If you find a possible Bank Secrecy Act (BSA) failure, you may be weighing two options: raise it through your organization's compliance channels or report it outside the organization. The answer depends on what you know, whether internal reporting is safe and effective, and whether waiting could allow harm or evidence loss.

There is no universal rule that you must report internally first. Internal escalation can help an organization investigate and correct a problem, but it is not always a prerequisite to contacting regulators or law enforcement. And reporting externally does not automatically mean the government will investigate, bring an enforcement action, or award money.

This is a general overview, not legal advice. BSA issues, whistleblower protections, and filing deadlines can be fact-specific. Consider speaking with an attorney before sharing sensitive information.

What the BSA Does—and Who Handles What

The BSA is the federal framework requiring financial institutions and certain other businesses to maintain anti-money-laundering controls and report specified financial activity. Its requirements include recordkeeping, customer due diligence, and suspicious activity reporting. Transaction monitoring systems may help identify activity that warrants review, but a system alert is not itself proof of a violation.

The Financial Crimes Enforcement Network (FinCEN) administers the BSA, issues implementing rules, and receives suspicious activity reports. Federal banking agencies examine and supervise the institutions they oversee. The Department of Justice (DOJ) investigates and prosecutes federal crimes. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have separate authority over securities- and commodities-related misconduct, respectively.

These roles matter. A report to one agency is not necessarily a substitute for a required filing with another, and an employee's whistleblower report is not the same thing as a financial institution's SAR filing.



Internal vs External Reporting: What's Changed

Historically, examiners often found the problems

For years, BSA enforcement often began with government supervision: an examiner reviewed a bank's controls, testing, records, or SAR processes and identified weaknesses. Supervisory findings could lead to required corrective action and, in serious cases, enforcement. That history still matters. Examinations remain an important way authorities assess whether a program is working.

But examiner-driven discovery is not the only route. Transaction monitoring systems can generate leads, employees may see gaps that testing misses, and information can reach regulators through other reporting channels. Waiting for the next examination is not a safe response to a known, material problem.

Whistleblower pathways changed the calculation

Congress created a formal AML whistleblower award program through the Anti-Money Laundering Act of 2020 (AMLA). The program created a potential financial incentive for individuals who provide original information that leads to qualifying enforcement actions. It also established anti-retaliation protections for certain protected disclosures.

That does not mean every internal report qualifies for an award, or that every BSA concern should go straight to the government. It does mean that internal vs external reporting is now a practical decision about safety, urgency, and legal protections—not simply a question of whether management gets the first chance to respond.

What the AMLA Award Can—and Cannot—Mean

Under the AMLA framework, an eligible whistleblower may receive an award of 10% to 30% of monetary sanctions collected in a qualifying action, subject to the statute and applicable rules. A key threshold is that the action must result in monetary sanctions exceeding $1 million. The threshold is not a promise of an award: the information must meet the program's requirements, and an award depends on a qualifying enforcement result and collected sanctions.

FinCEN administers the AMLA whistleblower program. A person considering a submission should check the current program rules and filing procedures rather than assume that a tip, internal complaint, or media disclosure preserves eligibility. An attorney experienced in whistleblower matters can assess whether the facts may qualify and help manage the submission.

The AMLA program is separate from SEC and CFTC whistleblower programs. If the alleged conduct involves securities or commodities laws, those agencies may have distinct reporting routes and award criteria. Which agency is relevant depends on the conduct and the legal basis for reporting—not simply on the type of financial institution involved.

Internal Reporting: When It Can Help

Internal reporting can be useful when the organization has a credible, independent compliance function and the issue can be escalated promptly without alerting potentially implicated people. It may allow the institution to preserve records, investigate a monitoring gap, correct a control, and meet its own reporting obligations.

Use established channels where appropriate, such as compliance, the BSA officer, internal audit, an ethics hotline, or the board's audit or risk committee. Keep a factual record of what you observed, when you raised

it, who received it, and what response followed. Avoid speculation and do not access records you are not authorized to review.

Internal reporting has limits. A report to a supervisor may not reach an independent decision-maker. The people receiving it may be involved in the conduct, or the organization may delay, narrow, or mishandle the review. If you reasonably fear retaliation, destruction of evidence, or an ongoing risk to customers or the financial system, consider getting legal advice before relying on internal channels alone.

External Reporting: When It May Be Appropriate

External reporting may be worth considering when internal channels are compromised, the concern is urgent, prior reports were ignored, or you have a reasonable basis to believe the conduct is serious. A person may also choose to seek advice about external reporting before raising the issue internally. There is no blanket rule requiring whistleblowers to complete an internal process first, but program-specific eligibility and lexinter.net procedural requirements matter.

