A useful whistleblower tip is not the most dramatic account. It is an account that helps reviewers distinguish what you personally observed, what records show, and what someone else told you. Mixing those categories can weaken an otherwise credible submission, obscure the facts that matter, and make it harder for investigators to assess your information.

If you are considering reporting a possible violation of the Bank Secrecy Act (BSA), take time to organize what you know before submitting it. Separate firsthand facts from secondhand statements, tie claims to dates and documents where possible, and be clear about what you cannot verify. This article explains how FinCEN fits into the process and how to prepare a careful, credible tip. It is general information, not legal advice.

What FinCEN Is—and What It Does

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury. It administers the BSA, collects and analyzes certain financial information, and shares financial intelligence with authorized law-enforcement and regulatory partners. Its work helps authorities detect and investigate activities such as money laundering and other financial crimes.

FinCEN also administers a whistleblower program under the Anti-Money Laundering Act. The program may provide an award to a person who voluntarily supplies original information that leads to a successful enforcement action and meets the statutory requirements. An award is not guaranteed. Eligibility, the value of the information, the outcome of an action, and other legal requirements can all matter.

For current program details, review FinCEN's official Whistleblower Program page. If you are considering reporting information connected to your job, a lawyer familiar with whistleblower matters can help you understand confidentiality, eligibility, and how to submit information safely.

BSA and SAR Reporting Basics

The BSA and its implementing rules require certain financial institutions and other covered businesses to maintain records, establish anti-money-laundering controls, and report specified activity. Requirements vary by institution and circumstance. A possible lapse in a control or a suspicious transaction is not, by itself, proof that a violation occurred.

One important BSA report is a Suspicious Activity Report (SAR). Covered institutions file SARs when they know, suspect, or have reason to suspect activity that meets applicable reporting criteria. A SAR is a report made by an institution; it is not a finding that a customer committed a crime. Law enforcement and regulators where to report money laundering use SAR information alongside other evidence.



SARs are subject to strict confidentiality rules. Do not try to obtain a SAR you are not authorized to access, copy or disclose one without proper authorization, or tell a subject that a SAR was filed. If you encountered SAR-related information through work, get legal advice about how to handle it. You can describe facts you personally observed without assuming that a SAR exists or disclosing protected information.

What May Be Reportable?

The whistleblower program concerns potential violations within the scope of the governing law, including certain BSA-related violations. The right question is not simply, “Did something look suspicious?” It is whether the information may show conduct that violates a legal or regulatory obligation. FinCEN and other authorities assess the facts; a tipster should report what they know rather than declare a legal conclusion.

Examples of conduct that could warrant closer review, depending on the facts, include:

- A covered institution repeatedly failing to investigate or report activity that appears to meet applicable SAR requirements.
- Employees or managers allegedly interfering with required monitoring, reporting, recordkeeping, or internal controls.
- Records being altered, concealed, or created to make a compliance process appear to have occurred when it did not.
- A pattern of transactions apparently structured to evade reporting or recordkeeping requirements, especially where records or communications show awareness of the pattern.
- A compliance program that appears ineffective in practice, supported by specific evidence such as repeated unresolved alerts or documented management decisions.

These are examples, not findings or a complete list. Context matters. A transaction may have an innocent explanation, and a control failure may have more than one cause. Avoid presenting suspicion as established fact.

Separate Firsthand Facts from What You Heard

The most important discipline is to label the source of each claim. A firsthand fact is something you personally saw, did, received, or heard directly. Secondhand information is something another person told you. An inference is your interpretation of facts. Keeping those categories distinct makes your account easier to evaluate.

Category Example phrasing What to clarify Firsthand observation “On March 12, I reviewed the transaction log for account ending 4821.” What you actually saw, when, and in what role. Documented fact “The email dated March 14 states that the alert was closed without further review.” Where the record came from and whether you have lawful access to it. Secondhand statement “A colleague told me on March 18 that the same issue affected another team.” Who told you, when, and whether you independently verified it. Inference or suspicion “I believe the repeated closures may indicate a control problem.” The facts supporting your interpretation—and other plausible explanations.

