Employees often notice warning signs before anyone calls them a violation: a suspicious-activity alert that keeps getting closed without a clear reason, customer information that is missing but never chased down, or a payment held for review and then released without a documented explanation. These situations deserve attention, but they are not automatically proof of a crime or even a legal violation. The details matter: what the law or regulation required, what the institution's procedures said, what employees knew, and what the organization did next.

The Bank Secrecy Act (BSA) is a U.S. anti-money-laundering framework. It requires covered financial institutions to maintain programs and meet specific reporting and recordkeeping obligations. The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, administers key parts of the BSA. This guide explains common problems employees may encounter, how to distinguish a control failure from a reportable violation, and what to consider before raising a concern.

Start with the duty—not the label

Calling something "fraud" or "money laundering" without evidence can obscure the real issue. A useful first question is: what specific BSA duty may have been missed? That might be a duty to file a required report, maintain an effective anti-money-laundering program, collect and use customer information, or keep required records. A mistake may be serious, but not every error, disagreement, or weak process is a legal violation.

Area What the obligation generally involves Examples of workplace warning signs Suspicious Activity Reports (SARs) Identifying and reporting suspicious activity when applicable rules require it Alerts repeatedly closed without a documented basis; possible suppressed SARs Currency Transaction Reports (CTRs) Reporting qualifying cash transactions under applicable rules Cash transactions appear omitted, misclassified, or improperly separated Customer Due Diligence (CDD) Understanding customer relationships and applying risk-based monitoring Ignored CDD gaps, stale risk information, or unexplained exceptions AML program Maintaining a program appropriate to the institution's risks and legal obligations Known control failures remain unresolved or testing is not meaningful

Common issues employees may actually see

1. Suppressed SARs or weak suspicious-activity escalation

A SAR is a report that a covered institution may be required to file when a transaction or pattern meets the applicable suspicion and reporting standards. Rules differ across institution types and circumstances, so a single dollar amount does not answer every SAR question.

Employees may worry about **suppressed SARs** when they see repeated efforts to prevent a concern from reaching the people responsible for review, or when a decision not to file appears inconsistent with the institution's procedures and available facts. Other warning signs can include:

- Alerts being closed with boilerplate explanations that do not address the activity.
- Cases being delayed or repeatedly reassigned until a filing deadline may be missed.
- Pressure to change a case narrative to remove relevant facts without a sound basis.
- Known patterns of suspicious activity being excluded from review without documented reasoning.

These signs are not conclusive by usattorneys themselves. A SAR decision is often based on a broader review, and institutions may lawfully decide that a particular case does not meet the filing standard. Employees generally should not disclose whether a SAR has been filed or share a SAR or information revealing its existence with a customer or unauthorized person. SAR confidentiality rules are important; raise concerns through authorized channels instead of circulating protected material.

2. CTR errors and possible structuring concerns

A CTR generally concerns qualifying cash transactions over $10,000 in one business day, including certain transactions that must be aggregated. The rules contain details and exceptions, and the obligation belongs to the covered institution—not to an employee acting alone. A customer who divides cash transactions to evade reporting may be engaging in structuring, but employees should not assume that ordinary cash activity proves intent.

Potential problems include a qualifying cash transaction not being captured, inaccurate information being submitted, or staff being directed to break up or misclassify transactions to avoid a reporting requirement. Record what you observed and how it was handled. Do not create, alter, or "fix" records outside your authority.

3. Ignored CDD gaps

Customer Due Diligence (CDD) helps institutions understand who their customers are, the nature and purpose of relationships, and the risks they present. Depending on the institution and customer, duties may include identifying beneficial owners of certain legal-entity customers and conducting ongoing monitoring. CDD is not a one-time form-filling exercise; relevant information may need to inform risk ratings and transaction monitoring.

Ignored CDD gaps may include missing or contradictory ownership information, a risk rating that is not updated after significant changes, repeated exceptions without review, or monitoring that does not reflect known customer activity. A missing document alone does not establish a violation. The key questions are whether a specific rule or required procedure applied, whether the gap affected the institution's ability to meet its duties, and whether the institution addressed it appropriately.

4. An AML program that exists on paper but does not work

Covered institutions generally must maintain an AML program with required elements, which can include internal controls, independent testing, a designated compliance officer, and employee training. The precise requirements depend on the type of institution and applicable rules. A polished policy manual does not, by itself, show that a program is effective in practice.

Employees may see recurring alert backlogs, inadequate staffing, training that does not match job responsibilities, audit findings that remain open, or systems that fail to capture known risk. One control failure may be an isolated problem. A pattern that management knows about and leaves unaddressed may raise more serious questions about program adequacy and oversight.

