Reporting suspected financial crime can help regulators uncover money laundering, fraud, sanctions evasion, and other misconduct. But a report is not more useful just because it sounds dramatic. Investigators need specific, reliable information they can assess and, where appropriate, verify.

That distinction matters for people considering a whistleblower submission to the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN). FinCEN awards are real, but they are not quick payouts. A strong submission can take time to review, investigate, and connect to an enforcement action. And even a well-supported tip does not guarantee an award.

Here are common mistakes people make when reporting financial crime—and how to avoid them.

1. Treating speculation as evidence

Suspicious behavior and proven misconduct are not the same thing. A company moving money between accounts, serving customers overseas, or having complicated ownership may raise questions. By itself, none of that proves money laundering or another crime.

Speculation becomes a problem when a reporter presents a hunch as a fact: "They must be laundering money" is less useful than "On these dates, these payments moved through these accounts, and this is why the transaction pattern appears inconsistent with the stated business." The second version gives investigators something concrete to evaluate.

Separate what you personally observed from what you inferred. For each concern, ask:

- What happened, and when?
- Who was involved, as far as I know?
- What record or firsthand observation supports this?
- What part is my interpretation rather than a confirmed fact?

Do not fill gaps with confident language. If you do not know who controlled an account, say so. If you suspect a transaction was designed to evade reporting, explain the facts behind that suspicion instead of presenting intent as established.

2. Submitting a report with a lack of documents—or no map to them

A report does not need a massive file dump to be useful. But a lack of documents, dates, transaction details, or other ways to check the account can make an allegation difficult to investigate.

Useful supporting material may include transaction records, invoices, internal messages, contracts, account information, or a clear chronology. A short explanation of what each item shows can be more helpful than hundreds of unlabeled files.

Preserve materials you are legally entitled to access. Do not break into systems, bypass access controls, take records you are not authorized to possess, or alter files to make a point. Do not expose customer information publicly. Financial records can contain sensitive data, and mishandling them can create new legal and privacy problems.

Before submitting, make a simple evidence index. Note each item's date, source, relevance, and whether it is an original or a copy. Keep an unaltered copy where you are permitted to do so. If you have no documents, give

investigators the best leads you can: dates, locations, systems, transaction identifiers, and names of people who may have firsthand knowledge.

3. Sending a pile of material without explaining the pattern

More information is not automatically better. A collection of screenshots and spreadsheets without context can bury the key fact. Investigators need to understand what you think happened and how the records support that account.

Start with a concise chronology. For example: "Between March and June, the company received payments from three entities, transferred most of the funds to a newly opened account, and recorded the transfers as vendor expenses. The attached ledger and invoices show the dates and amounts." That is a lead, not a verdict. It tells a reviewer where to look.

Then explain the roles of the people and entities involved, how you know those roles, and what remains uncertain. Flag the strongest evidence rather than asking a reader to discover the important detail in a large attachment set.

4. Repeating already-known allegations as if they are new

Already-known allegations can be a major weakness. If a regulator has already received the same information from another source, repeating it without adding meaningful new facts may do little to advance an investigation.

That does not mean a person should stay silent whenever a company has been criticized publicly or investigated before. New evidence, firsthand detail, or an explanation of a previously misunderstood transaction can matter. The practical question is: what does this submission add?

Do not assume that a news article, lawsuit, or social-media post proves a regulator already has the underlying evidence. But do not assume the opposite either. Identify what is publicly known, then clearly describe what you can add: records, specific transactions, people involved, or information that helps test the allegation.



For example, a post on Facebook accusing a business of fraud is not proof of fraud. An article on Tycoonstory.com may be useful background or a lead, but a published claim is not a substitute for transaction records or firsthand knowledge. Treat media and social posts as sources to check—not as a conclusion to copy into a tip.



5. Assuming every financial business is covered—or that only banks matter

The Bank Secrecy Act (BSA) is not just a rulebook for traditional banks. Its coverage reaches a range of financial institutions and businesses, with obligations depending on the type of entity and activity. Covered entities can include money services businesses, broker-dealers, casinos, and other categories, alongside banks.

