Employees of money service businesses (MSBs) may be able to report suspected Bank Secrecy Act (BSA) violations, and federal law can protect certain whistleblowers from retaliation. But "I spotted an AML problem" is not, by itself, enough to establish a violation—or guarantee protection or an award. The details matter: what happened, when it happened, what the employee knew, and how the information is handled.

This guide explains how to distinguish a possible BSA violation from a mistake, what evidence may help, and why reporting deadlines and confidentiality deserve early attention. It is general information, not legal advice. Employees facing retaliation or considering a report should obtain advice from a lawyer familiar with BSA whistleblower issues.

Does the BSA apply to money service businesses?

Generally, yes. Many businesses that exchange currency, transmit money, sell money orders or travellers' cheques, cash cheques, or provide certain prepaid access services may fall within the MSB definition. The precise classification depends on the activity and applicable rules. MSBs may have obligations that include registration with the Financial Crimes Enforcement Network (FinCEN), maintaining an effective anti-money laundering programme, keeping required records, and filing currency transaction reports (CTRs) or suspicious activity reports (SARs) when applicable.

"BSA coverage" is not identical for every business or every service. A business's size, products, transaction types, exemptions and role in a transaction may affect which requirements apply. An employee should avoid assuming that a rule applies simply because a similar business follows it. Check the relevant regulation and the company's documented procedures, and get qualified advice where the scope is unclear.

The FFIEC website provides BSA/AML examination resources that can help readers understand common control expectations. The FFIEC is not the primary regulator for every MSB, however, and its materials should not be treated as a substitute for FinCEN requirements or advice specific to the business. FinCEN is the key federal source for MSB registration and BSA rules.

Can an employee report a BSA violation?

Federal law includes a whistleblower programme for information about certain BSA violations. Under 31 U.S.C. § 5323, an individual may provide information to the US Department of the Treasury or the Department of Justice. Depending on the information and the outcome of an enforcement action, a whistleblower may potentially qualify for an award. The law also prohibits specified forms of retaliation against individuals who report information or assist with relevant proceedings.

These protections are not a blanket promise that every internal complaint is protected or that every tip qualifies for an award. The statutory requirements, the reporting route, the evidence, and the person's role all matter. The rules and procedures can be technical, so an employee considering an external submission should speak with a lawyer before disclosing confidential information or relying on anonymity.



A National Law Review article discussing AML/BSA whistleblower lawsuits may provide useful background: National Law Review: AML/BSA whistleblower lawsuit coverage. Treat commentary as a starting point, not a substitute for checking the statute, current agency instructions and advice on the facts.

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

A control failure is not automatically proof of deliberate wrongdoing. Compliance work involves human error: a new employee may mis-key a transaction, misunderstand a threshold, miss a review step, or make a good-faith judgement that later proves incorrect. The response should distinguish that from a pattern of knowingly bypassing controls or concealing a failure.

Potentially serious issues can include an MSB operating without required registration, having no effective AML programme, failing to maintain required records, or not filing a required report. A concern may become more significant where there is evidence that responsible people knew about the issue and deliberately ignored it, directed staff not to act, falsified records, or retaliated against someone who raised it.

Possible human error or control gap Potential warning signs of willful misconduct A one-off missed escalation that is promptly corrected and documented. Repeatedly suppressing alerts after receiving clear, dated warnings. Confusion about a procedure, followed by training or a process change. Instructions to alter, backdate or destroy records to hide a known failure. A reasonable disagreement about whether activity is suspicious. Evidence that managers blocked required review or reporting for improper reasons.

Context matters. A SAR is not required merely because a transaction is unusual; the legal standard and applicable rules must be assessed. Equally, an employee should not label conduct “fraud” or “cover-up” without facts. A useful report describes the transaction, the control involved, the people notified, and what happened next.

Evidence and documentation that may hold up

Credible reporting is usually specific and organised. A dated chronology is often more useful than a broad claim that “management ignored AML”. Record what you personally observed, what you were told, and what you inferred as separate categories. Identify the transaction or control issue as precisely as you can without taking or sharing material unlawfully.

