



Redwood  
Credit Union®

# Protecting Against Fraud & Scams

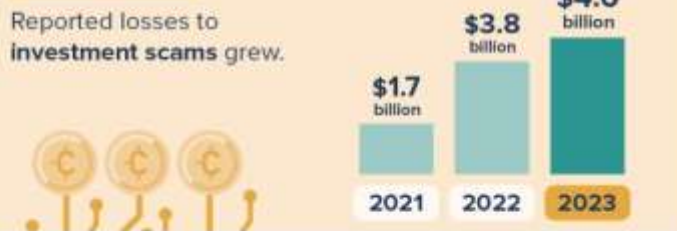
Hana Aymar, Enterprise Fraud Manager



# A Scammy Snapshot of 2023

(based on reports to Consumer Sentinel)  
ftc.gov/data  
ReportFraud.ftc.gov

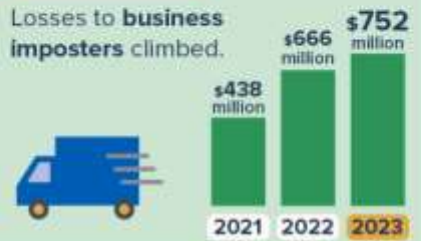
## Top Frauds



**REPORT** 2.6 million fraud reports

**\$** \$10 billion reported lost

The number of reports and the amount lost is up.  
(2022: 2.5 million fraud reports, \$9 billion lost)

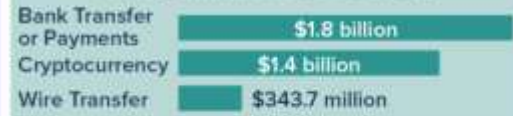


### ★★★ Reports by Military Consumers ★★★

**Imposters:** Highest # of reports: **42,000**  
Highest total losses: **\$178 million**

**Investments:** Highest % with loss: **81%**  
Highest median losses: **\$7,000**

### Top Payment Methods and Losses



Scammers contacting people by phone or on social led to big losses.

**Phone calls:**  
Highest per person reported losses

**\$1,480** median loss

**Social media:**  
Highest overall reported losses

**\$1.4 billion** total lost

**Email:**  
Highest # of reports

**358,000** reports

# 2023 FTC Scam Data

## We want to empower you

HOWEVER- You do not need to handle fraud alone

Contact your bank or credit union if you think you are being scammed

# Scam Variations

Scam stories and red flags

# Impersonation Scams

Financial  
Institutions

Phantom  
Hacking

Social Security

Friends &  
Family

Virus/  
Malware  
Pop-up or  
email

Tech  
Companies

Government  
Agencies





The system have found [15] viruses that pose a serious threat to your system.

Threat	Alert	Severity	Action	Status
Trojan.FakeAV-Download		Low	Quarantine	Active
Spyware.BANKER.ID		High	Remove	Active
Trojan.FakeAV-Download		High	Remove	Active
Trojan.FakeAV-Download		High	Quarantine	Active
Trojan.FakeAV-Download		High	Quarantine	Active



