A personal log can help you remember what happened, when it happened and who was involved. In a potential Bank Secrecy Act (BSA) or anti-money laundering (AML) whistleblower matter, those details may matter months or years later—especially if you face retaliation or need to explain why you raised a concern.

A log is not a legal finding, an official investigation file or a substitute for advice from a lawyer. Its purpose is to record your own observations accurately and contemporaneously. Keep facts separate from assumptions, distinguish an honest mistake from possible misconduct, and do not collect information you are not authorised to access.

This article offers practical record-keeping guidance, not legal advice. BSA rules, whistleblower protections and filing deadlines depend on the facts and the law in force. Speak to a qualified lawyer promptly if you may report misconduct or have experienced retaliation.

Start with a clear, secure record

Choose a method you can maintain consistently: a bound notebook, a secure personal device or a document stored in an account that your employer cannot access. Use one entry per event or reporting conversation. Keep the original entries and preserve earlier versions where possible. Do not backdate an entry or silently rewrite it; if you need to correct something, add a dated correction explaining what changed and why.

For each entry, record the date and time you made it, as well as the date and time of the event if different. If you are writing from memory later, say so. For example: "Written 14 May; recollection of meeting on 9 May." That distinction can make your notes more credible than presenting a later recollection as a same-day record.

A practical entry template

- **Date and time:** When the event occurred and when you made the note. Include the time zone if relevant.
- **Who was present:** Names, job titles and how you know they attended. Note anyone who joined or left part-way through.
- **What happened:** Describe actions, statements and decisions in plain language. Use quotation marks only when you are confident the words are exact.
- **Transaction or matter:** Identify the relevant account, alert, case or transaction using only details you are authorised to record. Do not copy sensitive customer information into a personal log unless a lawyer has advised you how to handle it lawfully.
- **Source of knowledge:** Say whether you saw something yourself, heard it from someone else or inferred it from a record.
- **Follow-up:** Record who you contacted, what you raised, the response and any promised next step.
- **Personal impact:** Note changes to your role, access, performance reviews, schedule or treatment at work, with dates and specific examples.

What may count as a BSA violation—and what may be a mistake?

The BSA and related rules require covered financial institutions to maintain AML programmes and meet obligations that may include customer due diligence, suspicious activity monitoring and reporting, record-keeping and other controls. Which requirements apply depends on the organisation and its business. The FFIEC provides examination materials and guidance that can help readers understand how regulators assess BSA/AML

programmes. Start at the FFIEC website; its materials are useful background, not a decision that a particular employer violated the law.

An operational error is not automatically evidence of deliberate misconduct. A missed alert may result from a system fault, unclear procedures, workload or a person's reasonable mistake. Conversely, repeated failures, deliberate suppression of alerts, falsified records or instructions to avoid required reporting may warrant closer scrutiny. Even then, context matters: a personal log should record what you observed, not declare that a named colleague committed fraud.

It is also important to distinguish a possible regulatory breach from criminal willfulness. Some compliance obligations may be breached without proof that an individual intended to break the law; criminal liability generally involves additional legal elements. Do not try to decide those elements yourself. Capture the lawyer-monthly.com facts that may help a lawyer, regulator or investigator assess what happened.

Record this Rather than this "On 3 April, I saw the alert marked 'closed' by 16:20. The case note said 'no escalation'; I do not know who changed the status." "Management covered up money laundering." "At the 10:00 meeting, Alex said, 'Do not send this to the next review queue.' Present: Sam and Jo." "Everyone agreed to ignore the law." "I believe the account may be the same one discussed on 3 April, but I have not confirmed the link." "This was definitely part of the scheme."

Evidence and documentation that holds up

Good documentation is specific, dated and honest about uncertainty. Build a timeline from events you personally witnessed and records you lawfully possess or may access through your work. Do not guess missing dates. Use labels such as "approximate", "recalled later" or "not confirmed" where appropriate.

Keep a separate index for documents or records you may need to discuss with a lawyer. It can identify a file by its title, date, system location and why it matters, without copying confidential content into your personal notes. For example: "SAR escalation log, entry dated 12 June; viewed in the case-management system during assigned review." A SAR (suspicious activity report) and related information may be subject to strict confidentiality rules. Do not forward, download, photograph or take home SAR material or customer records unless you are authorised and have received appropriate legal guidance.

