The Bank Secrecy Act (BSA) is a central part of the U.S. government's effort to detect and deter money laundering and other financial crime. It requires many financial institutions to keep records, maintain anti-money-laundering controls, and report certain activity to the government. For employees and other insiders, those duties can make BSA violations important to recognize—and potentially important to report.

But a useful tip is not simply an accusation that a bank "failed at AML." It explains what the person personally observed, what they learned from others, which records may support the concern, and why the conduct may matter. This guide covers the BSA, FinCEN's role, suspicious activity reporting, possible violations, and ways to prepare a clear tip without mishandling confidential information.

What Is the Bank Secrecy Act?

Enacted in 1970 and expanded by later laws, the BSA is a framework of laws and regulations aimed at making financial activity more transparent to law enforcement and national security agencies. It is often described as a **BSA cornerstone of banking law** because it establishes key recordkeeping and reporting obligations for covered financial institutions and other businesses.

The BSA does not require institutions to prevent every crime or report every unusual transaction. Instead, it requires them to maintain controls suited to their risks and to report specified information when legal standards are met. The rules vary by institution type and activity; banks, money services businesses, broker-dealers, casinos, and other covered entities may have different obligations.

Common elements of a BSA program include internal policies, designated compliance responsibilities, training, independent testing, customer identification and due diligence measures, recordkeeping, and monitoring for suspicious activity. These are often referred to as **AML program requirements**. A program should be appropriate to the institution's business, products, customers, and geographic exposure—not just a policy document that exists on paper.

What Is FinCEN, and What Does It Do?

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury. It collects and analyzes financial data, including reports filed under the BSA, and shares information with law enforcement, regulators, and other authorized users. FinCEN also issues regulations and guidance, administers BSA reporting systems, and plays a role in enforcing BSA requirements.



FinCEN is not the only agency involved in BSA oversight. Depending on the institution and issue, federal banking regulators, the Internal Revenue Service, the Securities and Exchange Commission, the Department of Justice, or other agencies may have relevant responsibilities. FinCEN's **enforcement authority** can include civil enforcement actions, but a particular matter may involve more than one agency. The agency that receives a tip is not necessarily the only agency that may investigate it.

FinCEN's whistleblower program page, at fincen.gov/whistleblower-program, describes how to submit information about potential violations within the program's scope. Eligibility and lexinter.net any possible award depend on the law and the facts; submitting a tip does not guarantee an investigation, enforcement action, or payment.

BSA and SAR Reporting Basics

What Is a Suspicious Activity Report?

A Suspicious Activity Report (SAR) is a report that a covered institution files with FinCEN when it knows, suspects, or has reason to suspect activity that meets applicable reporting criteria. Those criteria may involve potential violations of law, transactions designed to evade BSA requirements, or activity without an apparent lawful purpose that cannot be reasonably explained after review.

A SAR is not a finding that a customer committed a crime. It is a way to alert authorities to activity that warrants attention. Institutions generally make their own filing decisions under the rules that apply to them, and a SAR may be filed even when the institution does not know the full explanation for the activity.

Some BSA reports are not SARs. For example, institutions may have obligations to file Currency Transaction Reports (CTRs) for certain cash transactions above a regulatory threshold, subject to applicable rules and exemptions. BSA requirements also include recordkeeping obligations and other reports. The details depend on the institution and transaction.

Why SAR Confidentiality Matters

SARs and information revealing that a SAR was filed are subject to strict confidentiality rules. An employee should not copy, forward, download, or disclose a SAR—or tell a customer or another unauthorized person

that one exists—unless specifically authorized by law and policy. These restrictions do not mean a person cannot report suspected misconduct through an appropriate channel. They do mean that the person should think carefully about what information they may lawfully share and how to protect it.

If a concern involves a SAR, a tip may describe the underlying conduct or control failures without attaching or quoting the SAR itself. Before sharing internal records, consider access permissions, confidentiality obligations, and whether the submission process provides secure instructions. When uncertain, seek advice from qualified counsel rather than moving documents to a personal account or device.

What Conduct Might Be Reportable?

Potentially reportable conduct depends on the facts, the institution's obligations, and the applicable law. A disagreement about a customer decision or a single operational mistake is not automatically a BSA violation. More concerning patterns may involve intentional misconduct, repeated control failures, or management decisions that undermine required safeguards.

