SCOTTSDALE POLICE DEPARTMENT

Financial Crimes Unit

Victim Information Packet

Digital copy

CONTACT US:

480-312-5000 (NON-EMERGENCY)

WWW.SCOTTSDALEAZ.GOV/POLICE

SCOTTSDALE PD
FINANCIAL CRIMES UNIT
UPDATED: 04/2026

FINANCIAL CRIMES VICTIM QUICK FACTS SHEET

PROVIDED BY:
FINANCIAL CRIMES UNIT | SCOTTSDALE PD

FREEZE AND MONITOR YOUR CREDIT:

Experian
National Consumer Assistance 1-888-397-3742
www.experian.com/help

Equifax
Consumer Fraud Division
1-800-525-6285
https://www.equifax.com/

TransUnion
Fraud Victim Assistance Department 1-800-680-7289
www.transunion.com

REPORTING AND HELPFUL WEBSITES:

Reporting Websites:
https://www.identitytheft.gov
https://reportfraud.ftc.gov
https://complaint.ic3.gov
https://eservices.scottsdaleaz.gov/crimereport

Helpful Websites:
https://www.ic3.gov/PSA
https://www.identitytheft.gov/Steps
https://www.irs.gov/identity-theft-central/identity-theft-guide-for-individuals

EXAMPLES OF PAID SERVICES:

Delete Me*:
https://joindeleteme.com/

LifeLock*:
https://lifelock.norton.com/

McAfee*:
https://www.mcafee.com

AARP*:
https://www.aarp.org

*not an endorsement

SCOTTSDALE POLICE DEPARTMENT

NON-EMERGENCY: 480-312-5000
EMERGENCY: 911

UPDATED 04/15/2026 | J. FULLER

ELDER FRAUD VICTIM RESOURCE GUIDE

SCOTTSDALE POLICE DEPARTMENT

NON-EMERGENCY: 480-312-5000
EMERGENCY: 911
HTTPS://WWW.SCOTTSDALEAZ.GOV/POLICE

UPDATED 04/01/2026 | J. FULLER

Step 1: Don't Panic

Scams happen every day to thousands of people. While this is **NOT** okay - remember, you are not alone.

You **CAN** recover from this, and there are many options for help.

Step 2: Report It

Local Police — **Non-Emergency Line**

FBI through IC3 — **www.ic3.gov**

Step 3: Know Your Resources

After reporting to your local police department and the FBI check out the following websites:

Victim Assistance:

https://www.idtheftcenter.org
https://victimconnect.org
https://www.aarp.org/money/scams-fraud/
https://fightcybercrime.org

Government Support:

https://eldercare.acl.gov/home
https://www.identitytheft.gov
https://www.justice.gov/elderjustice
https://www.donotcall.gov
https://www.fbi.gov/how-we-can-help-you/scams-and-safety

Other Websites:

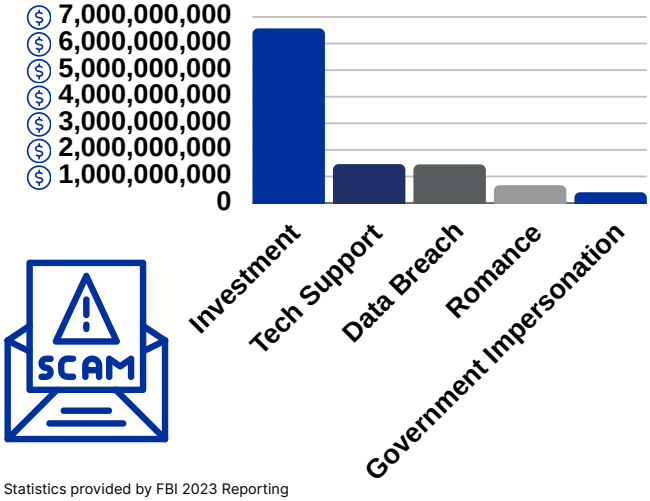
https://988lifeline.org/
https://www.annualcreditreport.com/
https://www.equifax.com/
https://www.transunion.com/
https://www.experian.com/help/

Step 4: Change Passwords

Check to see if your account where you "save" your passwords (computer / phone) was compromised. The scammers may have access to more than you think.

Set up multi-factor authentication with a minimum of two forms of verification. Examples include: Push alerts, Authenticator Apps, Emails, Phone Calls, Texts, Biometrics, etc.

