In brief: Under the Bank Secrecy Act (BSA), as amended by the Anti-Money Laundering Act of 2020 (AMLA), a person alleging retaliation generally must bring a civil action within **two years of the date the retaliation violation occurred**. That deadline can arrive sooner than expected: a dismissal, demotion or other adverse employment action may start the clock, and internal complaints or ongoing discussions with an employer should not be assumed to pause it.

This is a practical overview, not legal advice. The facts, the date of each employment action and the route used to report suspected misconduct can all matter. If you believe you have been retaliated against, speak promptly with a lawyer experienced in whistleblower and employment law.

The two-year retaliation deadline

The BSA's whistleblower-retaliation provision, at 31 U.S.C. § 5323(g), protects certain people who report suspected violations of the BSA or related requirements, or who cooperate with an investigation. It prohibits an employer from taking specified retaliatory actions because of that protected activity. The statute provides for a civil action in federal district court and sets a two-year limit, measured from the date the violation occurs.

That is the key **retaliation deadline**. It is different from any deadline that may apply to a whistleblower award application. An award claim and a retaliation lawsuit are separate matters, with different requirements and potentially different timelines. Do not assume that submitting a tip, making an internal report or applying for an award preserves a retaliation claim.

Timing can be fact-sensitive. For example, a worker might report a concern in January, receive a written warning in March and be dismissed in August. The relevant date may depend on which action is alleged to be retaliatory and the circumstances around it. A series of actions does not necessarily mean the clock starts only at the final event. Get advice early rather than trying to resolve the calculation after the deadline is near.

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

A whistleblower issue usually begins with a concern that a business or individual has failed to meet a legal obligation. The BSA and its implementing regulations establish anti-money laundering requirements for covered financial institutions and other regulated businesses. Depending on the organisation and facts, concerns may involve an inadequate AML programme, failures in record-keeping, or failures to file required reports such as suspicious activity reports (SARs).

But an error is not automatically a BSA violation, and a violation is not automatically proof that a particular employee acted deliberately. Compliance work is conducted under operational pressure. Data may be incomplete, a transaction may be misclassified, or a filing may be delayed through human error. Those facts are different from a deliberate decision to conceal a problem, suppress a SAR or mislead a regulator. The distinction between **human error and willful misconduct** matters when describing what happened; avoid claiming intent unless you have evidence to support it.

For example, a single late SAR filing might reflect a documented system outage and a prompt correction. A different concern would be dated instructions to exclude a category of suspicious transactions from review, followed by repeated overrides and misleading explanations to auditors. Neither example settles the legal question by itself. The relevant rules, the institution's duties, what decision-makers knew and the surrounding records all matter.

The Federal Financial Institutions Examination Council (FFIEC) publishes examination materials that can help readers understand how regulators assess BSA/AML programmes. Its materials are useful context, but they are not a substitute for the statute, regulations or advice on a specific case. See the FFIEC website and its BSA/AML examination resources.

What may qualify as an adverse employment action?

Retaliation is not limited to dismissal. Depending on the facts and applicable law, an **adverse employment action** may include a demotion, suspension, reduced pay or hours, a reassignment with materially worse duties, a formal disciplinary measure, or another action that would deter a reasonable worker from raising a concern. A hostile comment or disagreement at work may be relevant context, but it does not automatically amount to a legally actionable retaliation claim.

A claim generally turns on more than the sequence "I reported a concern, then something bad happened". Issues can include whether the report was protected, whether the employer knew about it, whether a prohibited action followed, and whether there is evidence linking the two. A close timeline may be significant, but it is not conclusive. Contemporaneous emails, performance records, comparator evidence and explanations given at the time may all help establish what happened.

Evidence and documentation that can hold up

Good documentation is specific, dated and factual. Record what you observed, when you observed it, who was involved and what you did next. Separate first-hand knowledge from assumptions or information you heard from someone else. Do not remove, copy or disclose confidential customer information or restricted company material without legal advice; mishandling sensitive records can create separate legal and employment risks.

Useful records may include:

- **A dated chronology:** the transaction or control issue, your report, the people notified, and each later employment action.
- **Reporting records:** emails, case-management entries, escalation tickets, meeting invitations and notes of verbal reports. Include the recipient and the exact concern raised.
- **AML records you are authorised to access:** for example, relevant SAR logs, escalation records, policy versions, quality-control results or audit findings. Do not put customer-identifying details into personal notes unless counsel advises that it is lawful and necessary.
- **Employment records:** performance reviews, targets, pay or schedule changes, disciplinary notices, job descriptions and stated reasons for a decision.
- **Witness information:** names and what each person directly saw or heard. Avoid asking colleagues to coordinate accounts.
- **Follow-up notes:** after a conversation, make a dated note recording who attended, what was said and any agreed next steps.

Keep records lawfully and securely. Do not alter a SAR log, backdate a note, forward restricted files to a personal account or access systems outside your role. If you are unsure what you may retain, ask a lawyer before taking action.