### Invoice updated

Billing Department of PayPal updated your invoice

Amount due: \$600.00 USD

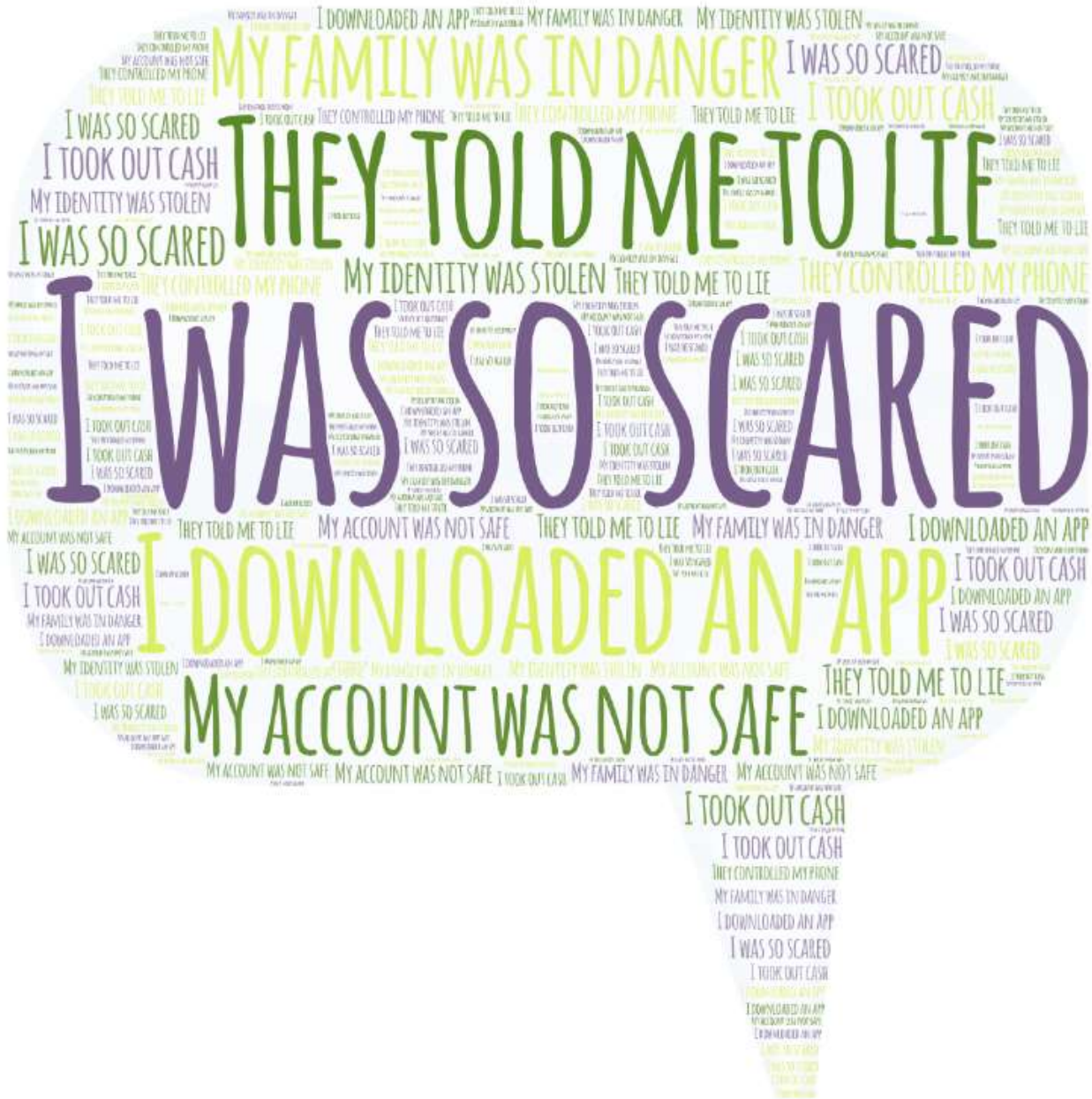
[View and Pay Invoice](#)

### Seller note to customer

There is evidence that your PayPal account has been accessed unlawfully. \$600.00 has been debited to your account for the Walmart eGift Card purchase. This transaction will appear in the automatically deducted amount on PayPal activity after 24 hours. If you suspect you did not make this transaction, immediately contact us at the toll-free number +1 (888) 865-0443 or visit the PayPal Support Center area for assistance. Our Service Hours: (06:00 a. m. to 06:00 p. m. Pacific Time, Monday through Friday)

- » Fraudsters create a sense of urgency
- » They often have some identifying information to increase legitimacy
- » They spoof real phone numbers
- » They request access, information, or money

- Online banking username/verification codes/partial card numbers
- Ask you to send a transfer to “protect funds”
- Ask that you download remote access apps (AnyDesk, Teamviewer, GoToMyPC, LogMeIn)





Source: [www.ftc.gov](http://www.ftc.gov) “How to Avoid a Tech Support Scam”



# Protect Yourself!

- » If you get a virus warning pop-up that instructs you to call a number, **TURN YOUR COMPUTER OFF/UNPLUG**
- » Don't trust caller ID. Instead call back at a trusted phone number
- » Be careful when searching for phone numbers online- use trusted websites rather than search results
- » Don't download software or allow device access
- » Don't share verification codes to someone who calls you– those are for online access or when you initiate contact

