Submitting an anti-money laundering (AML) whistleblower tip does not automatically trigger an investigation, guarantee that the government will contact you, or mean that you will receive an award. It gives the government information to assess. What happens next depends on the tip's detail, credibility, relevance, and whether it points to a possible legal violation the authorities can investigate.

This guide explains the U.S. Bank Secrecy Act (BSA) whistleblower program, the role of the Financial Crimes Enforcement Network (FinCEN), and what to expect after filing. It also explains how a tip differs from a Suspicious Activity Report (SAR)—a report that certain financial institutions must file with FinCEN when they detect suspected suspicious activity.

What Is the AML/BSA Whistleblower Program?

The BSA is a federal law requiring financial institutions and other covered businesses to help detect and report money laundering and other financial crime. Its requirements include maintaining certain records, developing anti-money-laundering controls, and filing SARs when applicable.

The BSA whistleblower program allows people with relevant information to report possible violations to the U.S. Department of the Treasury, including through FinCEN, or to the U.S. Department of Justice (DOJ). Depending on the circumstances and the applicable rules, a person may also qualify for a monetary award if their information leads to a successful enforcement action and the legal requirements are met. An award is not automatic.

The program is distinct from a financial institution's internal reporting process. You may raise a concern with your employer, but doing so is not necessarily the same as submitting information to the government through the whistleblower program. Nor does filing with the government guarantee that your employer will learn about internal reporting compliance the tip—or that the government will keep every detail confidential in every possible circumstance.

Legal Origin and Timeline

The BSA whistleblower provisions were created by the Anti-Money Laundering Act of 2020. The National Defense Authorization Act for Fiscal Year 2023, signed on **December 23, 2022**, made significant changes to the program, including strengthening protections against retaliation and revising the potential award framework.

Those changes do not mean that every tip is investigated or that every eligible whistleblower receives money. The government must assess the information, decide whether to act, and, for an award, satisfy the relevant statutory conditions. Current instructions and program information should be checked directly on the FinCEN website, because procedures and guidance can change.

Who May Be Eligible—and What Counts as "Original Information"?

Eligibility depends on the law and the facts of the submission. A person may have information from work at a bank, money services business, casino, or another covered institution, or from another position that provided access to relevant facts. A whistleblower does not necessarily need to be an employee of the institution involved.

"Original information" generally means information based on the person's independent knowledge or independent analysis that is not already known to the government, subject to statutory rules and exceptions. Information drawn solely from public sources may not qualify unless it adds meaningful insight. A tip that simply repeats an already public allegation, without additional facts or analysis, may have limited value.



For example, a compliance analyst might identify that a bank repeatedly closed alerts involving the same group of accounts despite documented links to a suspected shell-company network. The analyst's firsthand knowledge of the alert history, escalation decisions, and relevant records may make the tip more useful than a general claim that the bank has weak controls.

Eligibility can be affected by how the information was obtained and the person's role. Restrictions or exceptions may apply to people involved in the alleged misconduct, certain government personnel, auditors, or people who learned information through privileged or otherwise protected communications. Do not assume that having inside information automatically makes you eligible.

What Violations Can a Tip Address?

The program covers certain violations within its statutory scope. The details matter: a poor control or suspicious transaction is not, by itself, proof that a law was broken. A useful tip connects specific conduct to facts that may show a covered violation.

Issue Example of potentially relevant information Important distinction SAR-related conduct Evidence that an institution knowingly failed to file required reports or improperly handled reporting obligations. A SAR is the institution's report to FinCEN; a whistleblower tip is information a person provides to the government. They are not interchangeable. Structuring Facts suggesting transactions were deliberately divided to evade reporting requirements. Multiple transactions below a threshold do not alone establish structuring or criminal intent. Customer due diligence (CDD) Evidence of deliberate failures involving required customer information, beneficial ownership, or risk-based controls. A control gap may warrant review, but whether it violates a legal requirement depends on the facts and applicable rules. Records and reporting Evidence that required records were falsified, concealed, destroyed, or not maintained as required. Describe what happened, when, and who was involved; avoid conclusions unsupported by facts. Sanctions or money laundering Transactions or decisions that may relate to covered sanctions violations or money-laundering offenses. Coverage depends on the particular law and conduct. A sanctions concern should be described precisely, not treated as automatically qualifying.

What Happens After You Submit a Tip?

