Short answer: you do not necessarily need proof of intent before raising a concern about a possible Bank Secrecy Act (BSA) violation. A serious control failure, repeated breakdowns or ignored warnings may warrant a report even when you cannot establish why they happened. But a weak AML programme is not automatically proof of a legal violation, and an isolated error is not the same as deliberate or reckless misconduct.

The practical question is whether the facts point to a failure to meet a BSA obligation, and whether that failure is isolated, systemic or knowingly tolerated. If you are considering making a report or bringing a whistleblower claim, the evidence, reporting route and timing can matter as much as the underlying concern.

What counts as a BSA violation?

The BSA and its implementing rules impose duties on covered financial institutions. Depending on the institution and its activities, those duties can include maintaining an effective anti-money-laundering programme, keeping certain records, identifying customers where required, and filing suspicious activity reports (SARs) when the legal criteria are met.

A programme may be deficient because it lacks appropriate internal controls, independent testing, a designated compliance officer or staff training. Other potential problems include inadequate transaction monitoring, repeated failures to investigate alerts, or SAR decisions that do not follow the institution's procedures or applicable requirements.

However, "the AML programme is broken" is a conclusion, not a complete account of the facts. A regulator, investigator or lawyer will want to know **what obligation may have been breached, when, through which transactions or decisions, and what the responsible people knew**. The FFIEC BSA/AML Examination Manual is a useful reference for understanding how examiners assess programme components and controls. It is guidance for examination, not a substitute for the law or advice on a particular case.

Visit the FFIEC website and look for its BSA/AML examination materials. Comparing a specific control or process with relevant guidance can help you frame a concern precisely. It does not, by itself, establish that the institution violated the BSA.

Does a violation require intent?

Not every BSA compliance failure depends on proving a person intended to break the law. The legal standard varies with the particular requirement, enforcement action and potential penalty. A reporting failure, a deficient programme and a claim that an individual acted "willfully" are not interchangeable allegations. Do not assume that every mistake is a willful violation—or that intent must be proved before anyone can raise a concern.

"Willful conduct" is important in some BSA enforcement and penalty contexts. The precise meaning depends on the law and the facts. Evidence that decision-makers knew about a problem, received credible warnings and chose not to address it may be relevant. So may instructions to suppress alerts, avoid documenting decisions, or leave known gaps in place. Those facts can support a concern about knowing or reckless disregard, but they do not automatically settle the legal question.

Human error, isolated error and willful conduct

Distinguish a mistake from misconduct. A staff member may miss an alert because of a genuine misunderstanding, a one-off system issue or inadequate training. That may still reveal a control weakness that needs correcting, but it

is not the same as deliberately bypassing a control or knowingly allowing a failure to continue.

An **isolated error** is more plausible where the issue is limited, promptly corrected, escalated through normal channels and not repeated. A **pattern of noncompliance** is more concerning where similar failures recur across dates, customers, teams or transactions—particularly after managers or compliance staff have been told about them.

Observed facts What they may suggest What they do not prove on their own One missed alert, followed by prompt review and correction Possible human error or a control weakness worth assessing Intentional misconduct or a pattern of noncompliance Repeated missed alerts for similar transactions over several months A possible systemic issue, especially if the cause is known That a particular person knowingly caused the failures Written warnings followed by instructions to leave a known gap unaddressed Evidence relevant to knowledge, response and possible willful conduct A final legal finding; context and the full record still matter

Evidence and documentation that holds up

Good documentation is specific, dated and tied to observable facts. Avoid broad claims such as "management ignored money laundering" unless you can identify the underlying events. A useful account might say: "On 12 March, I escalated alert 456 concerning transactions on 8 and 10 March. The case was closed on 14 March without the supporting review required by procedure. I raised the same issue with my manager on 20 March." That is more useful than a label without dates or transaction details.

What to write down

- **Dates and sequence:** when the transaction, alert, decision, escalation and response occurred.
- **Specific identifiers:** case or alert references, relevant accounts or transaction IDs, using only information you are authorised to access and disclose.
- **The requirement or control:** the policy, procedure or obligation you believe may not have been followed, and why.
- **People and roles:** who made or approved a decision, who was informed, and when. Separate what you observed from what someone told you.
- **Evidence of follow-up:** dated notes, emails, issue logs, training records or escalation records you lawfully possess.
- **Alternative explanations:** system outage, unclear procedure, workload, training gap or a correction that may explain the event.
- **Retaliation concerns:** any change in duties, performance treatment, access or employment status after you raised the issue, with dates and documents.