Elder Fraud Stats:



Statistics provided by FBI 2023 Reporting

Step 5: Tell Someone

Ask for Help (Financially):

Recovering your data is a long process, the more help you have from a trusted friend or family member - the easier it will be. Having a Financial Power of Attorney can be extremely helpful during this time.

Ask for Help (Mentally):

Crime victims experience high rates of mental stress. Reach out to a counselor, pastor, spiritual advisor, friend or family member. Be open and honest about your feelings

Share Your Story:

Scammers use shame and embarrassment to continue to victimize people. Telling someone what you are going through can help stop the cycle.

Step 6: Learn About Prevention

01 https://www.fdic.gov/consumer-resource-center/2021-10/avoiding-scams-and-scammers

02 https://fraud.org/prevention-tips/

03 https://www.consumerfinance.gov/consumer-tools/fraud/

5 EASY TIPS TO DETECT A SCAM

01.

Stop and think..is it too good to be true?

No legitimate company would guarantee an initial investment of cash with an immediate return. Nor would any company send you a check for a large amount of money, and tell you to keep some of it, but deposit the rest for them. Remember - if it sounds too good to be true - **IT IS!**

02.

Look it up online

Check your preferred search engine (Google/Bing) and type in a description of the product/deal/business name and include the word "**scam**". If you get multiple matching results - it's a scam.

03.

Ask yourself why they need your info

Legitimate companies would **never** ask for your login information or passwords to your accounts. They also do not need your social security number. **Never** provide personal information to strangers online or on the phone.

04.

Were you expecting the message?

Emails, texts, and phone calls can seem legitimate, especially if they are coming from what appears to be a legitimate company! Do your homework or contact the company directly to verify if it is legitimate. Don't click on links!

05.

Still not sure? Call PD and ask!

You can contact Scottsdale Police Department Non-Emergency anytime at **480-312-5000** and speak to an officer. Remember -it is better to stop the loss before it happens.

LAST UPDATED 03/24/2026 | J.FULLER

STOP A SWINDLE

INVESTOR CHECKLIST

- [ ] **Where did you get my name?**
- [ ] **What risks are involved in the investment?**
- [ ] **Can you send me a detailed explanation of your investment so I can review it at my leisure?**
- [ ] **Would you mind explaining your investment opportunity to my lawyer/accountant?**
- [ ] **Can you give me the names of your company's principals and officers?**
- [ ] **Can you provide references?**
- [ ] **Can you provide a prospectus or risk disclosure statement?**
- [ ] **Is the investment offered on a regulated exchange?**
- [ ] **To what governmental regulatory supervision is your company subject?**
- [ ] **Will you provide written documentation of your track record?**
- [ ] **How long have you and your company been in business?**
- [ ] **Do you have a disciplinary history?**
- [ ] **Are you registered to sell securities?**
- [ ] **When and where can I meet with you or with another representative from your company?**
- [ ] **Where exactly will my money be?**
- [ ] **What type of externally audited financial statements do you provide?**
- [ ] **How much of my money goes for commissions and management fees?**
- [ ] **How can I liquidate (sell) my investment?**
- [ ] **If disputes arise, how can they be resolved?**

Questions provided by:
Arizona Corporation Commission | Securities Division
1300 W Washington, 3rd Floor
Phoenix, AZ 85007

TEL: 602-542-0662
FAX: 602-388-1335
TOLL FREE: 1-866-VERIFY-9
EMAIL: info@azinvestor.gov
WEBSITE: www.azcc.gov/az-investor

CREATED 04/15/2026
J. FULLER

What To Do As a Victim of An Account Takeover Fraud (ATO)

1 Contact Your Bank & Freeze Your Credit

Let all of your financial institutions know about the compromised account. Freeze your credit with all three credit bureaus

Request a "Hold Harmless Letter" or "Letter of Indemnity" from your Bank

2 Change All of Your Passwords

Check to see what information the suspects have accessed. Did they get into your iCloud? Microsoft? Do they have access to your "saved" pre-filled passwords?

Using an uncompromised device, change all of your passwords

3 Set up Multi-Factor Authentication (MFA)

Set up an MFA with your account so that it requires at least two sources of verification.

Security keys, push notifications, fingerprints and facial recognition are all good examples of MFA.

4 Install Anti-Virus Software and Attempt to Get Your Info Off the Internet

Various companies offer ID theft protection, anti-virus software and/or public redaction of your personal information.

