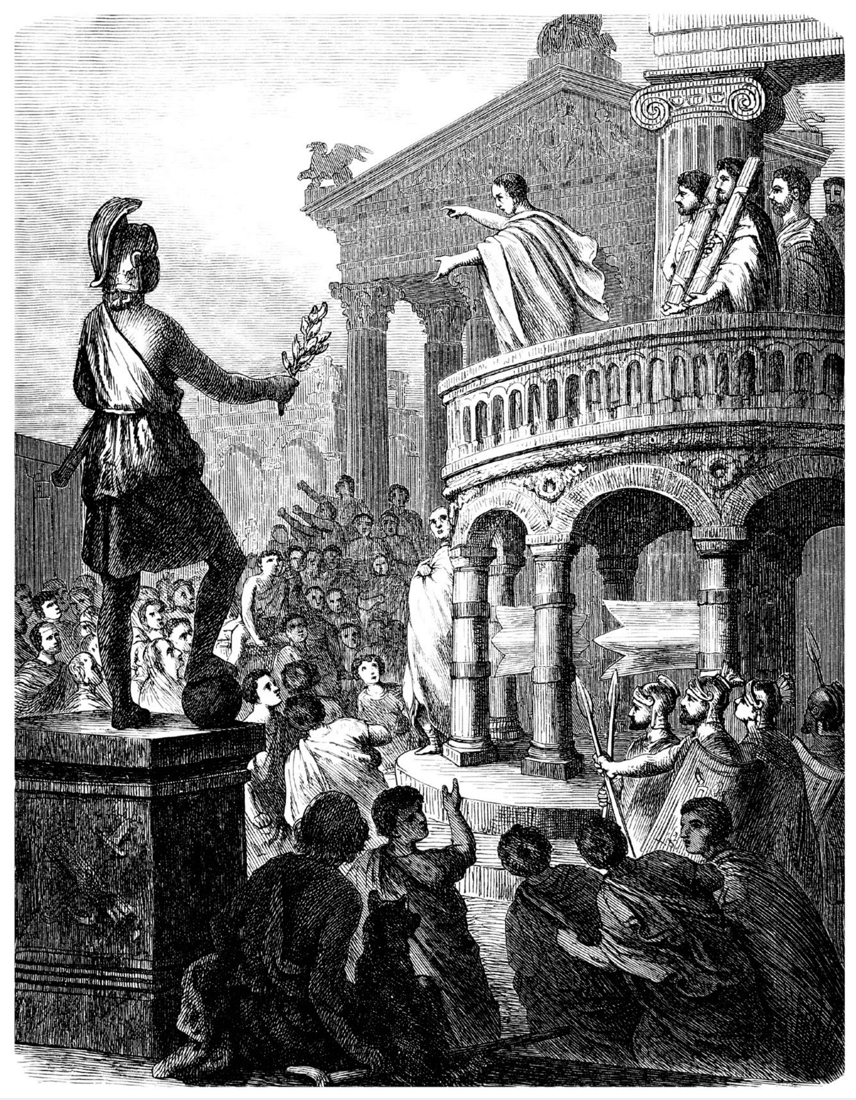
This strange episode was not a scam in the modern legal sense, and Julianus should not be confused with an innocent consumer targeted by a fraudster. In fact, ancient accounts suggest that Julianus may also have promised the guards more money than he could actually provide. Everyone involved was pursuing personal advantage, and no one entered the arrangement with entirely clean hands.

But there is a timeless warning beneath the corruption and political drama: wanting something to be true can make an unreliable promise feel much more credible. That is one reason scams succeed. A person may believe an investment will provide financial freedom, that a new relationship is genuine, or that paying an urgent fee will prevent a frightening consequence. The stronger the anticipated reward, or the greater the fear of losing it, the harder it can become to step back and question the promise.

When someone claims to guarantee an extraordinary outcome, do not let impressive titles, official appearances, time pressure, or your own hopes make the decision for you. Pause, verify the claim independently, and ask the question Julianus failed to consider:

Can this person actually deliver what they are promising?

History's answer in this case was swift and unforgiving. Julianus' money got him through the palace doors but could not keep him there.



## About the Series

This article is part of A Scam as Old as Time, our recurring series exploring the surprising history of fraud and the lessons it still offers today's consumers.