1. The agency receives and logs the submission

After submission, the receiving agency may record the information and review it for completeness, subject matter, and potential relevance. A submission may be made through a designated government channel. Follow the current instructions on FinCEN's website and retain any confirmation or reference number provided.

Do not assume that the agency will provide a detailed status update. Government agencies may not confirm whether a matter is under review, whether an investigation has opened, or what steps investigators have taken.

2. The information is assessed for an investigation threshold

"Investigation threshold" is a practical way to describe the point at which authorities decide that information warrants further inquiry. It is not a promise that a case will be opened, and the precise internal assessment may not be public. Reviewers may consider whether the tip is specific, credible, within the agency's authority, and capable of being checked against records or other evidence.

Compare these two descriptions:

- **Vague:** "The bank helps criminals launder money."
- **More useful:** "From March through August, I reviewed alerts for these account relationships. The attached timeline identifies three escalations that were closed after a manager instructed staff not to include linked-company information. The records are held by the institution's AML team."

The second example gives investigators potential dates, records, and people or functions to examine. It still does not prove a violation, but it offers a clearer path for verification.

3. Agencies may compare the tip with other information

FinCEN or another government office may compare a tip with other reports, regulatory information, law-enforcement leads, or material from other agencies. A tip may be useful even if it does not result in immediate contact or a visible enforcement action. Authorities may also decide that the information is outside the program's scope, too general to pursue, already known, or not supported by available evidence.

4. Investigators may seek additional information

If officials need clarification, they may contact the whistleblower or a representative. Keep your account of events consistent and distinguish what you personally observed from what you heard from someone else. If you do not know an answer, say so rather than guessing.

Do not independently investigate suspected wrongdoing, confront people you believe are involved, or access systems or records without authorization. Preserve information lawfully and follow your organization's retention rules. Never remove or disclose a SAR, or reveal that a SAR was filed, unless the law and an authorized process permit it. SAR confidentiality rules are strict.



5. An enforcement action may—or may not—follow

An agency may open an investigation, refer information to another authority, take no further action, or pursue a resolution that is not publicly announced. Investigations can take substantial time. Even when an enforcement action occurs, it may be based on many sources of evidence, and the government may not explain how a particular tip contributed.

Potential whistleblower awards depend on statutory eligibility and the outcome of a qualifying action. A tip alone does not establish a right to payment. Do not rely on an anticipated award when making financial or employment decisions.

Confidentiality and Retaliation

Confidentiality matters, but it is not absolute secrecy in every situation. The law generally includes protections for a whistleblower's identity, subject to exceptions—for example, where disclosure is required for a proceeding or otherwise allowed by law. The agency's handling of identity may also depend on how the information is submitted and whether the matter moves into a legal process.

Before filing, consider whether your submission identifies you directly or indirectly. A distinctive job title, a small team, or details only one person could know may reveal your identity even if your name is withheld. Ask an attorney familiar with whistleblower matters about safe submission options and how confidentiality may apply to your circumstances.

The law also provides anti-retaliation protections in covered circumstances. Retaliation can include adverse workplace action connected to protected reporting, but whether a specific act is unlawful depends on the facts and applicable law. Keep a dated record of relevant events, preserve communications lawfully, and seek legal advice promptly if you believe you have faced retaliation. Do not use a work laptop, work email, or employer-controlled device for sensitive personal communications with an attorney.

What to Do Next: A Practical Checklist

1. **Write a factual timeline.** Note dates, transactions, decisions, people or roles involved, and how you learned each fact.

2. **Separate observation from inference.** Label what you saw directly, what a record shows, and what you suspect.
3. **Identify records without taking them improperly.** Describe where records are held and how investigators could locate them. Do not access materials you are not authorized to view.
4. **Protect SAR confidentiality.** Do not attach or circulate a SAR, or disclose its existence, outside an authorized process.
5. **Use official instructions.** Check FinCEN's website for current whistleblower submission information and keep your confirmation details secure.
6. **Consider independent legal advice.** An attorney can help assess eligibility, original information, confidentiality, and retaliation risks. Avoid anyone promising a specific award or outcome.
7. **Keep a secure record.** Store your own submission and related notes somewhere you control, not on an employer's device or account.

The Bottom Line

After you submit an AML whistleblower tip, the government may review it, test whether it meets an investigation threshold, compare it with other information, and decide whether to pursue further action. You may not receive updates, and an investigation or award is never guaranteed. The most helpful submissions are specific, grounded in firsthand knowledge or analysis, and careful about legal boundaries—especially the strict confidentiality rules surrounding SARs.