What to write down

- **Dates and times:** when the transaction, alert, discussion or decision occurred, including time zone if relevant.
- **Transaction identifiers:** amounts, dates, branch or channel, internal reference numbers and relevant customer or counterparty details, handled in line with privacy and confidentiality rules.
- **The rule or procedure:** the policy, training instruction or regulatory requirement you believe may apply, and why.
- **People and actions:** who reviewed, approved, escalated or declined to act, and the words used where you can record them accurately.
- **Supporting records:** the existence and location of an alert, case file, SAR log entry, training record, audit finding, email or dated note.
- **Follow-up:** when you raised the concern, to whom, how they responded, and whether the issue was corrected.
- **Your uncertainty:** what you do not know, what is second-hand, and what alternative explanation may exist.

Do not remove customer files, download restricted databases, forward SARs to a personal account, or access records outside your authorised role. SAR information is subject to strict confidentiality rules. Discuss safe evidence preservation with counsel; a whistleblower process is not permission to breach privacy, security or SAR-disclosure restrictions.

Anonymous or identified submissions?

Some whistleblower mechanisms may allow a person to submit information anonymously through an attorney, at least at the initial stage. That is different from making an untraceable report with no contact point. An agency may need a way to ask follow-up questions, assess credibility and verify the information. If a person seeks a potential award, identity verification and additional formal steps may be required under the applicable process.

An identified submission can make follow-up easier, but it may also increase the employee's concern about workplace consequences. An anonymous submission may reduce immediate exposure, yet limit the investigator's ability to clarify facts and may not remove all practical risks. Before choosing, ask counsel about the current submission rules, confidentiality, eligibility for an award, and what happens if the employer identifies the source.

Internal reporting can also be useful, particularly where the issue may be a correctable error. But internal channels are not always safe or effective, and a company process does not necessarily pause an external legal deadline. Employees should not assume that they must report internally first—or that they can wait indefinitely for an internal investigation—without checking the rules that apply to their situation.

Timing pressure: limitation periods and retaliation

Deadlines depend on the type of claim and the facts. BSA civil and criminal enforcement may have different limitation periods; other laws may apply to employment claims or related conduct. A whistleblower retaliation complaint under the BSA has its own statutory process and short filing window. The applicable deadline may be measured from the alleged retaliatory act, not from the date an internal investigation concludes.

Because deadlines can be easy to miscalculate, get legal advice promptly after a report or an adverse workplace action such as dismissal, demotion, threats, reduced duties or unusual discipline. Keep a dated record of each event and preserve relevant notices. Do not wait for a regulator or employer to confirm that a violation occurred before asking about timing.

Retaliation risk is real, even where the law prohibits it. Consider a safe communication plan, use personal contact details when speaking with counsel, and avoid discussing a contemplated report on work systems if that statute of limitations retaliation claim could expose confidential legal advice. Do not secretly record conversations unless you have checked the law and obtained advice; recording rules vary.

A practical approach for an MSB employee

1. **Describe the facts neutrally.** Separate what you saw from what you suspect, and distinguish a one-off human error from a possible pattern of deliberate conduct.
2. **Check the requirement.** Identify the relevant MSB activity, procedure and potential BSA obligation. Use official FinCEN resources and, as background, appropriate FFIEC materials.
3. **Make a dated chronology.** Record transactions, alerts, escalation attempts, responses and corrective actions. Keep an accurate SAR log reference where authorised, without disclosing SAR content improperly.
4. **Protect restricted information.** Do not copy or transmit customer data or SAR material outside approved channels. Ask counsel how to preserve evidence lawfully.
5. **Get advice early.** A lawyer can help assess reporting options, anonymity, retaliation protection, award eligibility and deadlines before an irreversible disclosure.

The bottom line

Employees can report suspected BSA violations, and federal whistleblower protections may apply. But a missed step is not automatically willful misconduct, and a vague allegation is unlikely to be as useful as a dated, transaction-specific account. For MSB compliance concerns, document what happened, preserve evidence lawfully, protect SAR confidentiality, and get advice on reporting routes and deadlines before time runs out.

