Go-Crypto Fraud Evidence Checklist

A victim-friendly guide for organizing crypto scam, theft, and fraud evidence

IMPORTANT SAFETY WARNING

Do not send seed phrases, private keys, recovery words, passwords, two-factor codes, remote-access codes, or login credentials. Go-Crypto does not need those items to review transaction evidence. If a scammer is still communicating or pressuring you to send more money, stop responding and preserve the messages.

Purpose: Use this checklist to gather the information needed for a Go-Crypto review, attorney consultation, law enforcement report, exchange compliance request, or preservation request. The goal is to organize the case clearly: what happened, when funds moved, where the funds went, and what evidence supports the timeline.

How to use it: Complete what you can. Do not delay reporting because a section is incomplete. Save screenshots and files in a single folder, and keep original messages, receipts, emails, and transaction confirmations whenever possible.

1. Victim / Client Information

Basic contact information for the person reporting the fraud or the person assisting them.

Field	Information
Full name	
Phone	
Email	
City / State	
Best way to contact	
Attorney / helper name, if any	
Date checklist completed	

2. Quick Case Summary

Write a short summary in plain language. Include how the scam started, what the scammer promised, how funds were sent, and what happened when you tried to withdraw or recover funds.

How did first contact happen?: ____

What did the scammer or platform promise?:

____

Total estimated money sent: ____

Date first payment was sent: ____

Date fraud was discovered: ____

Is the scammer still communicating?:

____

Short narrative summary: ____

____

3. Urgent Safety Questions

These items help identify immediate risk and the safest next steps.

[ ] The scammer is still communicating or pressuring for more money.
[ ] The victim shared a seed phrase, recovery words, private key, password, or 2FA code.
[ ] The victim installed remote access software such as AnyDesk, TeamViewer, or similar tools.
[ ] The victim clicked links or downloaded files from Telegram, WhatsApp, email, or a fake support site.
[ ] There are still funds in a wallet or exchange account the victim controls.
[ ] The victim used a crypto ATM or kiosk.
[ ] The victim used Coinbase, Kraken, Binance, Crypto.com, Cash App, Robinhood, or another exchange.
[ ] The case involves an elderly person, vulnerable adult, repeat victimization, or threats.
[ ] A bank wire, Zelle, Cash App, gift card, check, or cash payment was also involved.
[ ] A police, FBI IC3, FTC, bank, or exchange report has already been filed.

4. Timeline of Events

List key dates in order. This timeline connects the off-chain story to the on-chain transactions.

Date	Event	Platform / App	Amount	Notes / Evidence File

5. Wallet Addresses and Transaction Hashes

Collect wallet addresses, transaction IDs, exchange withdrawal confirmations, and screenshots. Transaction hashes are often the most important evidence for tracing.

Type	Address / TXID	Blockchain	Who controlled it?	Notes
Victim wallet				
Scammer-provided address				
Exchange withdrawal TXID				
Fake platform deposit address				
Other related address/TXID				
Other related address/TXID				

6. Transaction Worksheet

For every transfer, list the date, asset, amount, USD value if known, sending service, receiving address, and transaction hash.

Date	Asset	Amount	USD Value	From	To	TXID / Confirmation

7. Exchange, Wallet, or Platform Records

Check every service used to buy, send, receive, store, or withdraw funds. Save account history, withdrawal history, receipts, support tickets, and confirmation emails.

[ ] Coinbase	[ ] Binance / Binance.US
[ ] Crypto.com	[ ] Kraken
[ ] Gemini	[ ] Cash App
[ ] Robinhood	[ ] Uphold
[ ] Trust Wallet	[ ] MetaMask
[ ] Phantom	[ ] Ledger / Trezor
[ ] Bitcoin ATM / crypto kiosk	[ ] Fake investment platform
[ ] DeFi platform	[ ] Other exchange or wallet

Account email or username used: ____

Exchange support ticket number(s):

____

Bank or card used to purchase crypto:

____

Crypto ATM or kiosk operator, if known:

____

8. Scammer Communications

Preserve the communication history. Screenshots are helpful, but exports are better when available. Keep profile links and usernames before accounts disappear.

