# Go-Crypto

**Digital Assets Investigations**

A Non-Profit project of Go Mobile Education Zone

## Investigation Guide

# Crypto Scam, Fraud, & Theft Investigation Case Flow & Fee Guide

We help affected individuals document what happened, trace where the funds moved, identify investigative leads, and understand realistic next steps.

### On-Chain Asset Tracing

Follow stolen or fraudulently transferred digital assets through wallets, exchanges, bridges, swap services, DeFi protocols, and unresolved destinations across supported blockchains.

### Evidence & Records Review

Organize and review transaction hashes, exchange records, bank or wire records, screenshots, chat logs, emails, websites, and other available evidence.

### Payment & Platform Review

Reconstruct exchange purchases, wires, payment-app activity, deposits, fake platform records, withdrawal attempts, and other funding events connected to the scheme.

### Wallet & Service Identification

Identify recipient wallets, exchanges, bridges, swap services, payment processors, and other platforms that received or moved the funds.

### Investigation Reporting

Prepare clear findings, transaction tables, flow diagrams, service leads, limitations, and recommended next steps for the client or an authorized professional.

### Scam & Transaction Timeline

Place communications, payment requests, deposits, transfers, account changes, withdrawal attempts, and blockchain activity into a clear chronological sequence.

### Address & Asset Discovery

Identify additional wallets, tokens, counterparties, services, and transaction paths based by the known evidence and on-chain activity.

### Off-Chain Intelligence

Research domains, websites, usernames, social accounts, businesses, and public identifiers associated with the suspected scam or perpetrators.

### Seizure & Freeze Monitoring

Monitor traced transaction paths for new movement, publicly identified U.S. government seizure interactions, and observable stablecoin issuer blacklist or freeze events involving assets such as USDC or USDT.

**Purpose**

This guide is for individuals affected by cryptocurrency scams, fraudulent investment schemes, pig-butchering scams, phishing, account compromise, hacks, impersonation, or unauthorized transfers. It explains how Go-Crypto can organize available evidence, trace digital asset movement, identify wallets and service leads, monitor recovery-related events, and prepare clear investigative findings and realistic next steps.

# Case Flow: Intake, Screening & Scope Selection

The first objective in a digital asset investigation is to determine what the client needs answered, what records are available, what records are missing, whether blockchain tracing appears feasible, and which type of engagement is appropriate. Many crypto related concerns begin with incomplete information, early scoping helps distinguish confirmed activity from suspicion, identify the missing records needed to support analysis, and estimate the case complexity. The client does not need to know in advance which type of blockchain analysis, report format, or tracing method should be requested. The intake and screening process will be used to understand counsel's intended use of the findings to translate those objectives into a recommended investigation package.

### What the Intake Process Is Designed to Establish

By the time the engagement scope is finalized, the client should understand what questions the investigation will address, what evidence is required, which transactions and wallets are included, the selected report format, anticipated deliverables, fees, known limitations, and how additional work will be handled.

1. **Initial Inquiry & Scam Questionnaire**

   The client contacts Go-Crypto and completes an initial questionnaire describing what happened, details of initial contact with scammer or fraudulent platform, payment dates/amounts, known exchanges or wallets, scammer identifiers, available evidence, reports already filed, and the outcome the client hopes to achieve.

2. **Initial "Fit / Service-Matching" Call**

   Go-Crypto may arrange a complimentary call to clarify the scam, theft, or account compromise, review the available evidence, explain the investigation options, and better understand what the client hopes to learn or document. This helps match the matter to the most appropriate standard package or custom investigation.

3. **Preliminary Screening**

   When the nature or scale of the digital asset activity is unclear, Go-Crypto may conduct a limited preliminary review of available records, known wallet addresses, exchange activity, or other indicators. This screening is used to evaluate whether tracing appears feasible, identify obvious records gaps, estimate likely complexity, and recommend the appropriate next step. Depending on the matter, screening may be included as part of intake, offered as an introductory service, or separately scoped.

4. **Scope Finalization & Engagement Agreement**

   Based on the questionnaire, fit call, and any preliminary screening, Go-Crypto recommends either a standard package or victim can build a custom analysis package. The finalized scope will identify the selected report format, included analysis modules, anticipated deliverables, fees, deadlines, assumptions, known limitations, and any optional support services.