## Coming Next: The Man Who Sold the Eiffel Tower – Twice

In our next installment, we'll travel to 1920s Paris to meet the con artist who convinced buyers that the Eiffel Tower was for sale, not once, but twice, and discover how appearances, authority, and a carefully crafted story helped him make the unbelievable seem real.

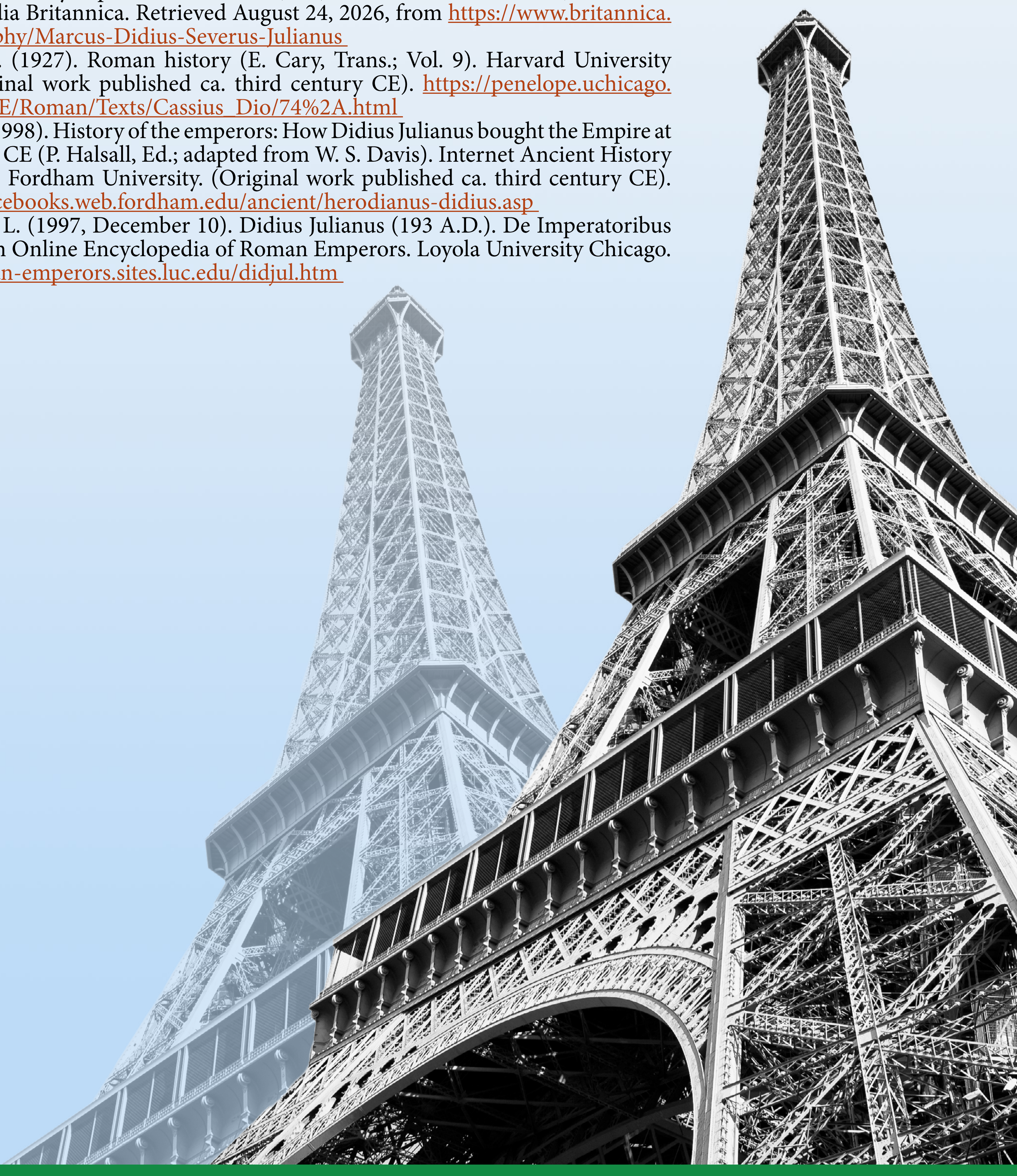
## References


The Editors of Encyclopaedia Britannica. (n.d.). Marcus Didius Severus Julianus. In Encyclopaedia Britannica. Retrieved August 24, 2026, from https://www.britannica.com/biography/Marcus-Didius-Severus-Julianus

