Yes. A person who has credible information about sanctions evasion involving cryptocurrency can report it. Depending on the facts, the conduct may also involve violations of the Bank Secrecy Act (BSA), money laundering laws, or other financial crime rules. Employees and contractors may have information that is not visible to regulators from public blockchain data alone: for example, internal messages about a customer's location, decisions to ignore a sanctions alert, or records showing that a crypto business continued processing transactions after identifying a prohibited party.

But not every compliance failure is a crime, and a report is not the same as a finding of guilt. The distinction between an honest mistake and deliberate evasion matters. So do the evidence, the reporting route, confidentiality, retaliation risk and timing. This article explains the practical issues for people considering a disclosure in the United States. It is general information, not legal advice about a particular case.

What sanctions evasion involving crypto can look like

Sanctions evasion is not limited to a direct transfer to a person or organisation on a sanctions list. Crypto can be used to obscure who controls a wallet, move value through intermediaries, or disguise a transaction's geographic connection. Relevant conduct might include processing transactions for a blocked person, helping a customer conceal their identity or location, or knowingly routing funds through wallets or services to avoid screening.

For example, a crypto exchange employee might see an internal alert linking a customer's wallet to a sanctioned entity, then receive instructions to close the alert without investigation. Alternatively, a business might repeatedly serve customers in a prohibited location after staff have documented reliable location indicators. Those facts could justify scrutiny. They do not, by themselves, establish that a particular person or company committed an offence.

Crypto transactions leave records on public blockchains, but those records do not necessarily show who controlled a wallet, what a business knew, or why a transaction was approved. Internal customer files, screening results, case notes and communications may help explain those questions. That is one reason a whistleblower's first-hand information can be important to crypto enforcement and wider efforts to counter financial crime.

BSA violation or compliance mistake?

The BSA requires covered financial institutions and other regulated businesses to maintain specified anti-money laundering controls, keep certain records and file reports when required. Which obligations apply depends on the organisation and its activities. A crypto business's legal status and obligations can be fact-specific; not every crypto company is subject to the same rules.



A missed alert, late filing or incomplete case note may reflect a control failure, inadequate training, a system problem or human error. It is not automatically a deliberate BSA violation. A serious assessment asks what happened, what the relevant rule required, who knew what and when, and whether the organisation corrected the problem.

Evidence of possible willful misconduct may include repeated decisions to bypass controls, instructions to suppress alerts, falsified records, or continued processing after responsible staff raised specific concerns. A dated message saying "do not file this because the customer is important", for instance, has a different significance from a one-off alert incorrectly closed by an employee who promptly escalated the error. Context matters: even an apparently strong document may have an innocent explanation, and a compliance lapse can still merit internal or regulatory attention without proving criminal intent.

Do not try to make the case stronger by guessing at intent or labelling conduct "fraud" without support. Describe the transactions, control failures and communications you actually observed. Regulators can assess whether the facts suggest a BSA lawyer-monthly offence, a sanctions violation or another issue.

Where can a whistleblower report?

The right route depends on what you know and what outcome you are seeking. Potential channels include the US Treasury Department's Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), or another relevant regulator or law-enforcement agency. A concern may involve more than one authority. Use official agency channels and check their current instructions; a general website or regulator contact page is not necessarily a formal whistleblower submission portal.

The Federal Financial Institutions Examination Council (FFIEC) website is a useful starting point for information about the US federal financial regulatory system and examination resources. It is not, by itself, a general whistleblower filing service. A person considering a report should identify the agency with jurisdiction over the conduct and confirm how that agency accepts information.

Some qualifying disclosures concerning BSA violations may be eligible for protections or awards under federal whistleblower provisions. Eligibility depends on statutory requirements and the information provided; a person should not assume that every report, or every crypto-related concern, qualifies. For a practical discussion of bringing an AML/BSA whistleblower claim, see the National Law Review and search its site for its article on filing an

AML/BSA whistleblower lawsuit. Read any article alongside current statutes, agency guidance and advice from a lawyer familiar with whistleblower law.

Evidence and documentation that can hold up

A useful report is specific, organised and grounded in information the reporter lawfully possesses. The goal is to help an investigator understand what happened without overstating what the records prove. A transaction hash may show movement of digital assets; it may not establish the identity or intent of the person behind a wallet. Pair technical details with the business records or firsthand observations that explain their significance.

Preserve records in their original form where lawful and safe to do so. Do not access systems without permission, alter files, take customer data beyond what you are authorised to handle, or remove privileged, classified or otherwise restricted material. Before copying or transmitting internal information, get legal advice about confidentiality, privacy, employment agreements and applicable reporting protections. Never put yourself or another person at risk to gather evidence.