**Never move or transfer your money to “protect it.”**

**It's a scam.**

**BANK**

**FEDERAL TRADE COMMISSION**



# Romance Scams



Source: [www.ftc.gov](http://www.ftc.gov) "Social media: a golden goose for scammers"

# Protect Yourself!

- » **Stick to in-app communications.** Fraudsters like to leave the app and chat on WhatsApp/Google Hangout or even through email and text messages
- » **Reverse Google Image Search.** Fraudsters often recycle photos or pull photos of legitimate people from the internet.
- » **Be wary of new romances that move quickly.** Fraudsters are often quick to “fall in love” and sometimes will refer to their victim as “wife” or “husband”
- » **Don’t share financial information or money.** Fraudsters often “can’t access” their bank accounts and need their victims to move money for them.
- » **Push to meet in person.** Fraudsters often cannot meet in person, resist video chats, arrange visits but then cancel last minute.
- » **Use caution in “international” romance.** Fraudsters are often US citizens who are abroad for various reasons, usually due to work or military obligations. They’ll even utilize identities that are “searchable” online

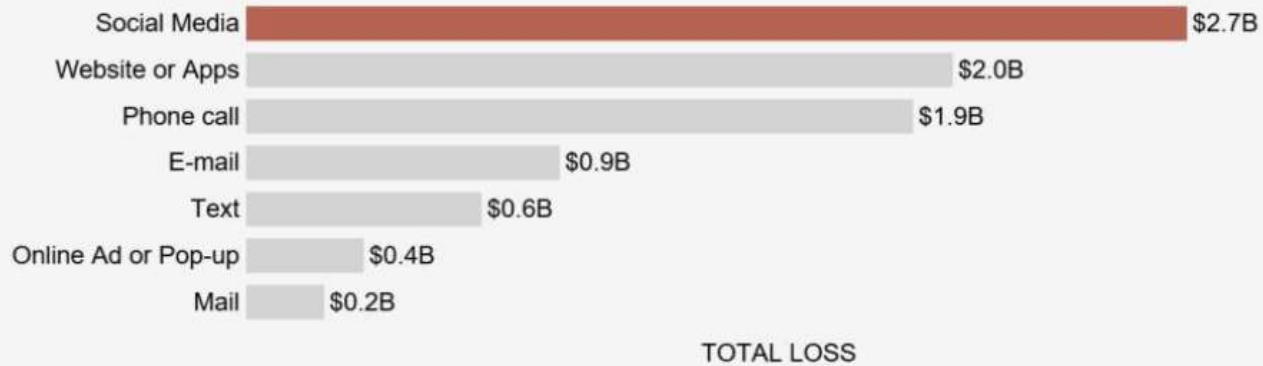


# Social Media Scams

## Reported fraud losses by contact method

January 2021 - June 2023

More money was reported lost to fraud originating on social media than by any other method of contact.



Not shown are contact methods classified as other, including TV or radio, print, fax, in person, and other methods consumers write in or that cannot be otherwise categorized.

## Top social media scams

January 2023 - June 2023

While the largest share of reports came from online shopping scams, investment and romance scams topped the list on dollars lost.



The median individual reported losses were as follows: \$100 (online shopping), \$3,000 (investment related), and \$1,716 (romance scams).

Source: [www.ftc.gov](http://www.ftc.gov) "Social media: a golden goose for scammers"

# Protect Yourself!

- » **If you get a message from a friend about an opportunity or urgent need, call them.** Their account may have been hacked. Fraudsters will use compromised social media profiles to profess incredible investment opportunities or emergencies. Call a trusted phone number rather than communicating within a social media application.
- » **Don't take investment advice from someone on social media.** Fraudsters will create fake/stolen profiles to generate likes and then will direct messages to individuals touting their "tried and true" investment methods.
- » **Before you buy, check out the company.** Search online for the business name and words like "scam" or "complaint".
- » **Limit who can see your posts and information on social media.** Fraudsters are more able to find you and cater to your interests if you have public settings on social media





# Employment Scams

BBB UPDATE FINDS JOB SCAMS GROWING AS WORKERS SEEK REMOTE WORK OPTIONS.