Cassius Dio. (1927). Roman history (E. Cary, Trans.; Vol. 9). Harvard University Press. (Original work published ca. third century CE). https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Cassius_Dio/74%2A.html

Herodian. (1998). History of the emperors: How Didius Julianus bought the Empire at auction, 193 CE (P. Halsall, Ed.; adapted from W. S. Davis). Internet Ancient History Sourcebook, Fordham University. (Original work published ca. third century CE). https://sourcebooks.web.fordham.edu/ancient/herodianus-didius.asp

Meckler, M. L. (1997, December 10). Didius Julianus (193 A.D.). De Imperatoribus Romanis: An Online Encyclopedia of Roman Emperors. Loyola University Chicago. https://roman-emperors.sites.luc.edu/didjul.htm

# FIVE PLACES YOU SHOULD NEVER USE A DEBIT CARD

Imagine your granddaughter has been begging to go to ballet lessons for over a year. She has been on the waiting list and the studio just called to tell you she has a spot, but you have to pay for the full season in advance - $2,600. You give your credit card information, hang up and immediately call your granddaughter with the good news. She is thrilled! A couple of days later, you notice the transaction was processed twice. You open the card app on your phone and open a dispute, and the second charge disappears. If you had used your debit card, it would be a completely different situation: the money would have come straight from your checking account, and it could have taken weeks to have that transaction reversed.

Credit and debit cards appear to be the same, but the security behind them differs vastly. Federal law limits your liability for unauthorized credit card charges at $50; some issuers waive that amount. However, if you report a debit card more than two days after it was stolen, you are liable for $500, or the entire balance if it has been 60 days or more.

An added bonus with credit cards is that some feature rewards. Did you know that in 2024, Americans earned $47.5 billion in credit card rewards? At an average of $228 per cardholder, that could be a nice dinner out with friends or a new pair of shoes. Debit cards do not earn rewards.

Since credit cards have stronger fraud protection (and rewards), there are five places you should always use a credit card instead of a debit card.

## Gas Stations and Convenience Stores

Gas stations are a favorite of criminals with skimmers, those hidden contraptions that nick your card information the second you swipe. [According to FBI estimates], skimmers cost consumers and financial institutions more than $1 billion per year. If you use a credit card, fraud can be detected in real time by keeping an eye on your account. Losing your debit card info to fraud means the crooks can drain your bank account and it could take weeks to get that back.

Using a credit card with gas rewards could even earn you cash back and keep your checking account safe.

Consumers who suspect that a gas pump has been tampered with should contact the gas station manager and file a complaint with FDACS. You can [file a complaint online] or by calling 1-800-HELP-FLA (435-7352) or, for Spanish speakers, 1-800-FL-AYUDA (352-9832).

## Travel Arrangements

Debit cards do not work well with reserving flights, hotels, or rental cars. Hotels and rental car agencies normally place holds on your debit card which can sit for several days, which can tie up your money. When you use a credit card, the hold is placed on the issuer of the card, leaving you free to continue using the card.

Credit cards have so many more advantages, the choice is easy.

- Trip protection: Many travel cards offer trip insurance, reimbursement for lost baggage and rental car coverage.
- Great rewards: Some travel cards provide even more points when you book through their website, which can save you money or save on your next trip.
- Extra incentives: Check to see if your card has more perks, like hotel upgrades, airport lounge access or TSA PreCheck credits.

To file a complaint against a seller of travel, use our online complaint form or call 1-800-HELP-FLA (435-7352).

## Online Shopping

Using your debit card while shopping online is risky. Even buying from a reputable source is perilous, as hackers are omnipresent. Then take into consideration the number of dodgy websites you see on social media. All it takes is one time for your debit card to fall into the wrong hands, and charges start appearing. By the time you notice and report the fraud, you could be out thousands of dollars, then your account is frozen for days while the investigation continues. By the way, there is no guarantee you will recoup those losses. Remember with a credit card, you're only on the hook for $50.

