A first meeting with a whistleblower attorney is usually a fact-finding conversation, not a test. You do not need to prove a violation or arrive with a perfect legal theory. ...where was I?. Your goal is to help the lawyer understand what happened, when it happened, what records may support your account, and what risks you face.

If your concern involves bank secrecy or anti-money-laundering requirements, the details matter. A missed control, a troubling customer, or a disagreement about policy is not automatically a legal violation. The lawyer will need to assess the institution's duties, the facts you personally know, and whether the information may qualify for a government reporting or award program.

This guide explains what to prepare, how to protect sensitive information, and what questions to ask a lawyer. It is general information, not legal advice about your situation.

Start With a Clear Timeline

Make **timeline notes** while your memory is fresh—ideally the same day something happens. Record dates, approximate times, people involved, what you observed, and what you did next. Separate what you saw firsthand from what someone else told you or what you inferred.

A useful entry might say: "On March 4, I reviewed a transaction-monitoring alert for Customer A. The alert showed repeated cash deposits at three branches. I escalated it to my manager through the case system. On March 8, the case was closed. I do not know whether a SAR was filed." That is more helpful than "Management covered up money laundering," unless you have evidence supporting that conclusion.

Include both events that support your concern and facts that may cut the other way. For example, note whether you know of a later review, remediation, or explanation. Avoid guessing about motives. "The case was closed" is an observation; "they closed it to protect a customer" is a conclusion unless you have evidence for it.

What to include in your timeline notes

- When you first noticed the issue and when each important event occurred.
- The roles or names of people involved, if you know them.
- The system, team, product, branch, or process involved.
- What you did, including reports to a supervisor, compliance, or another channel.
- Any response you received, including dates and the method of communication.
- Possible witnesses and where relevant records may be stored.
- Any employment actions or pressure you experienced after raising a concern.

Mark estimates as estimates. If you are unsure whether something happened on Tuesday or Wednesday, say so. A careful account is more useful than false precision.



Prepare a Key Documents List—Not a Secret File Dump

Bring a **key documents list** that describes relevant records and where usattorneys.com you believe they are kept. You do not need to walk into the consultation with a large collection of employer files. In many cases, a short index is safer and more useful than copying documents without advice.

Examples of records that may matter include policies, training materials, audit or quality-review findings, escalation records, transaction-monitoring case histories, emails or messages you are authorized to access, meeting notes, and records showing when a concern was raised or resolved. Explain what each item may show and whether it is an original, a personal note, or a summary.

Record category What to note for the attorney Important caution Policies and procedures Document title, version date, and the requirement you think may be relevant Do not take restricted copies without legal advice Case or alert records System name, case number if known, dates, and your role Do not access records outside your normal authorization Internal reports or messages Who received the report, when, and how the issue was described Preserve context; do not edit or selectively alter records Personal notes When you made them and whether they were written at the time Keep observations separate from later recollections

Do not email work documents to yourself, upload them to a personal cloud account, or use a personal device to bypass company controls. Records may contain customer information, SAR-related information, privileged material, or other confidential data. Rules about what you may retain or share depend on the facts and the law. Ask the attorney how to handle records before moving or copying them.

In particular, SAR information is subject to strict confidentiality requirements. Do not disclose the existence or contents of a SAR to a person who is not authorized to receive it. Tell the attorney, at a high level, if your concern involves SAR handling, and ask how to discuss the issue safely.

Understand the BSA Duties at Issue

The Bank Secrecy Act (BSA) and its implementing regulations impose obligations on covered financial institutions and certain other businesses. They do not make every employee personally responsible for every compliance outcome. It's not always that simple, though. A lawyer will want to identify the institution, the

applicable duty, the facts indicating a possible failure, and whether the issue is a legal violation rather than simply a poor decision or internal disagreement.

Suspicious Activity Reports (SARs)

Covered institutions must have processes to identify and report certain suspicious activity. The reporting rules depend on the institution and the type and circumstances of the activity; there is no single SAR rule that applies identically to every business or transaction. A concern might involve whether suspicious activity was recognized, investigated, escalated, or reported as required. But a SAR decision may involve judgment, and an employee generally will not know every fact or whether a filing occurred.

Do not assume that a customer's activity was reportable simply because it looked unusual. Bring the underlying facts, the applicable procedure if known, and what you personally observed. Do not try to confirm a confidential filing by asking unauthorized people or searching systems you are not permitted to access.

Currency Transaction Reports (CTRs)

CTRs generally concern reportable cash transactions over the applicable threshold, commonly more than $10,000 in currency for a covered financial institution, subject to regulatory rules and exceptions. Potential issues may include missed reporting, inaccurate information, or conduct designed to evade reporting requirements. The facts matter: a transaction's form, timing, customer, and possible related transactions can all be relevant.

Customer Due Diligence (CDD)

CDD requirements generally involve understanding customer relationships, assessing risk, and conducting ongoing monitoring appropriate to the institution and customer. Depending on the covered entity and circumstances, beneficial ownership requirements may also be relevant. A weak customer file or an unresolved question is not automatically a violation. Explain what information was required, what was missing or inconsistent, and how the institution responded.