5. **Formal Records Intake & Investigation Launch**

   After engagement, the client provides the evidence required for the agreed scope. This may include transaction hashes, wallet addresses, exchange exports, bank or wire records, screenshots, chat histories, emails, website or domain information, usernames, account records, and previously filed police or fraud reports. Go-Crypto inventories the evidence, identifies missing information, and begins the agreed investigative work. Additional evidence or clarification may be requested as the investigation develops.

6. **Analysis & Report Delivery**

   Go-Crypto performs the selected analysis, reviews material transaction activity, reconciles findings against available records, documents confirmed and unresolved issues, and prepares the report.

7. **Findings Review & Optional Ongoing Support**

   After delivery, the client may schedule a review call to discuss the findings, assumptions, limitations, unanswered questions, records gaps, or potential next steps. Feedback or newly produced records may result in corrections, an addendum, or additional analysis.

   Ongoing services, such as additional tracing, report expansion, address monitoring, exhibit preparation, deposition support, or expert testimony may be added through a supplemental scope or separate engagement.

### Professional Limitation

Go-Crypto provides blockchain tracing, transaction analysis, digital asset documentation, records-gap review, monitoring support, and attorney-support reporting. Go-Crypto does not provide legal advice, determine marital property rights, make legal conclusions, guarantee recovery, or request passwords, seed phrases, private keys, or login credentials.

## Standard Investigation Packages

Go-Crypto offers standard investigation packages for commonly encountered digital asset matters. Each package combines a defined investigative focus, report format, starting scope, anticipated deliverables, and fee. Go-Crypto helps match the matter's questions, available records, deadlines, and intended use of the findings to the most appropriate option.

### 1 - Fraud Service Review - $1,000

**Description**: Answers the question: *"Am I being Scammed?!"*

| | |
|---|---|
| • Public Records Review: OSINT | 2 leads/identifiers/entities |
| • Communications Review | 2 leads/identifiers/entities |
| • Service Address Screening | 3 addresses |
| • Informational Findings Report | Fast / Raw |
| • Recommended next steps | |

### 2 - Asset Flows Exploration - $1,250

**Description**: Answers the question: *"What happened to my funds?!"*

| | |
|---|---|
| • Theft Transaction Trace | 5 transactions |
| • Informational Findings Report | Fast / Raw |
| • Recommended next step | |

### 3 - Incident Response - $3,500

**Description**: *Criminal incident response investigation with a formal report detailing the on-chain and off-chain aspects of the theft, including actionable recommendations.*

| | |
|---|---|
| • Theft Transaction Trace | 5 transactions |
| • VASPs Actionable Recommendations | All VASPs Identified |
| • Communications Review | 2 leads/identifiers/entities |
| • Public Records Review - OSINT | 2 leads/identifiers/entities |
| • Formal Investigative Report | Detailed / Legal & Police |
| • Recommended next step | |

### 4 - Full Blockchain Investigation Report - $5,000

**Description**: *Professional report intended for legal / law enforcement action against the perpetrators.*

| | |
|---|---|
| • Theft Transaction Trace | 5 transactions |
| • VASPs Actionable Recommendations | All VASPs Identified |
| • Communications Review | 2 leads/identifiers/entities |
| • Public Records Review - OSINT | 2 leads/identifiers/entities |
| • Vector of Compromise | 1 wallet |
| • Financial Records Review | 1 account/institution |
| • Scam & Transaction Timeline | 1 date range |
| • Formal Investigative Report | Detailed / Legal & Police |
| • Recommended next step | |

### Investigation Options

Go-Crypto offers two options for investigations, the above pre-configured packages and the following "Build Your Own Investigation" to enable counsel/clients to meet their specific unique needs. All investigations extend at the same rate as the "Build Your Own Investigation" options.

## Build Your Own Investigation

Some digital asset matters require a more tailored combination of investigative work, reporting, delivery, or ongoing support. The **Build Your Own Investigation** option allows counsel to configure the engagement around the specific questions, records, deadlines, and intended use of the findings.

**STEP 1** — **Report Format**
Choose how the findings are packaged and presented.

→ **STEP 2** — **Analysis Options**
Select the analytical work needed for the matter.

→ **STEP 3** — **Report Delivery**
Findings and investigation report review with counsel.

→ **STEP 4** — **Ongoing Services**
Add review calls, monitoring, deposition, or testimony support.

## Step 1 - Report Format: Same Analytical Standard, Different Packaging

### Formal Investigative Report - $1,500

Designed for matters where findings may need to be reviewed by counsel, law enforcement, courts, opposing parties, or forensic professionals.