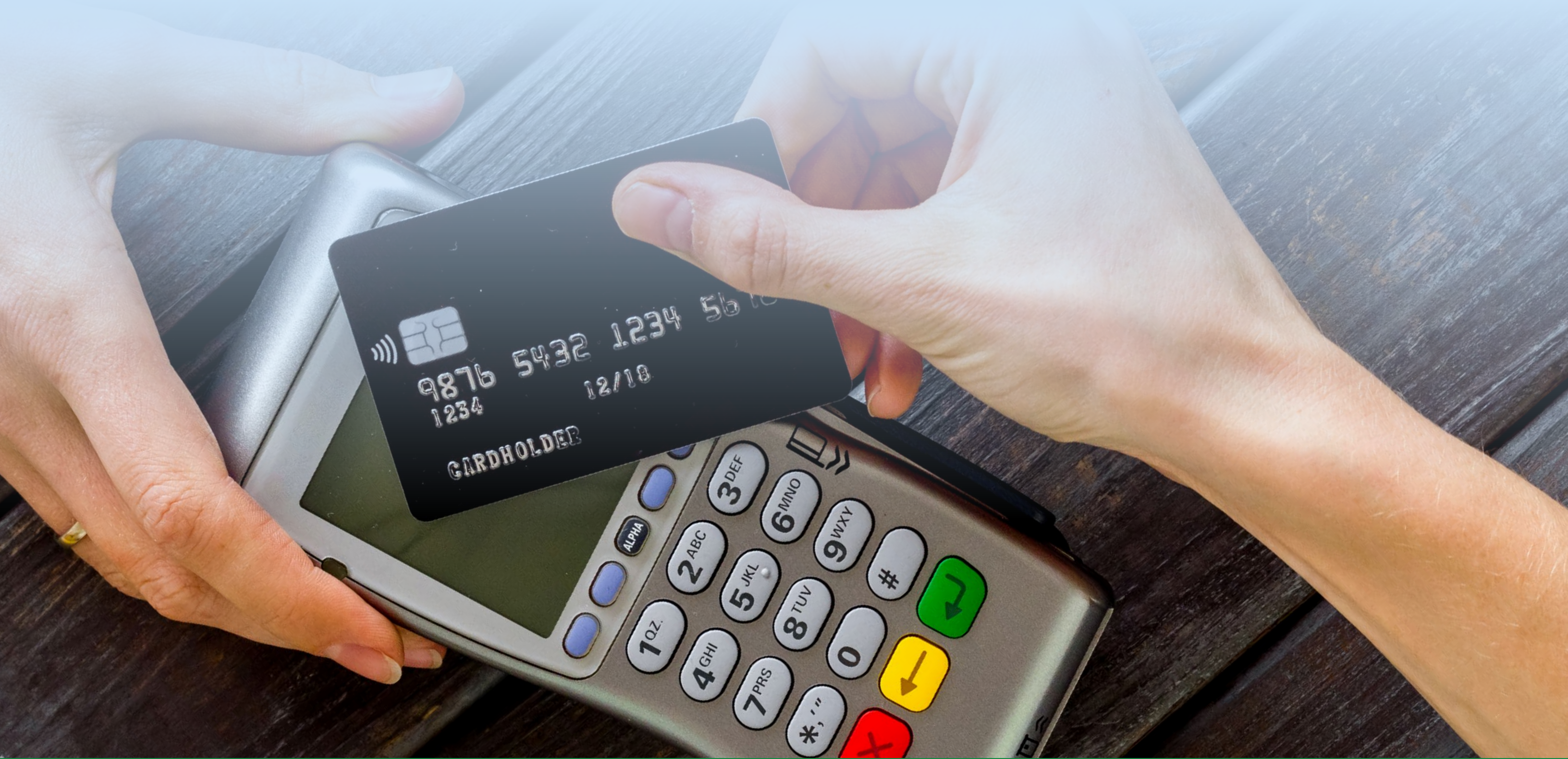
## Big Ticket Purchases

Many credit cards carry additional safeguards for the pricier items you purchase, such as an extended warranty, damage and theft protection for your new 72" television. Debit cards offer none of these.