[ ] Text messages	[ ] WhatsApp chat
[ ] Telegram chat	[ ] Facebook messages
[ ] Instagram messages	[ ] Email messages
[ ] Phone call logs	[ ] Voicemails or audio messages
[ ] Video call screenshots	[ ] Fake customer support chat
[ ] Screenshots of profile pages	[ ] Screenshots of threats, withdrawal demands, tax demands, or fee demands

Known names, aliases, phone numbers, emails, usernames, profile links:

____

____

____

9. Website, App, or Fake Platform Evidence

If a website, trading dashboard, wallet app, or fake exchange was involved, screenshot it before it disappears.

[ ] Website URL	[ ] Login page screenshot
[ ] Dashboard screenshot	[ ] Fake balance screenshot
[ ] Deposit page screenshot	[ ] Withdrawal denial screenshot
[ ] Tax / fee / verification demand screenshot	[ ] Terms or policy page screenshot
[ ] Customer support chat	[ ] Domain registration / WHOIS evidence, if available

Website / app name and URL: ____

10. Financial Loss Summary

Separate actual money sent from fake profits shown on a scam website. Only count money or crypto that actually left the victim's control as a loss.

Payment Type	Amount	Date Range	Evidence Available
Crypto sent			
Bank wire			
Debit/credit card			
Cash App / Zelle / PayPal			
Crypto ATM / kiosk cash			
Gift cards / checks / other			
Total estimated actual loss			

11. Reports Already Filed

Collect confirmation numbers, agency names, dates, and copies of any reports or complaint confirmations.

Report / Agency	Filed?	Date	Report Number / Contact	Notes
Local police / sheriff	[ ] Yes [ ] No			
FBI IC3	[ ] Yes [ ] No			
FTC	[ ] Yes [ ] No			
State attorney general	[ ] Yes [ ] No			
Bank fraud department	[ ] Yes [ ] No			
Exchange fraud/compliance team	[ ] Yes [ ] No			
Attorney	[ ] Yes [ ] No			

12. Evidence Folder Organization

Use a simple folder structure so the evidence can be reviewed quickly.

Folder Name	What to Put Inside
01_Case_Summary	This completed checklist, written summary, and timeline.
02_Transactions	TXIDs, exchange withdrawal confirmations, blockchain links, and transaction screenshots.
03_Exchange_Records	Account history, deposit/withdrawal history, receipts, and support tickets.
04_Communications	Chats, texts, emails, phone records, social media profiles, and scammer identifiers.
05_Website_App_Evidence	Fake website screenshots, dashboard screenshots, withdrawal denials, and support chats.
06_Financial_Records	Bank statements, card transactions, wires, kiosk receipts, gift card records, and loss summary.
07_Reports_Filed	Police reports, FBI IC3 confirmation, FTC complaint, bank reports, and exchange reports.

13. Final Review Before Sending

Before sending evidence to Go-Crypto, an attorney, or law enforcement, check the following.

[ ] I removed or redacted passwords, seed phrases, recovery words, private keys, and 2FA codes.
[ ] I saved original files where possible and did not delete scammer messages.
[ ] I included all known wallet addresses and transaction hashes.
[ ] I included screenshots or exports of scammer communications.
[ ] I included exchange withdrawal confirmations and crypto purchase records.
[ ] I included filed report numbers or confirmation receipts, if available.
[ ] I separated actual money sent from fake profits shown on a scam website.
[ ] I noted whether the scammer is still communicating or pressuring for more funds.

Go-Crypto Review Note

A complete checklist is helpful, but it is not required to start. If funds were recently moved, a wallet was compromised, or a scammer is still pressuring for more money, preserve what you have and seek help promptly.