From Jan-Mar 2023, losses reported to BBB hit **\$840k**, up over **250%** compared to the same time last year.

2020 - March 2023 complaints and reports

**12,925**  
BBB SCAM TRACKER<sup>SM</sup>  
REPORTS

**15.4%**  
REPORTED  
LOSING MONEY

**\$4.77 million**  
REPORTED LOSSES

**\$1,000**  
MEDIAN LOSS

Source: BBB Scam Tracker

**282,061**  
FTC REPORTS

**\$845.1 million**  
REPORTED LOSSES

Source: Federal Trade Commission's Consumer Sentinel Network

## Watch out for:



Jobs requiring you to pay money



Remote jobs involving checks



Cold calls about jobs



Higher-than-average pay



Interview processes done strictly over email



Mystery shopping, re-shipping, check-cashing, nanny and car wrap job offers

Source: [www.bbb.org](http://www.bbb.org) "BBB Employment Scams Study Update"

# Protect Yourself!

- » **Search online.** Look up the name of the company who is hiring you along with the words “scam” and “complaint”
- » **Pay close attention to how you are contacted.** Fraudsters will communicate through unofficial email addresses/phone that aren’t associated with the real company.
- » **Don’t take a check “up front” for set up costs.** Fraudsters will send (often through Priority Mail) counterfeit checks to pay for “equipment” or “services” needed for set up. Even cashier’s checks can be counterfeited.
- » **Don’t buy gift cards or use money transfer services.** Fraudsters often have you purchase gift cards or send money as “part of the job”. This leaves you holding the bag when they disappear.

**Don’t pay for the promise of a job.**

Spot a job scam?

Report it: [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft/identity-theft-reporting)



# Cryptocurrency Scams

## CONSUMER TIP

Get a text from the

**Wrong  
Number?**  
It might  
be a scam.



# How It Works:

- » **Wrong number text.** Fraudsters will initiate conversation with a “wrong number” text, and then continue the conversation.
- » **Fraudster may share a photo to connect with their victim.** The person depicted is often very attractive and friendly
- » **Once the relationship is established, they will begin to speak about their wealth and how they accumulated it.** This is where cryptocurrency comes in.
- » **They offer to connect you to their “advisor” who will get you set up with a cryptocurrency wallet.** They establish elaborate websites which operate similar to online banking. You can go there and “log in” to see your (exponential) gains
- » **They let you draw on your investments initially so you gain trust in the system.** Don’t be swayed by being able to draw. This is by design.
- » **When you have “earned” enough money and try to do a big draw, they will tell you that you need to pay more to free your money, often through “fees” or “upfront taxes”.** They will urge you to get loans at “whatever cost is necessary” since you’ll be able to pay it back once you have your funds.
- » **Then they disappear.**





# Identity Theft



## Preventing ID Theft

- » Do not provide identifying information to anyone over the phone if YOU didn't initiate the call
- » Use verbal passwords at financial institutions and with phone providers
- » Vary (complex) passwords across all online accounts to prevent unwanted access to your data
- » Use P.O. Box as your address
- » Shred all sensitive mail
- » Use a credit monitoring service
- » Freeze your credit
  - » If you have young children in your lives, urge their primary care providers to freeze their credit
  - » Use a credit monitoring services if it doesn't work for you to freeze your credit
- » Check your credit regularly
  - » [Annualcreditreport.com](http://Annualcreditreport.com)

**28% of victims**

have to borrow money from family or friends

**13% of victims**

had problems with coworkers

**40% of victims**

could not pay bills

**32% of victims**

reported that their identity crime incident lead to problems with family members

**54% of victims**

say they feel violated as a result of their identity being misused

## Reporting ID Theft

- » File a police report immediately
  - » Contact Federal Trade Commission- 877-382-4357
  - » Contact Social Security Administration Fraud Line- 800-269-0271
- » Contact your credit unions, banks, and credit card companies
- » Call National Credit Reporting Organizations
  - » Equifax- 800-525-6285
  - » Experian- 888-397-3742
  - » Trans Union- 800-680-7289





Questions?





FOR ALL THAT YOU LOVE.