You do not need to understand an entire money-laundering scheme to report information that may help authorities. If you saw only one transaction, handled one account, or heard a limited conversation, you can still describe what you know. The key is to be precise about what you observed, distinguish it from what someone told you, and avoid filling gaps with guesses.

A useful tip is not the same as a complete investigation. It gives FinCEN or other authorities concrete facts they can assess, such as dates, people, businesses, accounts, transactions, records, and the limits of your knowledge. You can say plainly that your information is partial.

This article explains FinCEN's role, basic Bank Secrecy Act (BSA) and Suspicious Activity Report (SAR) concepts, examples of potentially reportable conduct, and ways to prepare a clear tip. It is general information, not legal advice. If you are considering a submission and have confidentiality, employment, safety, or document-access concerns, speak with a qualified lawyer—ideally one experienced in whistleblower matters—before sending sensitive material.

What Is FinCEN, and What Does It Do?

The Financial Crimes Enforcement Network, or FinCEN, is a bureau of the U.S. Department of the Treasury. It administers important parts of the BSA, collects and analyzes financial information, and makes information available to appropriate law-enforcement and regulatory authorities. The BSA framework helps the government detect and investigate money laundering, terrorist financing, and other financial crimes.

FinCEN is not the only agency that may handle information about suspected financial misconduct. Depending on the facts, other federal or state authorities may have a role. FinCEN's whistleblower program page describes the program and its submission process. Review the current instructions at fincen.gov/whistleblower-program before taking action, because requirements and procedures can change.

A FinCEN tip is not a court filing, a public complaint, or a finding that someone committed a crime. It is information for authorities to evaluate. A submission does not mean an investigation will be opened, that enforcement action will occur, or that a whistleblower award will be paid. Avoid anyone who promises a guaranteed award or a particular outcome.

BSA and SAR Reporting Basics

What the BSA requires

The BSA and its implementing regulations impose recordkeeping and reporting duties on certain financial institutions and other covered businesses. Depending on the institution and activity, those duties can include keeping specified records, verifying customer information, monitoring activity, and filing reports such as Currency Transaction Reports (CTRs) or SARs.

These are generally institutional obligations. A bank employee or customer is not automatically responsible for filing a SAR just because they notice something unusual. An individual with relevant information may be able to provide it to authorities through an appropriate reporting channel, but should not assume that a personal tip replaces a covered institution's compliance duties.

What a SAR is—and is not

A SAR is a confidential report that a covered financial institution files when it identifies activity that meets applicable reporting criteria. A SAR reports suspicion; it is not proof of a crime. Financial institutions generally cannot tell a person whether a SAR has been filed, and SAR information is protected by strict confidentiality rules. Do not try to obtain, copy, or disclose a SAR or related confidential information unless you have clear legal authorization.

As an individual, you may describe conduct you believe is suspicious without claiming to know whether a SAR was filed. For example, you could write, “I observed repeated cash deposits at three branches followed by same-day wire transfers,” rather than, “The bank filed a SAR,” unless you have a lawful, reliable basis for that statement.

What Conduct May Be Reportable?

Potentially relevant conduct may involve suspected violations of the BSA or other laws within the scope of the whistleblower program. The facts matter: an unusual transaction is not automatically illegal, and a pattern that looks suspicious to one person may have a lawful explanation. Report what you can support and let authorities assess it.

Example of conduct Useful details to describe Transactions appear structured to avoid reporting or recordkeeping requirements Dates, amounts, locations, accounts or entities involved, and what makes the pattern appear deliberate Funds move through multiple accounts or businesses without an apparent business purpose Known account holders, transfer dates, amounts, counterparties, and the records or conversations supporting your understanding Customer or transaction information may have been falsified or concealed What information you saw, who created or changed it, when, and how you know A covered business may have ignored or concealed suspicious activity Specific instructions, monitoring failures, escalation decisions, or records you personally encountered Transactions may involve proceeds of fraud, sanctions evasion, corruption, or other crime The underlying facts you know, the suspected connection, and which parts are inference or information from others

These examples are not a checklist of legal conclusions. If you do not know whether an activity violated a specific rule, say so. A careful description of facts is more useful than confidently naming an offense you cannot substantiate.

How to Prepare a High-Quality Tip When Your Information Is Partial

1. Start with a short, factual summary

In a few sentences, explain what you believe may have happened, where and when it occurred, and why you have relevant information. State your connection to the events—for example, whether you worked in a particular role, handled a transaction, reviewed a record, or received a report from someone else. Do not imply that you witnessed the whole scheme if you did not.

2. Separate firsthand knowledge from hearsay

Clearly label the source of each important fact. “I saw” or “I reviewed” should mean you personally observed the event or record. “A colleague told me” identifies information you heard from someone else. Include the person’s role and when the conversation occurred if you know those details. If you cannot identify the source or verify the statement, say that too.

Type of information Clear way to describe it Firsthand observation “On May 12, I processed a wire transfer for $48,000 from Account A to Company B.” Record you reviewed “I reviewed a spreadsheet dated June 3 that listed four transfers. I did not create the spreadsheet.” Information from another person “On June 10, a coworker told me the customer had requested that the payment be split. I did not hear that request myself.” Inference or uncertainty “I do not know why the payments were split. The similar amounts and timing led me to question whether they were related.”

It is fine to identify gaps. You might know the sender but not the beneficial owner, or see a transfer but not know where the funds went next. Say what you know, what you do not know, and what could help verify the information. Do not turn an inference into a fact.

3. Build a simple timeline and identify the people and entities

List significant events in chronological order. Include dates or date ranges, amounts and currencies, locations, account or transaction references, and names or business names as you know them. Distinguish confirmed details from approximations. If you are uncertain about a date or amount, mark it as an estimate rather than presenting it as exact.