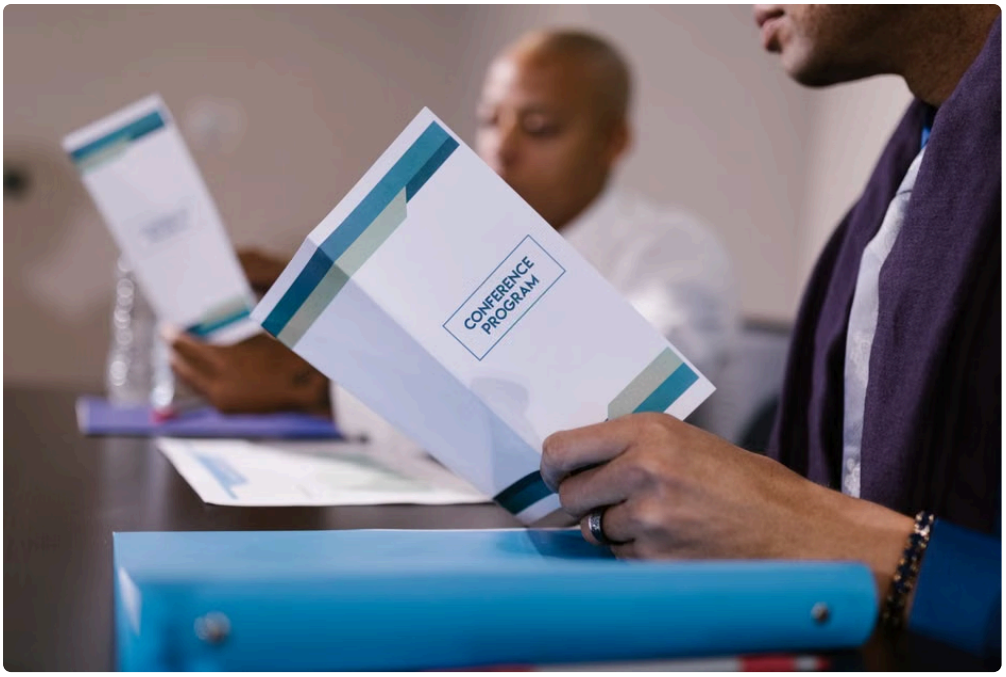
Quick “what to write down” checklist

- Date and time of each event, including when you learned about it.
- The transaction, control or process at issue, described as precisely as you safely can.
- What you personally observed, and what is inference or second-hand information.
- Who you reported it to, by what method, and the words or substance of the report.
- Any response, instruction or change to the relevant record or process.
- Every employment action, its stated reason, and who communicated it.
- Where supporting records are held and who may lawfully access them.

Anonymous versus identified submissions

People often ask whether they can report anonymously. The answer depends on the reporting channel and the purpose of the submission. A person may be able to provide information to an agency without initially identifying themselves, or to seek confidentiality through a process that permits it. The rules for an award submission are not necessarily the same as the rules for proving a retaliation claim.

Anonymity can reduce immediate exposure, but it may make follow-up harder. An agency may need more information to assess lawyer-monthly.com a report, and a person who later brings a retaliation lawsuit will generally need to establish their own protected activity and the employer’s knowledge of it. If an employer did not know who made the report, proving that a later action was taken because of that report may be more difficult—though the facts can differ.



Do not assume that an anonymous tip guarantees confidentiality, or that identifying yourself to an employer is always required to receive protection. Before submitting, consider what information the channel requests, how it handles identity, and whether you may need to demonstrate later that you made a protected report. A lawyer can help assess the trade-offs, including retaliation risks and the timing of any formal complaint.

Acting before the deadline

The AMLA provides a route to bring a retaliation action in federal court, but the details of a particular claim should be checked against the current statutory text and relevant case law. The National Law Review has published practical discussion about filing an AML/BSA whistleblower lawsuit; use it as a starting point for questions, not as a substitute for checking the law that applies to your facts.

1. **Build a dated timeline.** Identify each report and each possible adverse employment action. Do not rely on memory if contemporaneous records exist.
2. **Preserve lawful evidence.** Keep copies of materials you are entitled to access, and ask counsel how to handle restricted or customer-related information.
3. **Get advice promptly.** Ask a lawyer to assess whether the report may be protected, which action may trigger the deadline and whether any other deadlines apply.
4. **Do not rely on internal processes to stop time.** An HR review, internal appeal or regulator contact may be important, but should not be assumed to extend the statutory period.
5. **Plan for retaliation risk.** Consider safe communication channels, who needs to know, and how to document any new changes to duties, pay or treatment.

If a deadline may be close, tell your lawyer the dates first. A polished narrative can wait; a missed filing window may be much harder to fix.

Key takeaways

Issue Practical point Retaliation deadline The BSA generally sets a two-year period from the date the retaliation violation occurs. What is protected? Reports or cooperation covered by the statute may qualify; the precise facts and reporting route matter. What is retaliation? Dismissal is not the only possible adverse employment action.

Record each material change and its date. Error or misconduct? Distinguish an honest mistake from evidence of deliberate concealment or suppression. Do not overstate intent. Anonymous reporting It may offer privacy, but anonymity can complicate follow-up and proof of a later retaliation claim. Documentation Use dated, factual notes and preserve records lawfully; do not remove or alter restricted material.

The central practical point is simple: document carefully, distinguish what you know from what you suspect, and get advice early. The two-year retaliation deadline is a real timing pressure—not something to leave until an internal process has run its course.