Research and pick a company that best suits your needs

5 Tell Your Contacts About the Attack

Let your contacts know about your compromised account, as the scammers may contact them pretending to be you.

Scammers use shame to keep what is happening a secret - take their power away!

6 Report the ATO to IC3.gov & Contact Your Local PD

File a complaint with the FBI through www.IC3.gov. Include all banking information and use the words "account takeover" or "SEO Poisoning" in the description.

You can file with both the FBI and your local PD.

Scottsdale Police Department
Non-Emergency: 480-312-5000
Emergency: 911

UPDATED 04/15/2026 | J. FULLER

PROTECT YOUR HEART & YOUR WALLET

STOP AND REMEMBER:

SCOTTSDALE PD: 480-312-5000

DO YOU KNOW THIS PERSON?

- Where did you meet this person?
- Do you remember meeting them?
- Can you verify they are real?
- If a celebrity - why are they adding you?

IS THEIR PROFILE LEGITIMATE?

- When was their profile created?
- Is their name spelled correctly?
- If a celebrity - are they verified?*

*Note that some websites will allow you to pay for verification, check each website for qualifications

WHAT ARE THEY ASKING YOU?

Have they asked you:

- Where you live?
- If you live alone?
- If you have friends or family in your life?
- What you do (or did) for work?
- **Any** personal questions?

TIP: DON'T ADD STRANGERS ONLINE

Never add or talk to people you do not know online - **even** if you have "mutual" friends

Some scammers add your friends first, so they look less suspicious.

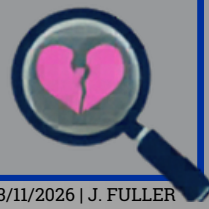
TIP: CHECK THEIR PROFILE FOR CLUES

Check to see if their photos are AI or stolen from other accounts.

This can be done through a reverse image search.

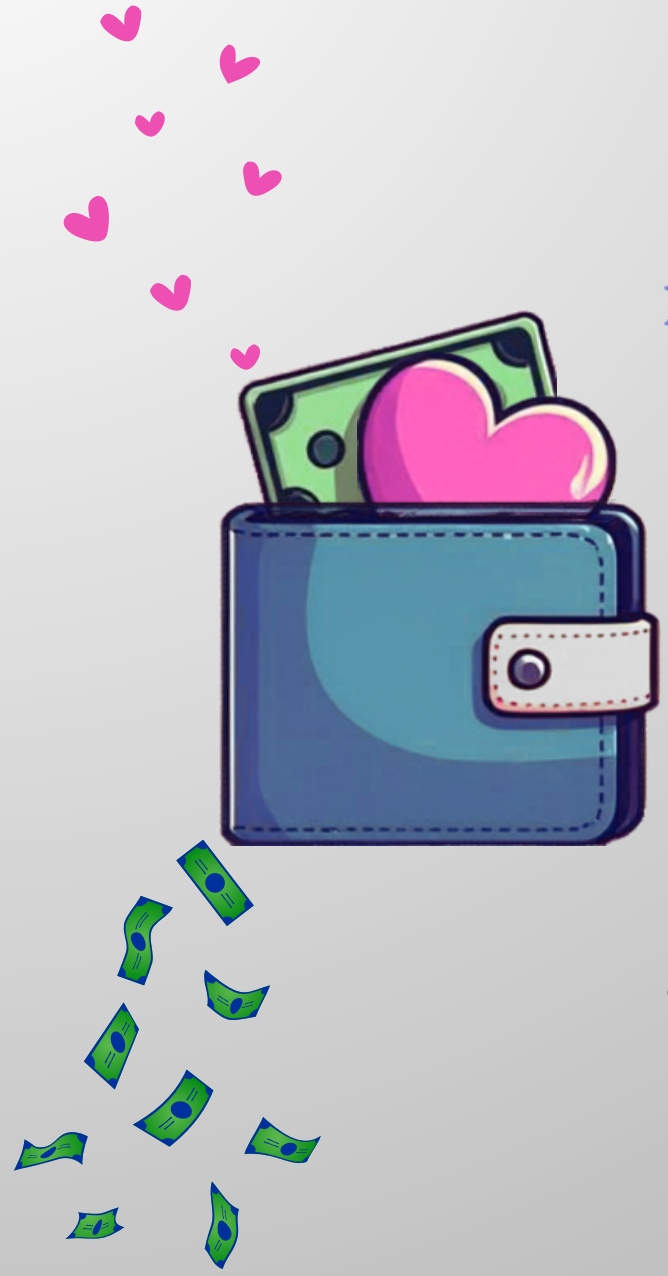
TIP: NEVER SHARE PERSONAL INFO

Remember - all data is valuable. The simplest fact can be used against you during a scam!



