Evidence Preparation Checklist

Keep original records and a clear account of where each item came from. This guide supports organization; it does not assess a claim or prescribe forensic handling.

Collect the records already available

[ ] **Communications**
Retain relevant emails, message exports, attachments, profile identifiers and contact details. Preserve context rather than relying only on selected screenshots.

[ ] **Platforms and representations**
Record exact website addresses, account identifiers, relevant terms, promotional statements and withdrawal conditions. Note when each item was captured.

[ ] **Payments and transactions**
Keep bank or exchange records and, where available, the date, time and timezone, asset, amount, network, transaction hash and sending and receiving addresses.

[ ] **Access and account events**
Record restrictions, support tickets, verification requests, suspected compromise and the sequence of provider notifications. Identify what you observed yourself.

[ ] **Existing complaints and reports**
Keep copies, submission dates, references and responses. Distinguish an authority report from a provider complaint or a privately commissioned technical report.

IC3 identifies cryptocurrency addresses, asset types and amounts, transaction hashes, dates and times as useful reporting information. Public reference: www.ic3.gov/CrimeInfo/Cryptocurrency

Keep the file usable

A simple index helps a reviewer connect a document to the event it supports, while making missing information visible.

Use an evidence index

[ ] **Reference and description**
Give each item a simple reference, such as E01, and a neutral description. Avoid a label that states a disputed conclusion as a fact.

[ ] **Date and source**
Record the document or event date, where the item came from and when you obtained it. Identify timezone and date estimates where relevant.

[ ] **Original and working copy**
Retain the original export or file. Make annotations on a separate working copy. Record any conversion or redaction you make.

[ ] **Why it matters and what is missing**
Link the item to a chronology entry or question. Mark incomplete conversations, missing attachments and uncertain attribution expressly.

A simple example

E01 | Exchange transaction export
Source: account download. Obtained: [date]. Relevant event: payment on [date]. Original retained: yes. Note: receiving-party identity remains unverified.

Before sharing

Share only relevant records through an agreed route. Do not send passwords, seed phrases, private keys or access codes. Keep a copy of what you submit and the receipt reference. Do not send additional funds or interact with a suspicious link simply to create more evidence.

Preparation does not replace individual advice

This checklist supports a free initial case review; no firm retainer is charged at that stage. It does not determine deadlines or establish misconduct. Any later representation requires checks and a written engagement after technical findings return. Obtain appropriate instructions before altering relevant systems or records.

Read more: cryptoslawyers.com/resources/evidence-checklist/
Contact: info@cryptoslawyers.com