A whistleblower complaint is more useful when a reviewer can follow the trail from a specific event to a possible breach of law. “The bank ignored money laundering” is an allegation, not a clear account of what happened. A stronger complaint identifies the transactions, the people involved, the relevant dates and locations, what the organisation knew, and what it did or failed to do.

This guide focuses on concerns involving the US Bank Secrecy Act (BSA) and anti-money laundering (AML) controls. It is general information, not legal advice. The right reporting channel and deadlines depend on the facts, the type of claim and the law that applies. Consider speaking to a lawyer experienced in whistleblower matters before submitting sensitive information or taking action that could expose you to retaliation.

Start with facts, not conclusions

Use plain language and separate what you personally observed from what you suspect or learned from someone else. Avoid labels such as “fraud”, “cover-up” or “systemic failure” unless you explain the underlying conduct. A reviewer needs enough detail to test the allegation—not merely a statement of your opinion.

For each event, ask: **who did what, when and where; which transaction or control was involved; what should have happened; and what actually happened?** If you do not know an answer, say so. Do not fill gaps with guesses.

- **Specific transactions:** Include transaction or case reference numbers where lawfully available, dates, amounts, currencies, channels and the accounts or counterparties involved. Do not include unnecessary customer information in an initial submission.
- **Names and roles:** Identify people by name and job title where known—for example, “Jane Smith, branch manager” or “the AML investigations team”. Explain each person’s connection to the events rather than listing names without context.
- **Dates and locations:** Give the date and, where relevant, the branch, office, business unit or jurisdiction. If a date is approximate, mark it as approximate and explain why.
- **Knowledge and response:** State who was told, how and when, and what happened next. Distinguish a report you made from an issue you merely heard about.

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

A BSA-related concern may involve alleged failures in areas such as a financial institution’s AML programme, record-keeping, reporting or internal controls. Examples might include a repeated failure to follow an established escalation process, knowingly bypassing a required control, or suppressing concerns about suspicious activity. Whether particular conduct breaches the law depends on the facts, the institution’s obligations and the applicable rules. A whistleblower should describe the conduct and evidence rather than try to make a final legal finding.

Not every error is misconduct. A missed field, delayed review or mistaken classification could be human error, a training problem, a technology issue or an isolated lapse. It becomes more concerning when the evidence suggests the problem was deliberate, repeated, concealed, ignored after escalation, or allowed to continue despite clear warnings. That distinction matters: **human error and willful misconduct are not the same thing**.

Observation Useful questions An alert was closed without the expected review Was this a one-off mistake? Who closed it, when, and what reason was recorded? Were similar alerts handled the same way? A suspicious-activity escalation did not progress Who received the escalation? Was it acknowledged? Is there a dated note, case entry

or email showing the response? Records appear to have been changed after a concern was raised What changed, when, and in which system? Is there an audit trail or version history? Avoid claiming intent unless you have evidence for it. A control was bypassed on several occasions Which transactions were affected? Were the same people, workflow or business unit involved? What shows the practice was known or repeated?

Explain the possible significance without overstating it. For example: “On 12 March, I escalated case 45821 to the regional AML manager. The case log records that the alert was closed on 14 March without the review step required by the procedure I was using. I do not know why it was closed.” That is more credible than “Management deliberately enabled laundering.”

Build a clear, lawful evidence trail

Good documentation allows a reviewer to verify your account. Keep a dated chronology and identify the source for each important fact. Useful material may include emails, case-management entries, alert histories, meeting notes, training or procedure documents, and records of internal escalation. A complaint does not need to reproduce every file: it should point to the most relevant evidence and explain what it shows.

Do not access records you are not authorised to see, bypass security controls, remove customer data, or share confidential material indiscriminately. Financial records can be highly sensitive. Ask a lawyer or the relevant reporting authority how to preserve or submit material lawfully. Do not alter originals, annotate source documents, or forward restricted information to a personal account unless you have first obtained appropriate advice.



What to write down

- The date and time you made each note, and whether it was written contemporaneously or later.
- The transaction, alert or case reference; amount and currency; and the relevant dates and locations.
- The names and roles of people involved, and exactly what each person did or said.
- How you learned each fact: personal observation, a record you were authorised to access, or information from another person.
- Who you told, when and through which channel; include a reference number or acknowledgement if available.
- What happened afterwards, including any response, investigation step or change to the record.