That breadth matters because financial crime can move through different channels. A reporter who assumes "it isn't a bank, so the BSA cannot apply" may overlook a relevant compliance obligation. The reverse mistake is just as risky: not every company that handles money is automatically subject to the same BSA requirements.

Be precise about the business, service, and conduct at issue. A money transmitter, for instance, is not the same as a bank, even though both may have BSA-related obligations. Describe what the entity does and what you believe it failed to do. Avoid declaring a legal violation unless you can support the facts; regulators assess how the law applies.

6. Expecting an award to be automatic or fast

FinCEN whistleblower awards are real. The legal framework was strengthened through the Anti-Money Laundering Whistleblower Improvement Act of 2022, which improved the program's funding structure and protections. The award provisions operate within the broader framework established by the Anti-Money Laundering Act of 2020, enacted in 2021.

For qualifying information that leads to a successful enforcement action with more than $1 million in monetary sanctions, the statutory award range is generally 10% to 30% of collected monetary sanctions. That range is not a guaranteed share for every person who submits information. Awards are discretionary and depend on factors such as the information's significance and how much it contributed to the result.

Here is the catch: a tip can be valuable without leading to a qualifying action, and an enforcement action can take years. An award process may involve additional review after sanctions are collected. Do not make financial plans around a possible award, and do not confuse "I reported it" with "I qualify."

Also, do not assume the same rules apply to every regulator or every type of claim. The relevant agency, the nature of the conduct, the information provided, and the outcome all matter. Read current FinCEN program materials before filing, and keep a copy of what you submit and any confirmation you receive.

7. Disclosing protected information in the wrong place

Some financial reports, including Suspicious Activity Reports (SARs), are subject to strict confidentiality rules. Do not post a SAR or information that identifies its existence on Facebook, send it to journalists, or include it in a public campaign. Sharing protected information can create serious problems and may compromise an investigation.

If you work at a financial institution, check the rules that apply to your role and to the records you can access. Internal reporting channels may be relevant, but they are not automatically a substitute for an external whistleblower submission. Keep confidential information limited to appropriate channels and follow the submission instructions for the agency involved.

8. Overstating your role, certainty, or the outcome

Credibility is an asset. Saying "I reviewed tycoonstory.com the records" when you only saw a screenshot, or "the company committed money laundering" when you have evidence of unusual transactions, weakens a report. So does claiming that a regulator has confirmed wrongdoing when no such confirmation exists.

Use careful labels: "I observed," "the record shows," "I was told," and "I suspect." Identify the source of secondhand information. Correcting a mistake early is better than defending an inaccurate detail later.

A practical pre-submission checklist

1. **State the conduct plainly.** Describe what happened without using a legal label as a substitute for facts.
2. **Build a timeline.** Include dates, amounts, accounts or entities, and the sequence of events where known.
3. **Separate facts from speculation.** Mark what you witnessed, what records show, and what you infer.
4. **Organize supporting material.** Create an index and explain what each document demonstrates.
5. **Identify what is new.** Explain how your information differs from public allegations or anything already reported.
6. **Protect sensitive information.** Do not publish confidential records or disclose SAR information improperly.
7. **Check the right channel and rules.** Review current agency instructions, eligibility requirements, and confidentiality protections.

Common mistake More useful approach Calling a suspicious pattern proof of a crime Describe the transactions and explain why they raise a concern Sending unlabeled files Provide a chronology and a short evidence index Repeating an online accusation Identify firsthand facts or records that add something new Expecting a fast award Understand that eligibility, impact, collection, and timing all matter

Bottom line

A strong financial-crime report is specific, honest about uncertainty, and supported by information investigators can check. The most common mistakes are not knowing the right legal phrase. They are relying on speculation, submitting a lack of documents or context, repeating already-known allegations without adding evidence, and expecting an award to arrive quickly or automatically.

Before filing, get precise answers to practical questions: What information can I lawfully share? Which agency's program fits the conduct? What makes my information new? What records support each key claim? Those questions produce a better report than a dramatic headline—or a confident accusation on social media.