If you suspect a Bank Secrecy Act (BSA) or anti-money laundering (AML) failure, the first challenge is often not deciding whether something feels wrong. It is recording what happened in a way that is accurate, useful and safe to preserve—without breaching customer confidentiality, taking restricted files or unnecessarily increasing your retaliation risk.

There is no method that guarantees you will not be fired. But careful documentation can help distinguish a genuine compliance concern from an ordinary mistake, preserve a reliable timeline and support a conversation with a lawyer or regulator. The goal is not to build a dramatic case. It is to make a clear, dated record of what you observed, what you did and how the organisation responded.

Start by separating a BSA concern from a mistake

Not every late filing, incomplete alert or missed escalation is evidence of a BSA violation. People make errors, systems fail and procedures may be unclear. A single mistake that is promptly identified, corrected and documented may call for remediation rather than an allegation of deliberate misconduct.

A more serious concern may arise where facts suggest a recurring or knowing failure—for example, alerts repeatedly closed without required review, transaction-monitoring controls knowingly disabled, or senior staff directing employees not to escalate suspicious activity. Context matters. So do the applicable legal requirements, the institution's procedures and the quality of the evidence.

In practical terms, ask yourself:

- **What was required?** Identify the relevant law, regulation, written procedure or control, if you can do so from materials you are authorised to access.
- **What actually happened?** Describe the specific transaction, alert, filing, instruction or control failure—not just that "AML was ignored".
- **Was it corrected?** Record any remediation, escalation or repeat occurrence you personally know about.
- **What suggests knowledge or intent?** Note direct instructions, repeated conduct after warnings, or records showing a decision to bypass a control. Do not assume intent simply because an outcome was poor.

This distinction matters. Human error may still require correction and reporting under internal procedures, but it is not automatically willful misconduct. Conversely, describing an issue as a "mistake" does not make it harmless if evidence shows a deliberate or repeated disregard of obligations.

Build a reliable record with dated personal notes

Keep dated personal notes as soon as you can after relevant events. Write in plain, neutral language. Separate what you saw directly from what someone told you, and distinguish facts from your interpretation. A useful entry might say: "On 12 March, I reviewed alert 8472 in the ordinary course of my role. The file showed three cash deposits over the stated threshold. I asked my manager whether escalation was required. At 15:20, she said, 'Close it; we are not sending these up this month.'"

That is more useful than "management is covering up money laundering". Include the date and approximate time, the people involved, the system or process, the action taken, and any follow-up. If you do not remember an exact time, say so. Never backdate an entry or quietly rewrite an old note; if you need to correct it, preserve the original and add a dated clarification.

What to write down: a quick checklist

- Date, time and location or system involved.
- Your role and why you had access to the information.
- Specific transaction, alert, filing or control issue, using an internal reference where lawful and appropriate.
- What you personally observed, and what you learned from others.
- Who you contacted, when, how and what response you received.
- Any correction, escalation, repeat incident or instruction not to proceed.
- Any change in treatment at work, with dates and supporting details.
- Where the note is stored and whether it contains confidential or customer information.

Preserve ordinary course documents—lawfully

Ordinary course documents are records created or used as part of normal business activity: for example, an approved procedure, a case-management entry, a training record or a routine escalation email. They may help establish what the process required and what happened. Make a note of a document's title, date, system location and relevant reference number if you are permitted to do so.

Do not assume that you may copy or send work records to a personal email account, cloud drive or device. Customer information, SAR-related material and internal investigative records may be subject to strict confidentiality and access rules. Do not download bulk data, take screenshots of restricted systems, access files outside your role or remove original records. A suspicious activity report (SAR) and information revealing its existence are especially sensitive. Do not put SAR details into personal notes or share them with people who are not authorised to receive them.

If a relevant record may be deleted or changed, note its location and raise the preservation issue through an appropriate channel or with counsel. Do not alter the record yourself. A lawyer can advise how to preserve or describe evidence without making an unauthorised disclosure. Keep your own notes secure, and do not store confidential business or customer data in them unless you have clear authority and a lawful basis.

Consider retaliation risk before escalating

Retaliation risk is not limited to dismissal. It can include demotion, reduced hours, threats, exclusion from meetings, poor performance reviews or other adverse treatment connected to raising a concern. Record events objectively, including the date, decision-maker, stated reason and any relevant comparison with how you were treated before the complaint. Save your employment documents—such as your contract, performance reviews and policies—only in ways you are authorised to use them.