5. Sanctions processing failures

Sanctions processing is often discussed alongside AML controls, but sanctions obligations are not simply another name for BSA duties. U.S. sanctions are administered principally by the Treasury Department's Office of Foreign Assets Control (OFAC), under authorities distinct from the BSA. A sanctions-screening

failure may therefore involve a separate legal or regulatory issue, though the same transaction-monitoring teams, systems, or escalation processes may be involved.

Possible warning signs include a payment released after a credible potential match without documented review, screening rules disabled without appropriate approval, or repeat false-negative concerns that are never investigated. A name match is not automatically a sanctions violation; identity resolution and the applicable sanctions program matter. Employees should follow the institution's escalation procedures and avoid independently stopping, releasing, or modifying transactions unless authorized.



When may a problem qualify as a reportable BSA/AML violation?

There is no universal checklist that turns every workplace concern into a reportable violation. A concern is stronger when it connects identifiable facts to a concrete legal duty, such as a required filing, recordkeeping obligation, CDD requirement, or AML-program element. It also helps to distinguish among:

- **An error:** a mistake that may have been corrected through ordinary controls.
- **A control weakness:** a process that may not reliably meet applicable obligations.
- **Potential misconduct or a violation:** facts suggesting a legal requirement was not met, particularly if the problem was repeated, concealed, or left unresolved after notice.

Intent is not the only relevant question. Some regulatory obligations can be breached through deficient systems or processes even without proof that an employee intended to facilitate wrongdoing. At the same time, an employee's disagreement with a risk decision does not establish that the institution violated the law. Keep descriptions factual: what happened, when, which process was involved, who was notified, and what response followed.

Reporting internally and preserving a reliable account

Internal compliance channels—such as a manager, AML officer, ethics hotline, or designated reporting portal—may be an appropriate place to raise a concern, depending on the circumstances and the organization's procedures. If you report internally, consider asking how the matter will be handled and whether there is a confidential route. Do not assume every channel guarantees anonymity or confidentiality.

Write down a timeline the same day something happens, while your memory is fresh. Keep it factual and separate what you personally observed from what someone else told you. Note dates, relevant job roles, case or system references when lawful to do so, and the steps you took. Preserve materials only through authorized means. Do not email work documents to a personal account, copy customer records for yourself, bypass access controls, or take SAR-related material outside approved channels. Confidentiality, privacy, employment, and evidence-handling rules may apply.

FinCEN whistleblower reports: original information and eligibility basics

FinCEN has a whistleblower submission process for information about certain violations within its authority. The **FinCEN whistleblower submission form** is an agency process referenced here, not a promise that every submission qualifies for an award or will lead to a particular outcome. The relevant statute and program rules control eligibility, and the program's scope and procedures can change.

In broad terms, whistleblower award programs generally focus on voluntary, original information that is specific and credible and that contributes to a successful enforcement action resulting in qualifying monetary sanctions. "Original information" is not simply a belief that misconduct occurred; it generally means information derived from the person's independent knowledge or analysis and not already known to the agency from certain sources. Statutory exclusions and limitations may apply. Employment in compliance, audit, or legal roles can raise additional questions about what information may be used or disclosed.

Before submitting, review the current FinCEN instructions and eligibility rules. A person should not assume that an internal report automatically disqualifies them—or that reporting internally is always required before contacting an agency. The answer depends on the governing program and facts. Never include customer information or confidential records in a submission without considering applicable restrictions and obtaining appropriate legal guidance.



Working with a whistleblower attorney

A lawyer familiar with whistleblower matters can help assess whether the facts connect to a legal duty, identify the right agency or reporting route, and discuss confidentiality, retaliation risks, and document handling. A lawyer can also help distinguish a BSA concern from a sanctions issue, securities matter, or general workplace dispute. USAttorneys.com may be one place people use to look for attorney information,

but verify a lawyer's experience, licensing, and fit for your particular situation before sharing sensitive details.

Some whistleblower attorneys work on a contingency-fee basis, meaning the fee is tied to a recovery or award under an agreed arrangement. "Contingency" does not mean every cost is covered or that an award is likely. Ask for the fee terms in writing, including how expenses are handled, what happens if there is no recovery, and whether the lawyer represents you in the specific agency process you are considering.

Practical next steps

1. Identify the potential duty involved: SAR, CTR, CDD, AML program, recordkeeping, or a separate sanctions obligation.
2. Write a same-day timeline and keep observations separate from assumptions.
3. Use authorized internal channels when appropriate, and note when and how you raised the concern.
4. Protect customer and institution information; do not remove or transmit records without authorization.
5. Review current agency instructions and consider speaking with qualified counsel before making an external submission.

Employees are often closest to the systems and decisions that reveal a control problem. A careful, factual account is more useful than a dramatic label. Focus on the duty, the evidence, and the steps taken to address the issue—and do not promise yourself that an investigation will move quickly. Agency processes can take time, and outcomes depend on the facts and the applicable law.