CREATED 03/11/2026 | J. FULLER

STAGES OF A ROMANCE SCAM:



Scammer makes contact

Friend requests, comments, private messages, emails, phone calls or letters

Switching Platforms

If met on legitimate website, they will likely attempt to move the conversation to another platform (WhatsApp, Telegram, etc.)

Trust & Love Bombing

The scammer showers the victim with declarations of love or flattery attempting to build a rapid emotional connection

Information Gathering

The scammer begins to gather information to identify vulnerabilities and financial capabilities

The Hook or Crisis

Scammer invents a sudden need for money; this could include an emergency or an unbelievable financial deal. If you don't comply, they use coercive tactics and guilt

Escalation & Continued Fraud

The scammer will make excuses about meeting in person or video chatting. They will use shame and embarrassment to continue financially extorting victims

CREATED 03/11/2026 | J. FULLER

POLICE
SCOTTSDALE
ARIZONA

HAVE YOU RECEIVED A MESSAGE WITH A LINK?

DON'T GET SCAMMED.

STOP. THINK TWICE. DELETE.

SCOTTSDALE PD 480-312-5000

UPDATED 04/15/2026 | J. FULLER

FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

CRYPTOCURRENCY TIPS FROM

DET. J. BRENNAN | CRYPTOCURRENCY EXPERT

SCOTTSDALE PD NON-EMERGENCY: 480-312-5000
EMERGENCY: 911

IT'S A SCAM IF:

- You get directed to WhatsApp or Telegram*
- If you are asked to open a crypto account on behalf of a person you think you are in a relationship with
- If you feel uneasy about any part of the process

**There are legitimate forms of WhatsApp and Telegram conversations, used to communicate between countries*

DO NOT:

- Wire money into a cryptocurrency account thinking you are investing in cryptocurrency

OR

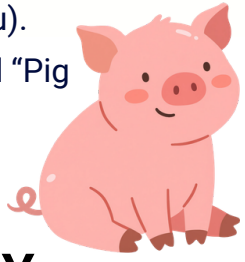
- Move money on behalf of another person - you could be money laundering or a money mule

NEVER:

- Wire money to another person or country thinking that you are 'mining' BTC as an investment.
- Download specific cryptocurrency apps that suspects are asking you to download

REMEMBER:

- Even if the suspect returns your initial investment with a percentage of earnings, they may be setting you up for a bigger investment and then never returning your money (ghosting you).
- This is called "Pig Butchering"



IMPORTANT!

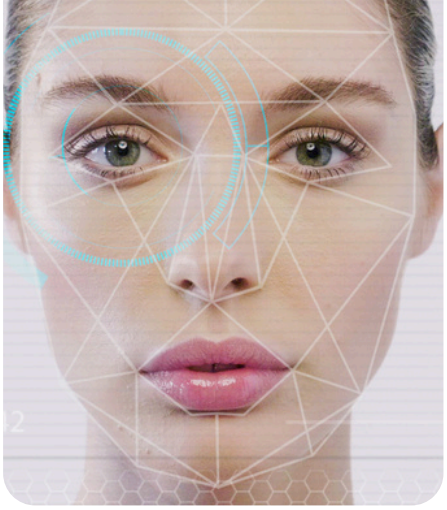
Do not give out any personal information over the phone.

Recently, there have been numerous Coinbase scams, of suspects pretending to be Coinbase representatives and convince you to transfer money out of your account because "it's not safe".

FINALLY:

- If you invest in cryptocurrency, it is imperative that you control the account, and the money at all times
- Trades must be facilitated by YOU
- If it is too good to be true - it is!

CREATED 04/15/2026 | J. FULLER

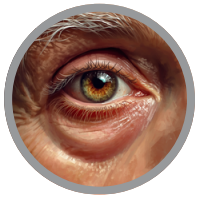


DEEPFAKE MEDIA SCAMS

& HOW TO SPOT THEM

Education is Prevention

Do your research, double check anything you see online... no matter how realistic!