What to write down

- **Dates and times:** when the transaction, alert, conversation or decision occurred, including the time zone if known.
- **Transaction identifiers:** wallet addresses, transaction hashes, amounts, assets, exchanges and relevant account or case references.
- **What you observed:** distinguish firsthand knowledge from information you heard from someone else or inferred from a record.
- **People and roles:** identify relevant decision-makers and witnesses by role, and note how you know their involvement.
- **Control and response:** describe the alert, policy, escalation, approval, filing or failure to act, and any corrective steps.
- **Supporting records:** note where a record is kept and its date, such as a SAR log entry, screening result, case note, ticket, email or chat.
- **Uncertainty and alternatives:** record what you do not know and any plausible explanation that may need checking.

For example, “On 14 March, I reviewed case 4821. The screening system matched wallet X to a listed entity. I escalated the match to my manager in the compliance ticket. The ticket was closed the following day with the comment ‘clear for commercial reasons’. I do not know who controlled the wallet” is more useful than “management helped criminals”. Keep contemporaneous notes securely, with dates, and do not rewrite them later as if they were made at the time.

Timing and limitation periods: why waiting can matter

There is no single limitation period for “reporting crypto sanctions evasion”. Different rules may apply to the underlying conduct, a civil or criminal enforcement action, a whistleblower award, or a retaliation claim. Applicable time limits can depend on the alleged offence, the date conduct occurred or was discovered, and statutory exceptions. A general criminal limitation period is not a safe deadline for every sanctions or BSA matter.

Retaliation claims can have particularly short procedural deadlines. Under federal BSA whistleblower provisions, the process and time to pursue a retaliation claim depend on the applicable statute and circumstances. Do not assume

you can wait until an internal investigation ends, or until you have a complete case file, before seeking advice. An employment decision, threat or other adverse action may start a clock. Promptly record what happened and when, and speak to a lawyer about the deadline that applies to you.

Timing also matters for evidence. Crypto businesses may change systems, retain records for limited periods, or reorganise teams. A regulator may be better able to trace a transaction while exchange records, account details and internal communications remain available. On the other hand, rushing to submit an unverified accusation can harm your credibility and expose you to avoidable risks. Seek confidential advice early, preserve lawful records, and avoid delaying simply to build a perfect narrative.

Anonymous or identified submission?

Some whistleblower programmes allow a person to submit information anonymously through an attorney, subject to programme-specific requirements. In some processes, the person's identity must be disclosed to the agency before an award can be paid or another step can be completed. Anonymous reporting is not universal, and a tip sent without identifying details may be difficult to investigate or may not qualify for particular protections or rewards.

An identified submission can make follow-up questions easier and may help investigators assess the reporter's access to the information. It can also increase concerns about workplace retaliation, confidentiality and personal safety. Anonymity may reduce immediate exposure but cannot guarantee that colleagues will not infer who made the report from the facts or timing. Do not assume that a report to an employer, a regulator or a public tip line has the same confidentiality rules.



Before choosing, consider whether you need advice about eligibility for a whistleblower award, how to protect your identity, and what to do if your employer learns of the disclosure. An attorney can explain whether a specific programme permits an anonymous submission through counsel and what information must be provided. Avoid sharing sensitive details in public posts or with people who do not need to know.

Retaliation risk and practical safeguards

Retaliation may include dismissal, demotion, reduced responsibilities, threats, exclusion from work or other adverse treatment linked to protected reporting. Protections are fact- and statute-specific; they do not make every

workplace dispute a retaliation claim. Keep a dated record of relevant events, including performance reviews, changes to duties, manager communications and the dates of internal or external disclosures. Preserve material lawfully and store personal notes somewhere secure.

If you face an immediate threat, prioritise safety and seek appropriate support. If you experience adverse treatment, consult a lawyer promptly rather than relying only on an internal grievance process. Internal reporting may be useful in some circumstances, but it can also create risks or affect timing. Get advice on the order and method of disclosure before notifying managers, especially where they may be involved in the conduct.

A careful report is more useful than a dramatic one

Whistleblowers can help expose sanctions evasion tied to crypto, but a credible report is built from verifiable facts, not conclusions. Separate a human error from evidence of willful misconduct; identify dates, transactions and decisions; and explain the limits of what you know. Use the FFIEC site as a source of regulatory context, not as a filing portal, and confirm the current procedures of the agency that may have jurisdiction.

Most importantly, do not let uncertainty about the perfect channel or a complete evidence file cause you to miss a deadline. Get independent legal advice early about the applicable reporting route, anonymity, confidentiality, award eligibility and retaliation protection. That is especially important when a report concerns live sanctions evasion, ongoing transactions or a workplace decision that may trigger a short time limit.