Be precise about the recipient. FinCEN administers the BSA and receives SARs, but a whistleblower tip is not a SAR. A financial institution's SAR filing is a separate legal obligation carried out by the institution. Banking regulators supervise institutions; DOJ handles criminal enforcement; and the SEC or CFTC may be relevant when their laws are implicated. A lawyer can help identify the right pathway and avoid sending sensitive material to the wrong place.

SAR confidentiality is a hard boundary

SARs and information that would reveal the existence of a SAR are subject to strict confidentiality rules. Do not forward, copy, or disclose a SAR—or tell someone that one was filed—unless disclosure is authorized. This restriction does not generally prevent reporting the underlying facts through a lawful channel. For example, you can describe suspicious transactions or control failures without attaching a SAR or confirming that a SAR exists. When in doubt, get legal advice before sharing documents.

Whistleblower Sequencing: A Practical Decision Framework

"Whistleblower sequencing" means deciding what to do, in what order, and how to protect yourself and the evidence. The right sequence is fact-dependent. A deliberate plan is usually safer than an improvised email or an unauthorized download.



1. **Assess urgency.** Is suspicious activity ongoing? Could delay lead to continued harm, lost records, or a missed legal deadline? If so, seek prompt legal advice about escalation.
2. **Separate observations from conclusions.** Note the transactions, control failures, dates, system alerts, and responses you personally know about. Avoid labeling conduct criminal without support.
3. **Check internal channels and conflicts.** Identify who can investigate independently. If the normal chain includes a person implicated in the issue, consider an alternate channel or external advice.
4. **Preserve lawfully.** Keep your own notes and relevant communications in accordance with policy and law. Do not take restricted customer data, access systems without authorization, or remove SARs.
5. **Get advice on the route.** Counsel can help assess AMLA eligibility, confidentiality, agency jurisdiction, deadlines, and how to submit information without compromising protected material.
6. **Document what happens next.** Record the date and substance of reports and any response or adverse treatment. Keep the record factual and secure.

Retaliation Risk Planning and Legal Protections

AMLA includes anti-retaliation protections for certain individuals who make protected disclosures to covered recipients, which can include an employer, the Treasury Department, DOJ, specified federal regulators or law-enforcement authorities, and Congress. The law provides potential remedies for prohibited retaliation, including reinstatement, double back pay, and compensation for litigation costs. Whether a particular disclosure and worker are covered depends on the facts and statutory requirements.

Protection is not the same as immunity from every workplace consequence. A person may still face legitimate discipline unrelated to protected reporting, and a dispute may arise over whether the report was protected or whether it caused the adverse action. Other laws may apply depending on the person's role, employer, and the subject of the report.

Emerging case law is developing the boundaries of AMLA protection. Courts may have to address issues such as who qualifies as a protected whistleblower, what counts as a covered disclosure, how causation is shown, and what procedures or deadlines apply. Do not assume that a general anti-retaliation principle resolves those questions in your favor. Ask counsel promptly about applicable deadlines and how to document a retaliation concern.

For retaliation risk planning, keep a contemporaneous record of performance reviews, job changes, threats, exclusion from work, or other adverse treatment. Preserve relevant communications lawfully. Avoid using personal devices or accounts to remove confidential information without advice. If you have already reported internally, note what you reported and when; if you have not, do not let fear of retaliation force you into an unsafe or legally risky disclosure.

What This Means in Practice

There is no one-size-fits-all answer to whether to report internally or go straight to regulators. Internal escalation may be effective when it is independent and timely. External reporting may be appropriate when internal channels are compromised, the concern is urgent, or you need a protected route outside the organization. You do not necessarily have to report internally first—but an award or legal protection is never automatic.

Situation Practical consideration Compliance channels appear independent and responsive Consider a factual internal report and document the response. Senior staff or the BSA function may be implicated Seek advice about an alternate or external reporting path. Possible ongoing harm or evidence loss Get prompt legal advice; do not wait for a routine examination. You are considering an AMLA award Check current rules, eligibility, submission procedures, and the $1 million sanctions threshold with counsel. You have access to SAR-related information Do not disclose a SAR or confirm its existence; report underlying facts through an authorized route.

The safest first step is often to make a careful, confidential plan—not to choose a side in the abstract. Understand what you observed, protect restricted information, identify who can act independently, and get legal advice about sequencing. BSA concerns deserve prompt attention, but a sound report should be accurate, lawful, and directed to the right place.