Use direct language. Write “I saw,” “I reviewed,” or “I was told,” as applicable. Do not change “a colleague said the manager knew” into “the manager knew.” Do not state that a transaction was money laundering unless you have a basis for that conclusion and clearly explain it as a concern, not a proven fact.

How to Handle Rumors

A rumor is not automatically useless, but it should not be presented as verified evidence. If it may point investigators toward a person, event, or record, identify it as unverified and explain its source as specifically as you safely can. If you do not know who originated it, say so. If it is not relevant or cannot be checked, consider leaving it out.

Be especially cautious with claims about intent, secret agreements, or what senior leaders “must have known.” Those claims are easy to overstate and hard to support. Instead, describe the conduct and communications you actually observed, then explain why they raised a concern.

Prepare a High-Quality Tip

A well-organized submission gives reviewers a path to check the account. Before submitting, build a short chronology and connect each important claim to its source. Include uncertainty rather than hiding it. Do not pad the account with speculation, repeated allegations, or conclusions you cannot support.



1. Make a dated chronology

List events in order, using exact dates when you know them and clearly marking estimates. Include the people or business units involved, what happened, and how you learned about it. If dates conflict across records, note the discrepancy instead of silently choosing one.

2. Identify records without over-collecting

For each key event, note whether a record exists, such as an email, transaction log, policy, meeting note, or audit finding. Describe the record's date, type, and location if appropriate. Do not access systems outside your authorization, remove records you are not permitted to take, or send sensitive files through an unsecured channel. Consider confidentiality, privilege, privacy, and company policies before sharing materials. A lawyer can advise on safe handling and submission.

3. Be precise about what you know

For every material statement, ask: Did I see this myself? Did I hear it directly? Did someone tell me? Is it an inference? What supports it? If you cannot answer, label the gap. "I do not know whether a SAR was filed" is more credible than guessing.

4. Explain why the conduct may matter

Briefly state the requirement or control you believe may be implicated, if you know it, and explain the factual basis. You do not need to write a legal brief. Avoid asserting that a violation is certain; the authorities determine whether the conduct violates the law.

5. Keep a paper trail

Keep a secure, lawful record of your own reporting steps: when you made a submission, what confirmation you received, and which materials you provided. Do not create a duplicate archive of confidential institutional records or retain material you are not allowed to keep. Record your own actions and preserve communications about the process in a way that respects access rules and legal advice.

Credibility of Submission: A Practical Checklist

Before sending a tip, review it for accuracy and clarity:

- **Separate firsthand facts:** Have you distinguished what you personally observed from what you heard?
- **Use dates and documents:** Are key events tied to dates, records, or clearly identified sources?
- **Mark uncertainty:** Have you labeled estimates, rumors, and inferences rather than stating them as fact?
- **Avoid exaggeration:** Have you removed unsupported claims about intent, scale, or senior-level knowledge?
- **Provide useful context:** Can a reviewer understand who was involved, what happened, and why it raised concern?
- **Protect sensitive information:** Have you considered whether you are authorized to access and share each item?
- **Keep a paper trail:** Have you noted your submission date and retained confirmation, without improperly retaining protected records?

Use Reliable Resources and Get Advice When Needed

FinCEN's Whistleblower Program page is the primary place to check current program information and submission instructions. Follow the official instructions rather than relying on an old checklist or an unofficial summary. For broader AML and BSA education, ACAMS offers training resources. Training can help explain compliance concepts, but it does not replace legal advice about your situation.

If you are unsure whether information is protected, whether you may share a document, or whether your role affects eligibility, consult a qualified attorney before submitting sensitive material. Do not assume that an award is guaranteed or that a particular timeline applies. The strongest starting point is a careful, factual account: what you saw, what you heard, what the records show, and what remains uncertain.