You do not need to identify a statute or regulation before you raise a concern about possible financial misconduct. In many cases, the most useful first step is to **describe conduct clearly**: what happened, when it happened, who or what was involved, and why it seemed unusual. You can share facts without deciding for yourself whether they amount to a violation.

That does not mean every suspicious transaction is illegal, or that every tip will lead to an investigation or an award. Financial activity can look unusual for innocent reasons, and **investigators assess relevance** by comparing the information with applicable laws, records, and other evidence. If you are considering a report, a **talk to legal professional** conversation may help you understand your options, confidentiality concerns, and any risks tied to your role or the information you have.

What Is FinCEN?

The Financial Crimes Enforcement Network, commonly called FinCEN, is a bureau of the U.S. Department of the Treasury. It administers the Bank Secrecy Act (BSA) and works to protect the financial system from illicit use, including money laundering and the financing of terrorism. FinCEN also collects, analyzes, and shares financial intelligence with law enforcement and other authorized partners.

FinCEN's work includes setting and administering requirements for certain financial institutions, receiving reports required by law, issuing guidance, and supporting investigations. It is not a general-purpose court or a hotline that decides, from a short description alone, whether a person committed a crime. Information may be considered alongside other records and reports.

FinCEN's whistleblower program provides a channel for people to submit information about certain possible violations and may provide awards when statutory requirements are met. The rules, eligibility criteria, procedures, and award determinations can be specific and may change. Review the current information directly on the FinCEN Whistleblower Program page before deciding how to proceed. An award is not guaranteed.

BSA and SAR Reporting Basics

What the BSA does

The Bank Secrecy Act is a U.S. framework of laws and regulations designed to help authorities detect and deter money laundering and other financial crime. Pretty simple.. It requires covered financial institutions and certain other businesses to maintain records, establish compliance programs, and submit particular reports when applicable. The exact obligations depend on the institution, activity, and governing rules.

BSA-related obligations can include customer identification and due diligence, transaction monitoring, recordkeeping, and reporting. A person who notices a possible breakdown in one of these areas may not know which rule applies. That is a reason to report the underlying facts carefully—not to guess at a legal conclusion.

What a SAR is—and is not

A Suspicious Activity Report (SAR) is a report that a covered financial institution or other reporting entity may be required to file with FinCEN when it detects activity meeting applicable reporting standards. A SAR is

a lead for authorities; it is not a finding that a customer or employee committed a crime. A SAR may describe activity that has a lawful explanation, and filing one does not by itself prove wrongdoing.

Members of the public generally do not file a SAR as if they were a bank. Instead, someone with relevant information may use an appropriate reporting channel, such as FinCEN's whistleblower program when the information and circumstances fit its requirements, or contact an appropriate law-enforcement or regulatory agency. Which route is suitable depends on the facts and the person's situation.

SARs and related information can be subject to strict confidentiality rules. Do not ask a bank employee to disclose a SAR, try to obtain one without authorization, or circulate documents that may contain protected information. If you have access to sensitive records through work, consider getting legal advice before copying, forwarding, or uploading anything.

What Can Count as a Reportable Violation?

Ever notice how "reportable" depends on the program's rules and the underlying facts. You do not have to settle that question before describing what you know. The examples below are general illustrations of conduct that may raise BSA-related concerns; they do not establish that a law was broken.

Conduct you may observe Why it may raise a question What to describe Repeated transactions just below an internal or legal reporting threshold Some patterns may suggest an effort to avoid reporting or monitoring, though there may be an innocent explanation. Dates, amounts, locations or channels, accounts if lawfully known, and the pattern you noticed. Customer activity that appears inconsistent with information the institution has about the customer It may raise questions about due diligence, monitoring, or whether the activity has been adequately understood. What information was available, what activity differed, and how you know each point. Possible failures to follow internal escalation or reporting procedures A repeated or deliberate failure may be relevant to an institution's compliance obligations. The procedure you believe applied, what happened instead, and whether you observed it directly. Use of shell companies, nominees, or complex transfers that obscure who controls funds These arrangements can have legitimate uses but may also conceal ownership or the source or destination of funds. The entities, transfers, dates, and specific facts that make the arrangement concerning. Instructions to alter, omit, or avoid documenting transaction information Such instructions may raise questions about recordkeeping, reporting, or efforts to evade controls. Who gave the instruction, the words used as accurately as possible, when it occurred, and any witnesses.