Explain how each person or entity fits into the events, but avoid guessing at someone’s role. If you know a company received a payment but do not know who controlled it, state that limitation. A concise timeline is often easier to assess lexinter.net than a long narrative with repeated or conflicting details.

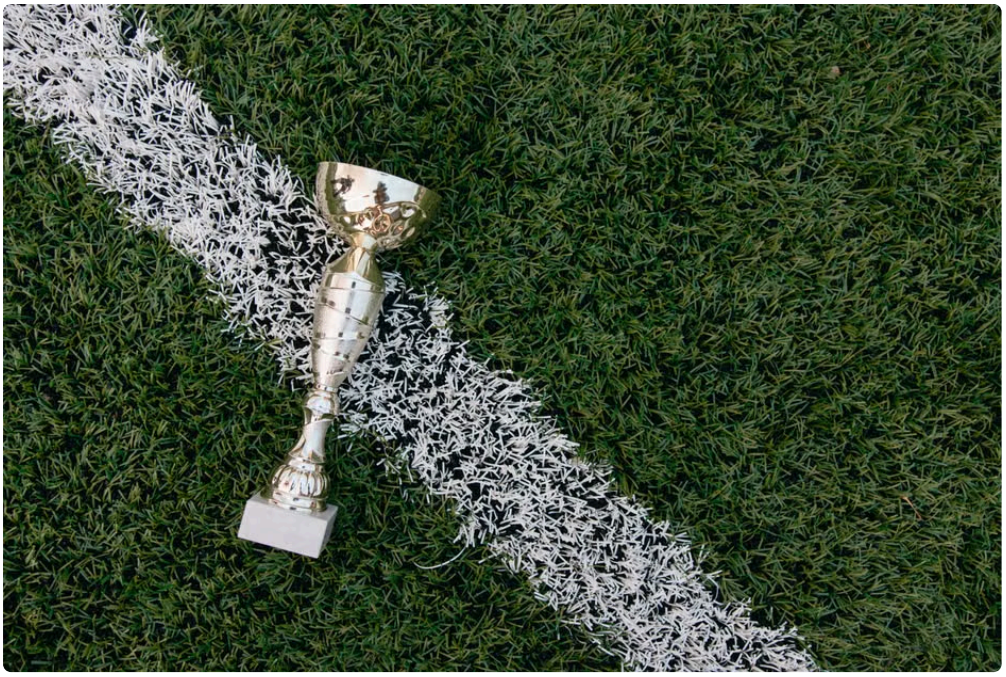
4. Identify records and possible witnesses without overcollecting

Tell authorities what evidence may exist, where it is kept, and who may have firsthand knowledge. Examples include transaction records, emails, internal messages, customer files, invoices, or meeting notes. You can describe a document without attaching it if you are unsure whether you may lawfully share it.

Do not access systems you are not authorized to use, take records you are not permitted to retain, alter files, or forward confidential information to a personal account without legal advice. Before sharing sensitive material, consider who will receive it, how it will be transmitted, and whether you have authority to disclose it. A lawyer can help assess confidentiality, privilege, trade-secret, privacy, and retaliation concerns.

5. Explain what you did and did not do

State whether you participated in any relevant conduct, what your role was, and what you did after becoming concerned. Be truthful and complete. Do not delete messages, change records, coordinate accounts with potential witnesses, or make accusations to people who may destroy evidence or put you at risk.



6. Use the current program instructions and consider counsel

Read the current FinCEN whistleblower program materials before submitting. If you are considering an award claim, reporting information through counsel may be important; confirm the applicable requirements with a lawyer rather than relying on a general article. Counsel can also help you understand identity and confidentiality issues, submission procedures, and how to describe your role accurately. “Follow up through counsel” does not mean a lawyer can guarantee confidentiality or an award; ask what protections and limits apply to your specific situation.



Keep a paper trail: Maintain a secure, lawful record of when you sought advice, what you submitted, and any acknowledgment or reference number you receive. Do not keep copies of sensitive company or customer information merely for your own records if you are not authorized to do so. Ask counsel how to preserve a record of your reporting without creating additional access or confidentiality problems.

A Practical Tip-Preparation Checklist

1. **Summarize:** What may have happened, where, and when?
2. **Identify your source:** What did you personally see, review, or hear—and from whom?
3. **Mark uncertainty:** What is an estimate, inference, or unverified statement?
4. **Map the activity:** Which people, businesses, accounts, transactions, or locations are involved?
5. **Point to evidence:** What records or witnesses may confirm or clarify the facts?
6. **Protect information:** Are you authorized to access and share each item? How will it be transmitted?
7. **Review the rules:** Check FinCEN's current program page and consult counsel when appropriate.

Keep a paper trail: Save your own notes and communications about the reporting process in a secure place, subject to your legal obligations and counsel's advice. Record the date and method of any submission, but do not create unauthorized copies of underlying records.

Training and Further Resources

FinCEN's whistleblower program page is the primary place to check current program information and instructions: fincen.gov/whistleblower-program. For broader AML and BSA education, ACAMS offers training resources at acams.org. Training can help explain financial-crime concepts, but it does not replace legal advice about your submission or your access to records.

The Bottom Line

You can provide useful information even if you saw only part of a suspected scheme. Describe what you observed, separate firsthand facts from what you heard, identify what remains unknown, and point to records or witnesses that could help verify the account. Avoid unsupported conclusions, protect sensitive information, and use counsel when confidentiality, employment, or award eligibility questions matter. A partial, carefully qualified account is more useful than a complete-sounding story built on assumptions.