## Restaurants and Bars

There is a new tapas place in town, and you cannot wait to try it. You and a friend head there on opening night and snag a great table. The place is bustling and the staff is a tad overwhelmed, but you are having such a good time. You hand over your debit card to pay. When your server returns, you realize it has been several minutes – plenty of time to clone or skim your card. Again, your checking account is at risk. If you had used a credit card, all you have to do is freeze the card through an app on your phone, and in seconds, your account is protected. Not to mention, there are a plethora of dining reward cards that cash back at restaurants, so being safe pays.

Adapted from: 5 Places You Should Never Use a Debit Card | The Motley Fool



# CRYPTOCURRENCY INVESTMENT FRAUD

From FBI.gov

Cryptocurrency investment fraud, which the media commonly describes as pig butchering, is one of the most prevalent and damaging fraud schemes today. Scammers, through various means of manipulation, convince victims to deposit more and more money into financial "investments" using cryptocurrency. In truth, these investments are fake; all victim money is under the control of—and ultimately stolen by—criminal actors, usually overseas. As a result, victims typically lose all money they invested.

Learn more about cryptocurrency investment fraud and the process scammers use to find potential victims.

## Process

### 1. Victim selection

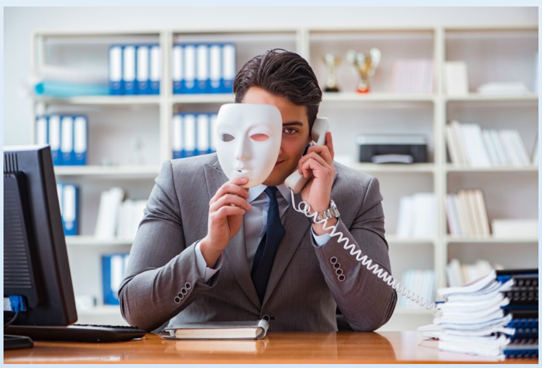
Scammers use a variety of methods to initially lure and contact victims. If you met someone through a method described below, and that person pitched an investment opportunity that involved cryptocurrency, beware, as this is likely cryptocurrency investment fraud. Here are some of the most common methods:

- **Social media:** Scammers use social media to reach out to victims directly—by messaging them—or indirectly through deceitful job advertisements or investment opportunities that can be found on social media platforms.
- **Texting:** Scammers text victims pretending they mistyped a number, sending a photo of themselves, or saying they work for a company that is hiring for job opportunities.
- **Dating sites:** Scammers create thousands of fake dating profiles on all common dating sites and match with victims to establish a romantic relationship based on trust.
- **WhatsApp, Telegram groups:** Being invited/added to a chat group that begins to provide investment advice to a seemingly large group of witting participants.
- **Searching online:** Many of these fake investment applications can be found by searching the Google Play Store or Apple Store on your own. It's no longer necessary to be provided with a malicious platform from someone you meet online.
- **Online advertisements:** Scammers heavily advertise fraudulent investment platforms on social media and on websites such as YouTube and Reddit.

## 2. Building trust

Once initial communication has been established, scammers seek to deceive victims about who they are (their persona) and what they want (their "desires") to build trust with the victim. Tactics vary, but below are common characteristics of cryptocurrency investment fraud scammer personas:

- excessive flattery or expressing a strong romantic interest in the victim
- empathizing with, and often suffering from, similar life events as the victim (e.g., if a victim is going through a divorce, then the scammer may be going through a divorce, too)
- suffering from a hardship that requires help from the victim
- sharing pictures, often selfies, of themselves
- providing screenshots over chat applications on each step of investing in the new platform
- allowing you to withdrawal sums of money when you first start "investing" in the malicious platform
- coaching on how to respond (or ignore) law enforcement emails and calls, or how to respond to banks if they ask questions regarding money transfers
- claiming they've been victims of cryptocurrency frauds themselves, and warning you against certain platforms
- offering to meet in person but making those meetings contingent upon the victim accomplishing a task (e.g., we can meet once you raise enough money), always finding an excuse at the last minute for why they can't



## 3. Pitch

Once trust is established with victims, criminals introduce the topic of investing. It's common for scammers to say they themselves—or people in their family or close network—are experts in such investments. They may promise they can bring the victim in on "the ground floor."