Before making an internal report, check the organisation's reporting channels and policies, including any confidential hotline or compliance escalation route. Consider whether the person you would report to is implicated, and whether another channel is available. Do not confront colleagues or circulate allegations broadly. A limited, factual report is generally easier to assess and less likely to expose confidential information unnecessarily.

If you are concerned about retaliation, speak with an employment or whistleblower lawyer before taking a step that could be difficult to reverse. Ask specifically about internal reporting, regulator submissions, confidentiality obligations, protected activity, and how to keep a record without taking company or customer data. If you receive a threat or are disciplined, write down what happened promptly and keep relevant employment records lawfully.

Understand the deadlines before you wait

Timing can be critical. The federal BSA whistleblower framework, including its anti-retaliation provisions, is set out in 31 U.S.C. § 5323. The law provides avenues for certain whistleblower disclosures and remedies for retaliation, but the right route and applicable requirements depend on the facts. Deadlines can be short, and a worker should not assume that an internal complaint pauses a legal deadline or preserves every claim.

For example, the statute includes a two-year period for bringing a civil action concerning alleged retaliation. That is not a reason to wait: other deadlines, procedural requirements or employment claims may apply, and the date from which a period runs can be disputed. Keep a dated timeline of each report and any subsequent workplace action. Get legal advice promptly if retaliation occurs or you are considering an external submission.

The FFIEC website (ffiec.gov) is a useful starting point for supervisory and examination materials, including information relevant to BSA/AML compliance. It can help you understand the regulatory context, but it is not a substitute for legal advice about your rights, evidence or filing deadlines.

The National Law Review has also published an article discussing filing an AML/BSA whistleblower lawsuit. Read it as general background, not as a conclusion that a particular case qualifies or that a lawsuit is the right first step. Check the article's date and follow links to the current statute and official guidance; legal rules and agency processes can change.

Anonymous or identified: choose with care

Anonymous reporting can reduce immediate exposure, but it may make it harder for an investigator to ask follow-up questions, assess your first-hand knowledge or contact you about protection. An anonymous internal hotline is not necessarily the same as an anonymous submission to a government programme.

Under the BSA whistleblower framework, an individual may in some circumstances submit information anonymously through an attorney, particularly in connection with an award claim, while the person's identity is provided as required if the claim proceeds. The details matter. Do not assume that an anonymous tip automatically preserves eligibility for an award, creates anti-retaliation protection or allows you to remain unidentified throughout an investigation. Ask a lawyer to confirm the current rules and the process for the specific channel you plan to use.

An identified submission may make follow-up and protection claims more straightforward, but it can also reveal your identity to people or agencies involved in the process, depending on the rules and circumstances. Before submitting, find out who will receive the information, what confidentiality protections apply, whether your identity may be disclosed and how to report later retaliation. Avoid promising yourself that any route is completely confidential.





Make the complaint precise and proportionate

A useful complaint gives the reader a route through the evidence. State the concern, the relevant dates, the transactions or controls involved, who was told, and what happened next. Use transaction or case references rather than copying sensitive customer details into an unauthorised channel. Identify which statements are based on your own observation and which are second-hand. Explain uncertainty rather than filling gaps with assumptions.

Before submitting, check that your account is internally consistent and that you have not included speculative accusations, unnecessary personal information or material you were not authorised to obtain. Keep a copy of your own submission and a dated record of when and how it was made, provided *lawyer-monthly.com* doing so is lawful and safe.

A practical next-step sequence

1. Write a dated, factual note while events are fresh.
2. Identify the relevant policy or control using materials you are authorised to access.

3. Record ordinary course documents by reference; do not remove restricted records.
4. Review internal and external reporting options, confidentiality limits and retaliation risks.
5. Speak promptly with a qualified lawyer about deadlines, anonymity and evidence handling.
6. If you report, keep the submission narrow, specific and supported by facts.

Good documentation does not require you to prove the whole case yourself. It requires a careful timeline, concrete details and honesty about what you do—and do not—know. That approach helps an investigator assess the concern while reducing the risk that a well-intentioned report becomes a separate confidentiality or workplace issue.

Record Useful detail Important caution Dated personal notes What you observed, when, who was involved and what followed Do not backdate, exaggerate or include unauthorised customer data Ordinary course documents Title, date, system location and internal reference Do not copy, export or remove records without authority Retaliation timeline Workplace action, date, decision-maker and stated reason Seek advice promptly; internal reporting may not pause deadlines

This article is general information, not legal advice. Your rights and obligations depend on your role, the facts, the reporting channel and current law.