This format may include additional case context, methodology, exhibits, findings structure, limitations, and suggested next steps. It is better suited for matters involving testimony preparation, litigation, or potential inclusion in formal proceedings.

### Informational Findings Report - $750

Designed for more direct delivery of the results without the deeper narrative structure and formality of a full investigative report.

This format is useful for early-stage review, narrower fact questions, or situations where counsel wants a faster and more economical delivery of the findings. It can later be expanded into a formal investigative report for an additional cost.

## **Step 2 - Analysis Options**: Select the Work Needed

The investigation services define what records, wallets, transactions, assets, platforms, or on-chain activity will be examined. Each service has a base fee and an included starting scope. When the matter requires more work than the base scope includes, only the affected service is extended according to the factors that drive that analysis.

| Analysis Module | Description | What It Covers | Extensions |
|---|---|---|---|
| Theft Transaction Trace<br>**$1,500** | Follows the theft transactions across supported chains and services to document hops, destinations, counterparties, and unresolved endpoints. | 5 transactions | $200 per additional transaction |
| Wallet & Portfolio Review<br>**$200** | Summarizes known holdings, cross-chain balances, portfolio value at requested snapshot dates, activity, services used, counterparties, and material inflows and outflows. | 5 wallets / 1 snapshot | $50 per additional wallet |
| Communications Review<br>**$200** | Review all communication between the victim and the suspected perpetrators, includeing messages, emails, and chat logs  to identify aliases, phone numbers, emails, websites, wallet addresses, exchange names, and instructions given to the victim. | 2 leads/identifiers/ entities | $50 per additional lead, identifier, or entity. |
| Service Address Red-Flag Screening<br>**$200** | Review addresses associated with the blockchain platform/project for illicit activity and other incidations of fraud / scams. | 3 addresses | $50 per additional address |
| Financial Records Review<br>**$200** | Reviews bank statements, exchange exports, tax records, screenshots, discovery responses, and financial disclosures to identify crypto-related activity, accounts, dates, amounts, and inconsistencies. | 1 account/institution | $200 per additional record set |
| Vector of Compromise<br>**$1,000** | Investigate and identify the suspected methods employed to compromise wallets, hack accounts, and conduct unathorized transactions. This may include phishing links, fake support contacts, Key loggers, wallet-drainer approvals, seed phrase exposure, account takeover, remote-access tools, etc. | 1 wallet | $500 per additional wallet |
| Use-of-Funds Analysis<br>**$500** | Examines how identified funds were used after entering the digital asset ecosystem, including transfers, trades, purchases, DeFi deployment, bridge activity, counterparties, and cash-out activity. | 1 wallet | $100 per additional wallet |
| Source-of-Funds Analysis<br>**$500** | Examines where identified digital assets or transaction funding originated by reviewing fiat deposits, exchange accounts, upstream wallets, counterparties, transfers, and supporting records. | 1 wallet | $100 per additional wallet |
| Scam & TransactionTimeline<br>**$350** | Organize transfers, swaps, communications, and other events such as laundering over time analysis against relevant dates. | 1 date range | Flat-rate base scope |
| DeFi Activity Review<br>**$1,000** | Reviews decentralized exchange swaps, bridges, staking, liquidity pools, lending and borrowing, vaults, governance participation, and other protocol activity. | 2 wallets | $100 per additional wallet |
| Public Records Review - OSINT<br>**$200** | Uses public-source research to identify ownership clues, entities, services, domains, usernames, business relationships, and other off-chain leads connected to the matter. | 2 leads/identifiers/ entities | $50 per additional lead, identifier, or entity. |
| VASPs Actionable Recommendations<br>**$100** | Provide additional actionable intelligence regarding VASP invovled in the case, including available contact information, legal or compliance reporting channels, applicable jurisdiction, and their known responsiveness to law-enforcement. | All identified in investigation | N/A |

| Analysis Module | Description | What It Covers | Extensions |
|---|---|---|---|
| VASP Notification Letters<br>**$200** | Send a formal notification letter to each VASP identified as having received funds connected to the victim's theft. The letter will identify the relevant transactions, explain the reported origin of the funds, and place the provider on notice that the associated assets may represent proceeds of fraud or theft. | All identified in investigation | N/A |
| Freeze & Seizure Connections Snapshot | Analyze the victim's stolen-asset transaction paths to identify potential connections to cryptocurrency seized or forfeited by government agencies. | Custom | Custom |
| Custom Analysis Request | Analysis requested by counsel that does not fit the other modules and/or analysis that requires custom approaches/constraints | Custom | Custom |
| Expedited Delivery | Priority scheduling and accelerated delivery for investigations requiring completion sooner than the standard turnaround. | Based on the requested deadline | N/A |

## Step 3 - Report Delivery: Choose How the Findings Are Communicated

After the report format and investigation services are selected, client determines how the completed findings should be delivered.