These examples are not a checklist for labeling customers or coworkers. A large cash transaction, an international transfer, or a complicated ownership structure is not automatically unlawful. Context matters. Focus on specific behavior and records rather than assumptions about a person's identity, nationality, occupation, or appearance.

How to Prepare a High-Quality Tip

A useful tip is clear, specific, and honest about uncertainty. You do not need to sound like a lawyer or use technical terminology. The goal is to help a reviewer understand what may have happened and how the information can be checked.

1. **Separate what you saw from what you heard**

   State whether you personally observed an event, reviewed a record you were authorized to access, or learned something from another person. Use phrases such as "I observed," "I reviewed," and "A

colleague told me." If you do not know whether a statement is accurate, say so. Do not present hearsay as firsthand knowledge.

2. **Build a factual timeline**

   List dates or date ranges, the sequence of events, and the people or business units involved, to the extent you know them. If a date is approximate, label it as approximate. A short chronology is often easier to assess than a long, unstructured narrative.

3. **Explain the concern without declaring guilt**

   Describe what seemed unusual and why. For example, rather than writing "the bank committed money laundering," explain that you saw a series of transfers between specified accounts, describe their timing and amounts, and note any instructions or missing review steps that concerned you. Let reviewers assess which rules may apply.



4. **Identify possible supporting information**

   Note the types of records that may help verify the account, such as transaction dates, internal messages, audit entries, or policy versions. Explain where those records may be located and who may have access. Do not obtain records by bypassing controls, accessing accounts without permission, or asking someone else to do so.

5. **Be precise about gaps and limits**

   Say what you do not know: for example, whether a transaction was reported, who ultimately controlled an entity, or whether an exception was approved. A candid account of limits helps reviewers weigh the information and identify what would need to be verified.

6. **Check the reporting channel and protect sensitive material**

   Use the current instructions on the relevant agency's official website. Before submitting sensitive documents, consider whether you are authorized to share them, whether they contain customer or

employee information, and whether you can use a secure channel. Do not send confidential material to an address or person whose authority you have not verified.

7. **Keep a paper trail**

   For your own process, keep a secure record of when you sought advice, which public instructions you reviewed, and what you submitted or were asked to provide. Do not retain, copy, or remove protected business records just to create your own file. Ask a legal professional how to preserve relevant information lawfully, especially if you are an employee or have confidentiality obligations.



Practical Questions to Ask Yourself

- What did I personally observe, and what did someone else tell me?
- What are the dates, amounts, entities, or actions I can describe accurately?
- Which details are facts, and which are my interpretation?
- What records might confirm the information, and am I authorized to access or share them?
- Could sharing this information expose customer data, confidential business information, or my identity?
- Have I checked the current official reporting instructions and considered speaking with a legal professional?

Training and Legal Guidance

If you need to learn more about anti-money laundering concepts, ACAMS offers training resources and professional education on AML and financial-crime compliance. These materials can help explain terminology and common controls, but training is not a substitute for legal advice or an official determination about a particular report. See ACAMS for current resources.

If you are deciding whether to submit a tip, how to handle workplace records, or how a report may affect you, talk to a legal professional familiar with whistleblower matters, financial regulation, or employment issues. A lawyer can help you assess the right channel and the limits on what you may disclose. Do not

assume that every reporting route offers the same **lexinter.net** confidentiality protections or that your identity will always remain unknown.

The Bottom Line

You can raise a concern without knowing the exact law that may have been broken. Start with what you know, distinguish firsthand observations from information you heard, explain the pattern that concerns you, and be candid about what remains uncertain. Avoid legal labels you cannot support, protect sensitive information, and use official reporting instructions. The agency or other authorized reviewers—not the tipster—assess whether the facts are relevant to a possible violation.

Keep a paper trail of your reporting process, but do so without improperly retaining or disclosing records. And if the decision involves confidential information, employment concerns, or potential legal exposure, talk to a legal professional before taking the next step.