Possible concern Example to examine Why context matters Weak or ineffective AML controls Monitoring rules repeatedly fail to flag known high-risk activity, and documented remediation is postponed. A control gap may be a serious concern, but the tip should explain its scope, duration, and effect—not merely label the program "inadequate." Failure to investigate or escalate alerts Alerts involving similar transactions are routinely closed without review despite available information suggesting a potential risk. Describe the decisions and records you know about. Do not assume every closed alert was improper. Possible SAR reporting failures Employees identify recurring suspicious activity, but responsible teams are directed not to escalate it or reporting is consistently delayed. Distinguish a concern about the process from a conclusion that a particular SAR was legally required. Avoid disclosing SARs or their existence improperly. Structuring or evasion concerns Transactions appear divided or arranged to evade reporting or recordkeeping requirements. Patterns and surrounding facts matter; a transaction pattern alone may not establish intent or a violation. False or misleading records Compliance documentation is altered or approvals are recorded as complete when required work was not performed. Identify what you personally saw, when you saw it, and how you know the record was inaccurate.

Other concerns can include inadequate customer due diligence, failure to maintain required records, or attempts to obstruct an internal or regulatory review. These examples are not legal conclusions. The best tip describes observable facts and lets the appropriate authority assess the law.

How to Prepare a High-Quality Tip

A clear, factual submission is more useful than a long narrative built on assumptions. The following steps can help organize what you know while reducing the risk of mishandling protected information.

1. **Separate firsthand knowledge from information you heard.**

   State what you personally saw, did, reviewed, or were told. Identify secondhand information as such: who told you, approximately when, and whether you have a basis to assess its reliability. Do not present something you heard as something you witnessed.

2. **Build a concise timeline.**

   List the relevant events in order, including approximate dates, business units, roles, and decisions. If you do not know an exact date, say so. A timeline can help investigators understand whether the issue was isolated, repeated, or escalated.

3. **Explain the suspected conduct, not just the label.**

   Instead of writing “the bank ignored money laundering,” describe the transactions, alert handling, instructions, control gaps, or management actions that led you to that concern. Note what you believe the institution’s obligation may have been, while making clear when that is your understanding rather than a confirmed legal conclusion.

4. **Identify potential corroboration.**

   Point to records, systems, teams, meetings, or witnesses that could help verify the account. Explain where the material may be located and who may have access. You generally do not need to possess every document to describe a credible concern.

5. **Handle records carefully.**

   Do not access information you are not authorized to view, alter records, or send confidential files to a personal email account or storage service. SARs and information that could reveal a SAR filing require particular care. Follow secure submission instructions and consider getting legal advice before sharing sensitive or privileged material.

6. **Use the appropriate channel and keep a record.**

   Review FinCEN’s whistleblower program page for current submission instructions and scope. Depending on the issue, other regulators or law enforcement agencies may also have relevant channels. Keep a private, factual record of your own reporting steps, including dates and confirmation details, without retaining material you are not permitted to keep.

Keep a paper trail: Maintain a secure record of when you made a report, which channel you used, and any follow-up—while respecting confidentiality rules and avoiding unauthorized copying or storage of evidence.

Training and Getting Oriented

People who are new to BSA concepts may find it helpful to learn the basic terminology before describing a concern. ACAMS offers training resources and educational materials at acams.org. These resources can help readers understand AML concepts, but training materials are not a substitute for legal advice or an agency’s current filing instructions.

When reviewing any guidance, keep the distinction between a compliance concern and a legal finding in view. A person may have a reasonable basis to report facts without knowing the final legal analysis. Conversely, a broad allegation without specific, verifiable details may be difficult to assess.

Why BSA Whistleblower Tips Matter

Financial institutions often see patterns across transactions and customers that no single outside observer can readily identify. Employees and other insiders may know how controls work in practice, whether warnings were escalated, and whether written policies matched actual behavior. Their information can help authorities evaluate potential violations and identify evidence that might otherwise be difficult to locate.



That does not mean every internal disagreement belongs in a whistleblower submission, or that every submission will lead to enforcement. The strongest approach is measured: report what you can support, identify what remains uncertain, protect sensitive information, and use an appropriate channel. FinCEN's program page explains current requirements and procedures; consult qualified counsel for advice about your particular situation, confidentiality obligations, or potential retaliation concerns.

This article is general information, not legal advice. BSA duties, whistleblower eligibility, and reporting procedures can change and depend on the facts.