The types of investments can vary; common ones include:

- Cryptocurrency options or futures trading
- Artificial Intelligence (AI)-based trading programs
- Short-term, fixed time trades
- "Quantitative" trading programs
- Gold futures

## 4. Initial investment

Once the scammer convinces the victim to participate in their scheme, the scammer will tell the victim how to invest the money, as follows:

- Open a cryptocurrency account at a reputable exchange.
- Transfer money from a traditional bank account to the new cryptocurrency account.
- Convert the money—now hosted on the cryptocurrency exchange—to the cryptocurrency type the scammer specifies, e.g., Bitcoin, ETH, Tether, USDC.
- Open an account on the "investment platform" provided by the scammer or an individual or group that the scammer directed the victim to.
- Deposit the cryptocurrency to the investment platform either directly or through a private wallet.

Investment platforms: These "platforms" exist in the form of what appear to be traditional websites, either accessible via the web or through a specific browser only accessible via cryptocurrency applications. Common factors include:

- Registration using an email address or phone number.
- Two-factor authentication (e.g., a phone number + an email address) to log in.
- A website name that closely mimics—or "spoofs"—a legitimate site.
- A professional-looking site design that shows the portfolio in an appealing manner.
- A customer support portal used to communicate about investments and withdrawals.

### 5. The growing investment

Once the victim starts to "invest," returns shown on the investment platform will appear to be extremely lucrative, encouraging the victim to invest more and more.

Scammers use various means to "sweeten the pot," or encourage further investing. Examples include:

- Matching: Providing their own funds to the victim's portfolio to help the victim reach an (arbitrary) investment goal.
- Scarcity: Stating that returns or investment opportunities are only available in a short time period.

## What do you do if you're a victim?

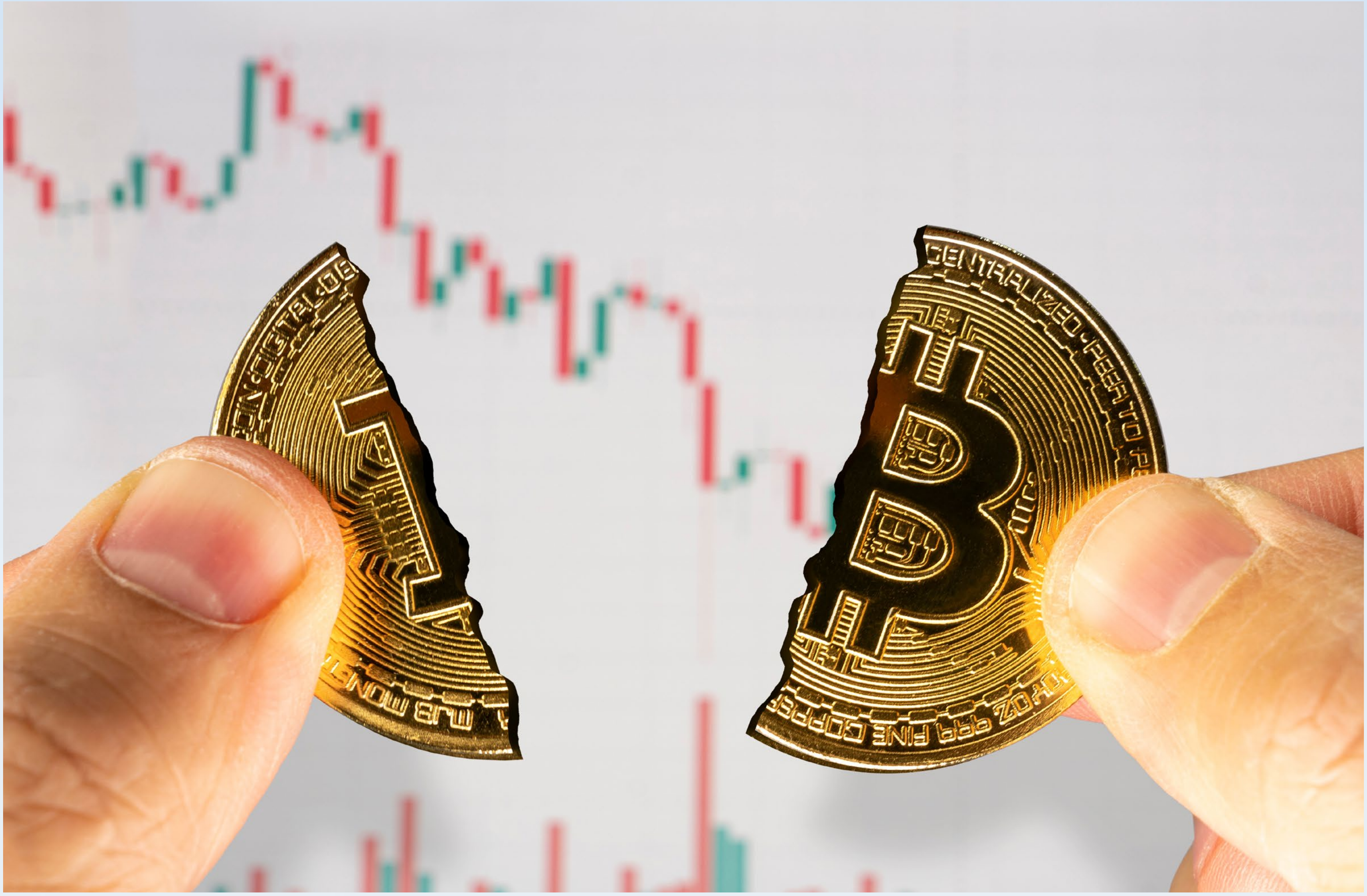
If you feel that you are a victim of a cryptocurrency investment fraud, stop sending any money to the suspected criminals and file a report at FBI's Internet Crime Complaint Center at ic3.gov. Do not notify the suspected criminals of the FBI's involvement, as that may compromise law enforcement's ability to investigate.