AML program effectiveness

Covered institutions are generally expected to maintain an anti-money-laundering program with required elements, such as internal controls, independent testing, a designated compliance officer, and training, as applicable to the institution. A program can have flaws without every flaw amounting to a reportable violation. The legal analysis may turn on whether required controls were absent or ineffective, whether known problems were ignored, and what the institution did after learning about them.

What Might Qualify as a Reportable BSA/AML Violation?

A potentially reportable matter may involve a breach of a specific BSA duty or regulation, such as failures in required reporting, recordkeeping, customer due diligence, or an AML program. Other facts could raise concerns about deliberate evasion, concealment, retaliation, or repeated control failures. Those labels should not replace evidence. Calling something "fraud" without identifying the legal duty and supporting facts can make an account less clear.

For the consultation, describe the conduct in plain terms. What requirement do you believe applied? What did the institution do or fail to do? When? Who knew? What records or witnesses might confirm it? Be candid

about uncertainty and alternative explanations. Pretty simple.. The attorney—not the employee—can assess which laws and reporting routes may fit.

Original Information and Eligibility Basics

Some whistleblower programs require information that is original, meaning it comes from the person's independent knowledge or analysis and is not already publicly known or merely copied from another source. The precise definition, exclusions, filing requirements, deadlines, and potential award rules depend on the program and current law. Employment in compliance, audit, or legal roles can raise additional eligibility questions, but it does not automatically answer them.

The Financial Crimes Enforcement Network (FinCEN), a bureau of the **U.S. Department of the Treasury**, administers BSA-related functions and has a whistleblower process. A **FinCEN whistleblower submission form** is one agency process referenced in this area. Do not assume that submitting a form guarantees an award, protects every disclosure, or satisfies every deadline. Ask a lawyer to verify the current requirements and whether your role or how you obtained the information affects eligibility.

Do not make a public post or send detailed allegations broadly before getting advice. Premature disclosure can create confidentiality, employment, privacy, or eligibility complications. If you have already reported internally or to an agency, bring the dates, confirmation numbers, and copies of what you submitted if you are allowed to retain them.

Internal Reporting and Retaliation Concerns

Bring a record of any use of **internal compliance channels**, such as a hotline, compliance portal, supervisor escalation, or written report. Note whether the report was anonymous, what it said, and what response followed. Internal reporting may help establish notice and the sequence of events, but whether it is required or affects eligibility depends on the applicable program and facts.

If you fear retaliation, write down what happened and when: changes to duties, performance reviews, threats, exclusion from meetings, discipline, or termination. Keep this factual. Do not secretly record conversations without first checking the law and getting legal advice; recording rules vary by location and circumstance.

Questions to Ask a Lawyer

Use the consultation to assess both the legal issues and whether you can work comfortably with the attorney. You can bring this **questions to ask lawyer** list and add your own:

- Which BSA or other legal duties might apply to the facts I described?
- What facts are missing, and what should I avoid doing while you assess them?
- Could my role, access to information, or prior reporting affect eligibility?
- Which reporting options may be available, and what deadlines or sequencing issues should I know about?
- How should I preserve my own notes and identify relevant records without improperly taking or accessing company material?
- What confidentiality protections apply to our conversations, and are there limits?
- How do you handle possible retaliation or employment issues?

- Do you have experience with FinCEN or other whistleblower matters involving financial institutions?

Ask Clearly About Contingency Fees and Costs

Some whistleblower lawyers work on a contingency-fee basis, meaning the attorney's fee is tied to a recovery or award rather than billed in the usual hourly way. The terms vary. Ask what percentage applies, whether it changes at different stages, which costs may be deducted, who pays costs if there is no recovery, and whether you could owe anything if you end the representation.

Ask for the fee agreement in writing and take time to read it. A contingency arrangement does not mean the lawyer can guarantee an award or a particular timeline. Agency reviews and investigations can take a long time, and the lawyer may not be able to share updates about confidential government activity.

How to Choose and Prepare for the Meeting

Look for counsel with relevant whistleblower and financial-regulatory experience, and ask how the attorney evaluates conflicts and confidentiality. USAttorneys.com may help you research lawyers or locate legal resources, but a directory listing is not an endorsement or a substitute for checking experience, licensing, and fit directly with the lawyer.

1. Write your timeline notes and mark what you know firsthand.
2. Prepare a key documents list without taking or transmitting restricted files.
3. Bring a short list of people, systems, and reporting channels that may be relevant.
4. Write down your questions to ask lawyer, including fee and confidentiality questions.
5. Tell the attorney about any prior internal or agency reports and any urgent employment concerns.

You do not have to solve the case before the first meeting. A careful timeline, a focused documents list, and honest answers about what you know—and do not know—give the attorney a sound place to begin. If something important happens after the meeting, make timeline notes that same day and ask counsel how to handle any related records or communications.