Smoothed Skin & Blurry Features

Deepfake images and videos often have an "airbrushed" look to them. If the image looks too perfect - no blemishes or stray hairs, it is likely edited.

Inconsistent Lighting & Shadows

Videos and photos appear to "float" above surfaces without casting a shadow, or the lighting on the person's face does not match the rest of the picture. Zoom in for a deeper look.

Unnatural Movement

Check to see if the person is "blinking" too much, too little or not at all. Check for "glassy" stares or eyes that do not track naturally.

Audio & Video Inconsistencies

If the audio and video are out of sync, this could be a good indication the video is a deepfake. Watching the video slowed down can also reveal issues that were originally undetectable to the naked eye.

While deepfakes can be used for legitimate purposes (commerce, media, entertainment) they are commonly used in the exploitation of individuals.

Remember to be cautious online and question everything.

Additional Information:

- www.FBI.gov
- www.IC3.gov
- www.DHS.gov
- www.GAO.gov

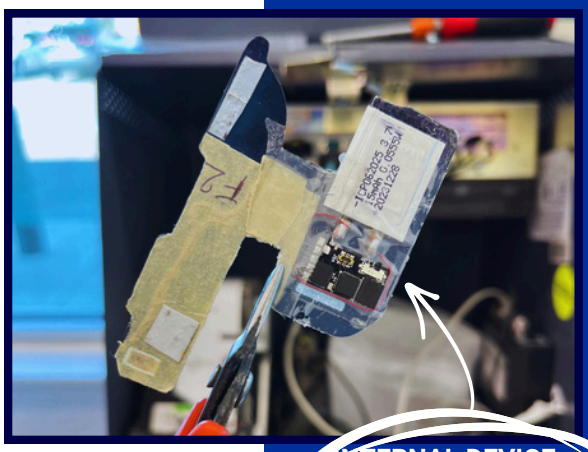
SCOTTSDALE PD
FINANCIAL CRIMES UNIT

CREATED 04/16/2026 | J. FULLER

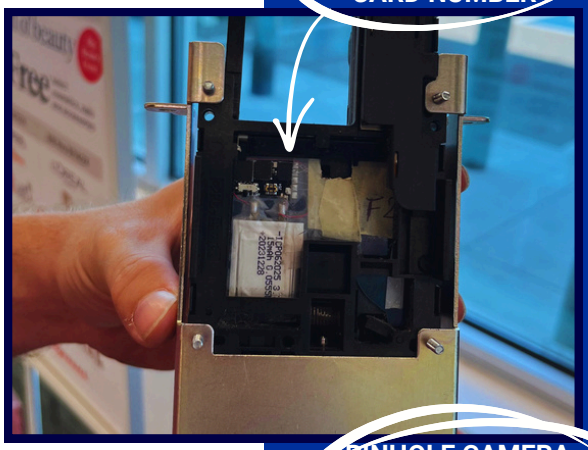
480-312-5000 (Non-Emergency)
@ scottsdalepd
www.scottsdaleaz.gov/police

SKIMMERS
& HOW TO SPOT THEM

WHAT IS A SKIMMER?
Skimmers are devices that are installed on ATMs or Point of Sale Machines which secretly record bank account data when the user inserts or swipes an ATM or EBT card into the machine.
Per the FBI, approximately 1 billion dollars are stolen via skimmers each year



WHERE ARE THEY FOUND?
The skimmer (which looks similar to the original card reader) fits over the existing card reader internally. A skimmer will curve outward and is removeable. There can also be hidden cameras or keypad overlays installed to capture your pin number.



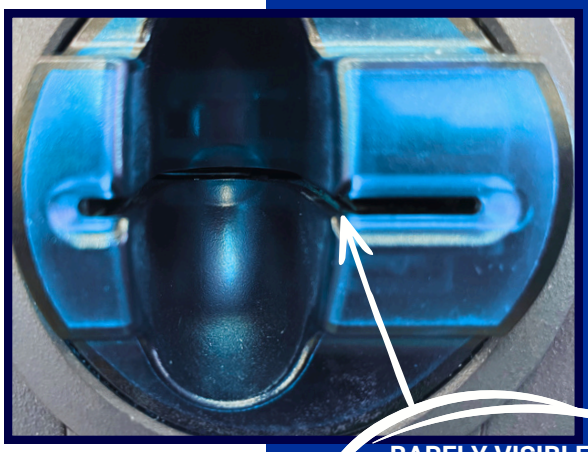
HOW TO SPOT THEM
Skimmers are NOT easy to spot. Inspect all ATMs before use. Check for anything damaged, loose or scratched. Pull at the edges of the keypad before entering your PIN (or do not enter your PIN at all). When possible, use “tap to pay”.