When filing a report at ic3.gov, if possible, please include the following:

- information regarding how the scammer initially contacted you and how they identified themselves (include identifying information such as name, phone number, address, as well as email addresses and usernames of the scammer)
- financial transaction information such as the date, type of payment, amount, account numbers involved (to include cryptocurrency wallet), the name and address of the receiving financial institution, and receiving cryptocurrency addresses

If you believe you or someone you know may be a victim of a cryptocurrency investment scam, immediately submit a report to ic3.gov or contact your local FBI field office and provide as much transaction information as possible.

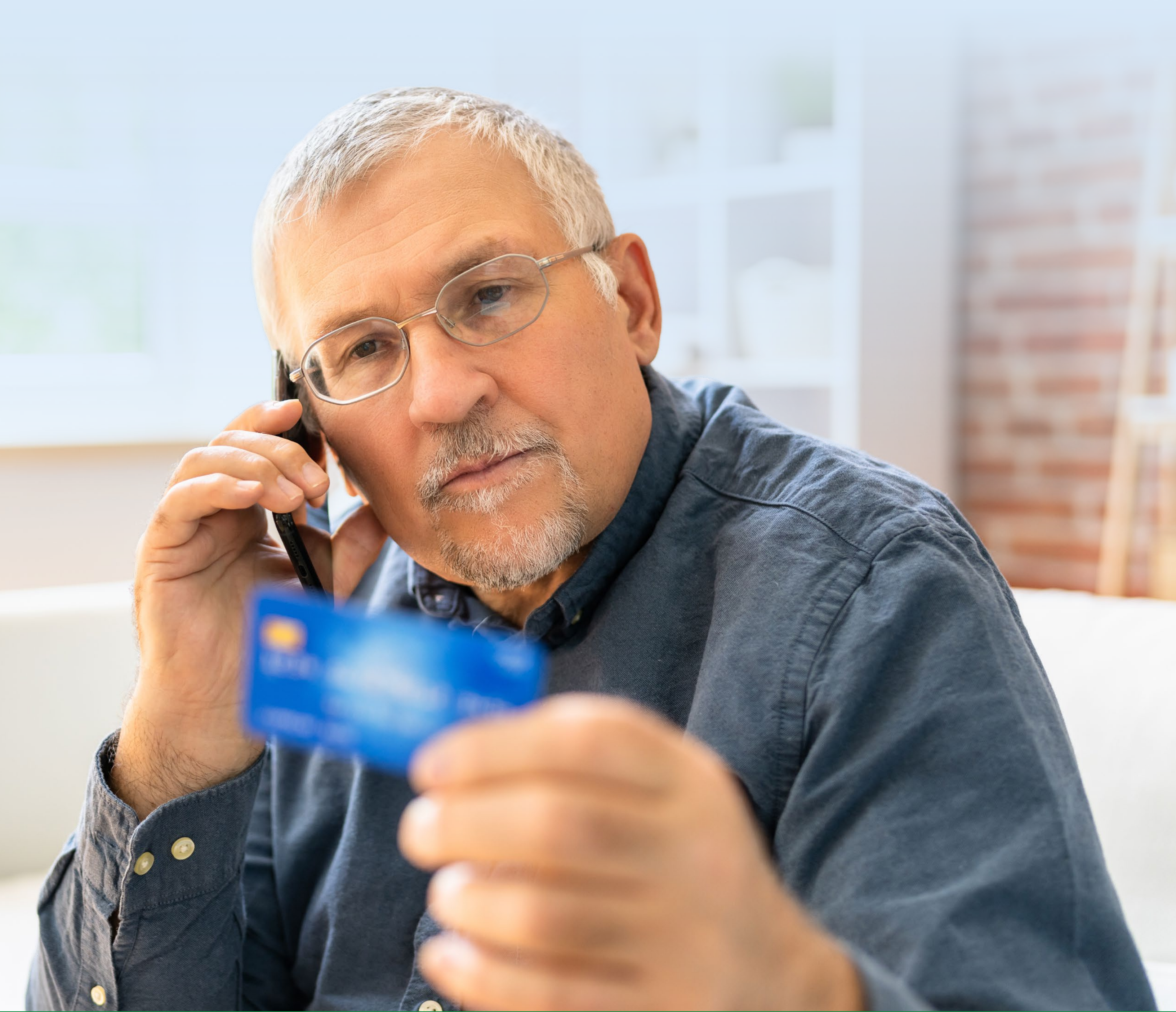
For more information, see the following FBI Public Service Announcement: Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Schemes. Be wary of anyone claiming they can recover your funds, as this may be another scam.



## Tips for avoiding cryptocurrency investment fraud

The FBI has identified potential ways individuals can recognize and deter this activity:

- If an unknown individual contacts you, do not release any financial or personal identifying information (PII) and do not send any money.
- Do not invest per the advice of someone you meet solely online.
- Verify the validity of any investment opportunity from strangers or long-lost contacts on social media websites.
- Be on the lookout for domain names that impersonate legitimate financial institutions, especially cryptocurrency exchanges.
- Misspelled URLs, often with a slight deviation from the actual financial institutions' website, may be fake.