Findings may be delivered directly to client, coordinated with another professional involved in the matter, or provided through an agreed professional-partner or white-label arrangement. The scope can identify the intended recipients, branding and attribution, file formats, confidentiality requirements, communication responsibilities, and whether Go-Crypto will participate in review meetings or presentations.

### Standard Delivery: (included)

Report submitted to client for off-line review and clarifications.

### Full Delivery: $350

Report submitted to client for off-line review and clarifications.

- 1 video call explanation walk-through with Counsel/Law Enforcement/Client

### White-label Delivery: Inquire

Report submitted to client for off-line review and clarifications.

- 2 video call explanation walk-throughs with Counsel/Law Enforcement/Client
- Service Notification Letters
- White-label Arrangement

## Step 4 - Ongoing Services

The engagement may conclude with delivery of the selected report, or client may add support after reviewing the findings.

Optional services may include findings-review calls, report expansion or addenda, additional tracing, address and transaction monitoring, exhibit preparation, deposition support, or expert testimony support. These services can be included in the initial scope or authorized later if new records, questions, or transaction activity require follow-up.

| Support Area | Description |
|---|---|
| Follow-Up Consulting Support<br>**$250/hour** | Report walk-through with counsel or client, subpoena response review, updated wallet monitoring, additional tracing, preparation of exhibits, coordination with forensic accountants, or explanation of findings for mediation or settlement discussions. |
| Expert Witness / Deposition / Testimony Support<br>**$350/hour** | Consulting expert or expert-witness support at counsel's request, including plain-language explanation of blockchain tracing methods, transaction timelines, wallet activity, exchange interactions, and digital asset movement. |
| Wallet Monitoring<br>**$100/month** | This monitoring service observes publicly visible blockchain activity associated with specified cryptocurrency wallets. Using blockchain transparency tools, we track incoming and outgoing transactions and provide alerts. |

## Our Background

At Go-Crypto, we are teachers first. With 49 years of combined teaching experience, investigative knowledge, digital asset tracing skills, and the perspective of a U.S. Army veteran, our team is committed to helping victims, families, attorneys, law enforcement, and organizations understand blockchain fraud and what steps may come next.

## Our Team

### Reymundo Gómez

Senior Blockchain Investigator
Expert Witness & Forensic Analyst

Certified Anti-Money Laundering (CAMS)
Certified Cryptoasset AFC (CCAS)
ACI & CI (TRM Labs)
CRC / CCI / CCAI (Chainalysis)
Certified Blockchain Investigator (BIG)

Reymundo Gomez is a U.S. Army veteran, blockchain investigator, and expert witness specializing in digital asset tracing, cross-chain activity, DeFi, wallet attribution, and litigation support. His investigative work spans cryptocurrency theft, phishing, account compromise, investment fraud, divorce, bankruptcy, and corporate disputes. He translates complex on-chain evidence into clear, attorney-ready reports, visual exhibits, and testimony.

Reymundo@Go-Crypto.org
LinkedIn

### Reneé Gómez

Chief Product Officer
Crypto Tracing Analyst

Certified Blockchain Investigator (BIG) | OSINT | Blockchain Analysis

Renee Gomez is a certified blockchain investigator whose scientific background and experience teaching high school biology inform her careful, evidence-driven approach to digital asset investigations. Her strengths include meticulous records review, off-chain research, and connecting fragmented information into clear investigative leads. She is committed to making specialized investigative support more accessible to underserved individuals and communities.

Renee@Go-Crypto.org
LinkedIn

### Jannette Gómez

Chief Operations Officer
Blockchain Investigator

Certified Blockchain Investigator (BIG) | OSINT | Blockchain Analysis

Jannette Gomez holds a master’s degree in education and is a Texas-certified teacher with 34 years of teaching experience. As a Certified Cryptocurrency Investigator, she combines her background in education with specialized digital asset knowledge to help attorneys, individuals, and organizations better understand cryptocurrency activity, blockchain tracing, and fraud-related concerns.

Jannette@Go-Crypto.org
LinkedIn

### Next Step

To discuss whether crypto asset review or blockchain tracing may be appropriate for your investigation, contact Go-Crypto to schedule a Fit / Service Match call.