Never access systems outside your role, alter a record, delete messages, or ask a colleague to obtain materials for you improperly. Do not make covert recordings without advice: recording laws and workplace rules vary, and a recording can create risks even if you believe it would support your account. Preserve ordinary business records through authorised channels and tell your lawyer what exists and where it is held.

What to write down: quick checklist

- Make dated entries, including when you wrote the note and whether it is a later recollection.
- Record who was present, their roles and the exact meeting or communication involved.
- Write timeline notes that connect the event to earlier reports, later actions and relevant deadlines.
- Separate what you saw from what you heard, inferred or were told by another person.
- Note the source and location of relevant records; do not improperly copy protected material.
- Record the exact words used when you are confident of them; otherwise summarise and say it is a paraphrase.
- Document internal reports, acknowledgements, responses and follow-up dates.
- Record potential retaliation as concrete changes, with dates, decision-makers and any stated reasons.
- Preserve your original notes and make corrections transparently.

Reporting concerns and protecting your position

If you raise a concern internally, make a factual record of the date, recipient, channel and substance of the report. Keep any acknowledgement or response that you are authorised to retain. Avoid sending confidential customer or investigation details to a personal email address as a way of "preserving evidence". A lawyer can help you identify a lawful way to describe the concern and protect relevant information.

Think carefully before discussing the matter widely at work or with colleagues who may be witnesses. Do not coordinate accounts. Your notes should reflect your own memory, not a version agreed with someone else. If a manager asks you to change a record or keep quiet, document the request accurately, including who made it and when, without embellishment.

Retaliation concerns deserve their own dated timeline. Record events such as a sudden change in duties, exclusion from meetings, a negative review, a suspension or termination. Include what happened before and after you raised the concern, who made the decision and any explanation given. A sequence of events can be relevant, but timing alone does not prove retaliation. Distinguish a documented employment action from your interpretation of its motive.

Statute of limitations and timing pressure

Do not assume that a personal log pauses a deadline. Different legal claims and reporting routes can have different time limits, and the applicable period may depend on the type of alleged violation, when it occurred, when it was discovered and the law that applies. Whistleblower retaliation claims can have short filing windows. Under the BSA whistleblower provisions, a retaliation claim may involve a 180-day period, but whether that deadline applies to your circumstances—and how it is calculated—requires legal advice.

Keep a dated record of the first potentially retaliatory act and later developments, but do not wait to "complete" your log before seeking advice. A lawyer can assess which deadlines may apply, what steps preserve a claim and whether a report should be made through a particular channel. The National Law Review has published material on filing AML/BSA whistleblower lawsuits; see its search results for AML/BSA whistleblower lawsuit information. Treat commentary as a starting point, not a substitute for checking current statutes, agency instructions and case-specific advice.

Anonymous or identified submissions?

Whether you report anonymously or identify yourself can affect how a submission is handled. An anonymous report may reduce immediate exposure, but investigators may have difficulty asking follow-up questions or assessing the source. If you provide identifying information, it may help an agency contact you, yet confidentiality is not the same as absolute secrecy. Disclosure rules and procedures vary by programme and circumstances.



Some whistleblower routes may allow a person to submit anonymously through a lawyer, subject to specific requirements. Do not assume every BSA-related report, award application or retaliation claim can be made anonymously—or that anonymity will remain guaranteed at every stage. Before submitting, ask a lawyer which programme applies, what information must be disclosed, whether counsel can submit on your behalf and what protections or limits govern confidentiality. Verify current instructions with the relevant agency; do not rely on an old article or a form found through a search engine.



Keep the log useful, not dramatic

The strongest personal log is often unremarkable: short, consistent entries that identify the date, people, events, source and follow-up. It does not need to prove a case on its own. It needs to help someone evaluate what you know, how you know it and what happened next.

Preserve the distinction between human error and possible willful misconduct. A single incorrect case disposition may have an innocent explanation; a dated sequence of repeated exceptions, warnings and instructions may raise

different questions. Record the sequence without turning suspicion into fact. Then get prompt, independent legal advice before accessing, sharing or submitting sensitive material.