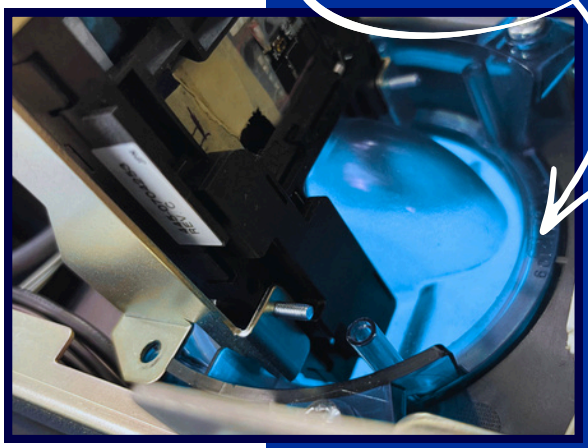
SCOTTSDALE PD
FINANCIAL CRIMES UNIT
CREATED 04/22/2026 | J. FULLER

SKIMMERS
& HOW TO PROTECT YOURSELF

TIPS:

- Inspect all ATMs and POS devices prior to use
- When possible, use ATMs in direct view of cashiers or gas station attendants
- Try to always use ATMs in well-lit or indoor areas
- Pay for gas in cash
- Avoid using your debit card PIN number - run it as credit instead
- If you need to use your pin, cover the keypad with your other hand
- Use “tap-to-pay” instead of inserting or swiping your card
- Keep an eye on your bank accounts
- Use a strong PIN - avoid PINs that are easily guessed (birthdays, 1234, etc.)
- If you suspect your card has been compromised - contact your financial institution ASAP





ONLINE RESOURCES:

- https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming
- https://www.secretservice.gov/investigations/skimming

SCOTTSDALE PD
FINANCIAL CRIMES UNIT
CREATED 04/22/2026 | J. FULLER

POLICE
SCOTTSDALE
ARIZONA

01. MARICOPA COUNTY OFFERS A FREE TITLE ALERT

Maricopa Title Alert is a free program which monitors and alerts subscribers when documents are recorded with the Maricopa County Recorder's Office under an individual and/or business' name. The program, which launched in June 2023, can help to monitor you and your business' name.

More than 92,900 Maricopa County residents currently have an account.

02. THE PROCESS:

Users can sign up in less than two minutes. All that is needed is a valid email address.

The user can select alerts for multiple names under a single email.

Users can monitor both personal names and business names.

03. AFTER SIGN UP:

Email Notifications and Document Review:
When a document is recorded that includes one of the entered names, Maricopa Title Alert will send an email notification with a link to review the recorded document.

04. SIGNING UP IS EASY

Visit the official website at:
TitleAlert.Maricopa.Gov

Created 04/16/2026 | J. Fuller

WHAT TO REPORT AFTER GETTING SCAMMED:

Scottsdale Police Department Non-Emergency: 480-312-5000
Emergency: 911

Date(s) of Fraud:

Time(s) of Fraud:

How Where You Contacted?
Examples: In-Person, Phone, Email, Etc.

Total Initial Loss:

Recovered Funds:

Information About the Scam:

"Company" Name(s)	Type of Scam:	Location of Scam:	Compromised Data:
Examples: "Chase" Bank, "Publisher's Clearing House"	Examples: romance, investment, tech support, etc.	Location of initial contact and/or locations directed to:	Examples: SSN, DOB, addresses, phone numbers, emails, etc.

Information About the Scammer:

Names of Scammer(s)	Contact Information:	Descriptions of Scammer(s)	Other Identifying Info:
Include the names of anyone you can remember:	Examples: phone numbers, email addresses, texts.	Examples: physical and/or voice descriptions.	Examples: usernames, account names, profile names, etc.

Financial Information:

Methods of Payment:	Banking Institutions:	Account Numbers:	Where Funds Were Sent:
Examples: cash, check, wire, crypto, mail, etc.	Examples: banks, payment apps, crypto companies	Examples: routing & account #s, debit/credit card #s	Examples: routing & account #s, payment apps (usernames)