- Do not download or use suspicious looking apps as a tool for investing unless you can verify the legitimacy of the app.
- If an investment opportunity sounds too good to be true, it likely is. Be cautious of get rich quick schemes.
- Confirm the validity of any investment opportunity or cryptocurrency investment website or app.
- If you already invested funds and believe you are a victim of a scheme, do not pay any additional fees or taxes to withdraw your money.
- Do not pay for services that claim to be able to recover lost funds.




# Fraud Prevention Workshops

## Spot the signs. Stop the scams.

**Jacksonville**
Tuesday, September 29
5:45 p.m.
**Hancock Whitney Bay Meadows Financial Center**
8195 Point Meadows Way
Jacksonville, FL 32256

**Tallahassee**
Tuesday, October 22
5:45 p.m.
**Florida State University Campus**
Tallahassee, FL 32306

hancockwhitney.com

Refreshments will be provided.

Hancock Whitney, in partnership with the Gus A. Stavros Center for the Advancement of Free Enterprise and Economic Education at Florida State University and the Florida Department of Agriculture and Consumer Services, invites you to a **free community Fraud Prevention Workshop**.

### What You'll Learn

- Recognize common fraud and scam warning signs
- Tips to help protect your personal information
- What to do if you suspect fraud or become a victim
- Resources to help safeguard your finances

### Reserve Your Spot Today

SCAN QR CODE TO REGISTER

Workshops are free and open to the public, but **registration is encouraged.**



1564151 0826

# 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 FloridaConsumerHelp.com 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.*