For example, a dated SAR log entry showing a case's status may help establish chronology. It does not necessarily prove why a SAR was not filed, whether the filing threshold was met, or who was responsible. Preserve records in accordance with your duties and your organisation's policies. Do not access systems without authorisation, remove confidential customer data, or send sensitive material to a personal account. Ask a qualified lawyer how to preserve and share evidence lawfully, especially where SAR confidentiality or other restrictions may apply.

Reporting channels and retaliation risk

Possible routes may include internal compliance or audit channels, a regulator, SAR logs evidence law enforcement, or a whistleblower programme. The right route depends on the institution, the suspected conduct, the information

available and any legal obligations that apply to you. An internal report can create a useful record and allow a problem to be corrected, but it may not be appropriate in every situation—particularly if the concern involves the people responsible for handling internal escalations.

Before reporting, consider retaliation risk and timing. Keep a contemporaneous record of when you raised the concern, whom you contacted, what you said and how the organisation responded. If your job changes afterwards, record the date and facts without assuming the reason. Retaliation protections have legal conditions and procedures; they are not a guarantee that an employer cannot take any adverse action for a legitimate reason.

The National Law Review has published material on filing an AML/BSA whistleblower lawsuit. Read its AML/BSA whistleblower lawsuit coverage as a starting point, not as a substitute for checking the current statute, agency process and facts with counsel. A lawsuit about retaliation or an award-related claim is different from simply giving an agency information about suspected misconduct.



Statute of limitations and timing pressure

Timing can be decisive. Different deadlines may apply to an administrative complaint, a retaliation claim, an award application or another legal action. Under the BSA whistleblower provisions, the law includes protection against retaliation and a deadline for bringing certain retaliation actions. The applicable deadline and procedure should be verified against the current statute and your circumstances; do not assume that an internal investigation, HR process or agency tip pauses the clock.



There may also be practical reasons to act promptly: records can be overwritten or deleted under ordinary retention schedules, colleagues may leave, and memories fade. At the same time, speed is not a reason to make unsupported accusations or take confidential records unlawfully. If you are considering a formal claim, obtain advice promptly about the relevant deadline, who must receive a filing and what information is required.

Anonymous or identified submissions?

An anonymous report may reduce immediate exposure, but it can make follow-up difficult. An agency may be unable to ask clarifying questions or assess the source's role and access to information. A report that names a source may be easier to investigate, but the source may have confidentiality and retaliation concerns to weigh.

Whistleblower programmes can have specific rules about confidentiality, anonymous submissions and eligibility for an award. Do not assume that a general anonymous tip automatically preserves the right to an award or provides the same protections as a submission made through the programme's required process. In some circumstances, a person may be able to submit through counsel while keeping their identity confidential initially; the exact requirements depend on the programme. Check the relevant agency's current instructions before filing.

A practical decision framework

1. **Identify the obligation:** name the BSA-related duty, control or reporting process that may have failed.
2. **Build the timeline:** list the relevant dates, transactions, alert outcomes and escalations.
3. **Assess recurrence:** distinguish a single error from a pattern of noncompliance and note whether corrective action followed.
4. **Separate fact from inference:** record what you personally observed, what records show and what you infer about intent.
5. **Consider safe reporting:** review internal and external channels, confidentiality limits and retaliation risks.
6. **Check deadlines promptly:** ask a lawyer familiar with BSA whistleblower matters whether any filing or preservation deadline applies.

The bottom line

A broken AML programme can be a legitimate reason to raise a concern, even if you cannot prove intent. But the quality of the report depends on concrete facts: what failed, when it happened, whether it recurred, who knew, and what happened after the issue was raised. A genuine human error should not be casually labelled willful misconduct; equally, repeated failures left uncorrected after clear warnings may deserve closer scrutiny.

Document the chronology, preserve only information you are authorised to handle, and get advice on reporting options and deadlines before they expire. A careful, evidence-based account is more useful—and fairer to everyone involved—than a vague allegation.