- What you do not know, what is uncertain, and what evidence could confirm or disprove your understanding.

Use a simple chronology rather than a long narrative that mixes events together. Keep the original records intact and maintain a separate index. A dated note is not proof by itself that every detail is correct, but it can help show when you raised a concern and what you understood at the time.

Be precise about what you are alleging

A useful complaint generally answers five questions:

1. **What happened?** Describe the conduct in concrete terms.
2. **When and where did it happen?** Give dates, locations and the relevant business unit.
3. **Who was involved?** Name people and roles where known, and explain their actions.
4. **Why might it matter?** Identify the BSA or AML process you believe may have been breached, while making clear that the authority determines whether a violation occurred.
5. **What supports your account?** Point to records, witnesses, case references and internal reports.

If there are multiple incidents, number them. For example, distinguish a specific transaction from a later management response and from a separate retaliation concern. This helps a reviewer understand whether the allegation is about a control failure, an individual decision, a pattern of conduct or more than one issue.

Timing pressure: do not assume you have unlimited time

Some BSA whistleblower provisions include deadlines that can depend on when a violation occurred or when it was discovered. Anti-retaliation claims may have a separate, shorter filing window. The exact deadline and procedure can depend on the claim and the facts; a general article or online summary cannot determine your filing date.

Do not wait for an internal investigation to conclude before checking your options. Internal reporting may be relevant, but it does not necessarily pause a legal deadline. Record the date of the underlying conduct, when you learned the relevant facts, when you raised the concern and any date on which you experienced adverse treatment. Get prompt legal advice if you are unsure which clock applies.

The National Law Review has published material discussing how to file an AML/BSA whistleblower lawsuit. Use it as a starting point, not a substitute for advice about your circumstances: search the National Law Review for AML/BSA whistleblower lawsuit guidance.

Anonymous or identified: weigh the practical trade-offs

An anonymous submission may reduce the immediate risk of your identity being disclosed to the organisation, but anonymity can lawyer-monthly.com make it harder for investigators to ask follow-up questions, assess your access to the facts or verify documents. It may also limit your ability to receive updates or pursue certain protections or awards, depending on the applicable process.

An identified submission can make it easier to assess your role, knowledge and evidence, but it can raise real concerns about retaliation or workplace exposure. Before identifying yourself, consider who will receive the complaint, what confidentiality protections apply, how your information may be used, and whether you need advice about retaliation risks. Do not assume that a confidential channel guarantees your identity can never become known.

Whether you submit anonymously or by name, be consistent and accurate. Do not include details that identify you indirectly unless needed to explain your evidence. If you fear retaliation, keep a separate dated record of relevant workplace events—such as changes in duties, threats, unusual discipline or exclusion—and seek advice promptly about the applicable reporting route and deadline.

Use the right reference tools

The Federal Financial Institutions Examination Council (FFIEC) website provides supervisory materials and resources relevant to financial institutions. It can help you understand the regulatory context, but it is not a substitute for making a complaint to the appropriate authority or obtaining legal advice. Start at ffiec.gov and check that any guidance you rely on applies to the institution and issue you are describing.

When reviewing guidance, separate what a regulation or supervisory source says from what you personally observed. A reference to a rule can orient a reviewer; it does not prove that a particular person or institution violated it.



A practical final check

Before submitting, read your complaint as if you were an investigator unfamiliar with your workplace. Can that person identify the specific transactions, names and roles, dates and locations? Can they tell which facts you witnessed and which are second-hand? Is there a clear distinction between a possible mistake and evidence suggesting deliberate or repeated conduct?

- Replace broad claims with dated events and transaction or case references.
- Separate facts, inferences and unanswered questions.
- Describe the response to each escalation, including no response where that is what occurred.
- Preserve evidence lawfully and explain where each item came from.
- Check filing deadlines and retaliation risks before relying on an internal process.
- Keep a copy of what you submit and a dated record of when and how it was sent.

A concise, specific complaint is usually more useful than a lengthy one filled with conclusions. Focus on verifiable events, be candid about uncertainty, and avoid claiming intent unless the evidence supports it. That approach

helps a reviewer assess the concern while protecting the credibility of your account.