Anti-money laundering (AML) and Bank Secrecy Act (BSA) investigations can take years because investigators often have to reconstruct complicated financial activity across accounts, institutions, people, and borders. A suspicious transaction may be only one visible part of a much larger pattern. Finding out who controlled the money, where it came from, and whether the activity violated the law can require extensive records, analysis, and coordination.

That process can be difficult to see from the outside. A bank may file a Suspicious Activity Report (SAR), but the filing does not automatically mean that law enforcement has opened a case, that anyone has been accused of a crime, or that an investigation will conclude quickly. SARs are confidential, and agencies generally do not provide a public running account of investigative steps.



This article explains why AML and BSA investigations can take so long, what the federal whistleblower program is, and what someone considering a report should understand about eligibility and "original information." It is general information, not legal advice.

What the AML and BSA Whistleblower Program Is

The BSA is a federal law that requires certain financial institutions and other covered businesses to keep records and report specified financial activity. AML laws and regulations are intended to help detect and deter money laundering and related conduct. The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, administers the BSA and receives SARs and other required reports.

The BSA whistleblower program allows eligible people to provide information about certain violations to the Treasury Department. Under the program, a whistleblower who meets the legal requirements may qualify for a monetary award if the information leads to a successful enforcement action and the applicable monetary thresholds are met. An award is not automatic, and no one can guarantee that a tip will result in an investigation, enforcement action, or payment.

The program is distinct from a bank's internal reporting process. A worker might raise a concern with a supervisor or compliance department, report information to a government agency, or do both. Each route has different procedures and risks. People considering a report—especially current or former employees with access to

confidential records—should get advice from a lawyer familiar with whistleblower matters before sharing sensitive information.

Legal Origin and Timeline

The BSA whistleblower framework was created by the Anti-Money Laundering Act of 2020, enacted as part of the National Defense Authorization Act for Fiscal Year 2021. Congress later expanded and revised the framework in the National Defense Authorization Act for Fiscal Year 2023, signed on December 23, 2022. These changes strengthened the potential award structure and broadened aspects of the program.

That legislative history matters, but a statute alone does not answer every practical question a potential whistleblower may have. Reporting procedures, eligibility rules, confidentiality protections, and how claims are handled depend on the governing law and current agency guidance. FinCEN's website, at fincen.gov, is a useful place to look for official program information, instructions, and updates.

Separately, the life of an investigation may begin well before a whistleblower submits information. A bank may identify activity through monitoring, a regulator may refer a matter, or investigators may encounter financial records while examining another case. A SAR can be one lead among many, rather than the start—or the end—of the investigation.

Why Investigations Take Years

Complex transaction patterns take time to reconstruct

Suspicious activity rarely arrives as a neat, self-explanatory package. Investigators may need to compare transfers, cash deposits, payments, withdrawals, invoices, account openings, and communications over a long period. A pattern can be spread across multiple accounts or institutions and obscured by ordinary-looking transactions.



For example, a business might receive a series of payments that appear consistent with its stated operations. Investigators may later discover that the payments were routed through several related companies, followed by withdrawals or transfers that do not match the business's profile. To assess the activity, investigators may need to establish the source of funds, identify the people directing the transactions, and determine whether the pattern reflects criminal conduct, a compliance failure, or an innocent explanation.

Multiple entities can conceal who is in control

Companies, trusts, nominees, and intermediaries can make it difficult to identify the people who ultimately own or control assets. An investigation involving multiple entities may require corporate filings, account-opening records, beneficial ownership information, contracts, tax records, and evidence of who actually made decisions.

Names and addresses may differ across records. Entities may have been formed in different jurisdictions or used for legitimate business alongside suspect activity. Investigators must distinguish a complicated but lawful structure from one used to disguise ownership, evade reporting, or move illicit proceeds.

International components add legal and logistical barriers

When transactions cross borders, investigators may need records from foreign banks, payment providers, businesses, or government agencies. Different countries have different privacy laws, disclosure rules, and timelines for responding to formal requests. Records may need translation, verification, or authentication before they can be used in a proceeding.

International components can also mean that funds pass through several financial systems before reaching a destination. Each institution may hold only part of the picture. Coordinating with overseas authorities and tracing money across currencies and jurisdictions can take substantial time, even when investigators already have a strong lead.

Records must be gathered, checked, and connected

A financial investigation may involve millions of records. Investigators and analysts have to obtain relevant material, confirm its reliability, and organize it into a usable chronology. They may compare bank statements with invoices, shipping documents, tax filings, messages, or public records. A single discrepancy may need to be verified rather than treated as proof of wrongdoing.

Institutions may also need time to locate older records, especially when activity spans many years or involves systems that have changed. Law enforcement and regulators may have to use formal legal processes to obtain information, and those processes can be contested or delayed.

Agencies must establish what the evidence proves

Suspicious activity is not the same as a proven violation. Investigators need evidence that supports the elements of a particular offense or regulatory breach. They may examine intent, knowledge, control, reporting duties, and the relationship between transactions and underlying conduct.

They may also investigate explanations that weaken or contradict an initial theory. That can slow a case, but it is part of building a reliable record. In a criminal matter, prosecutors must assess whether the evidence can support charges and be presented in court. In a regulatory matter, agencies must follow their own procedures and establish the basis for enforcement.

What SARs Do—and Do Not—Show

A SAR is a report that a covered institution files when it detects activity that meets applicable reporting criteria. It can alert authorities to activity worth examining and can help connect information across institutions or investigations. SARs may describe transactions, accounts, people, and the reasons activity appeared suspicious.

A SAR is not a verdict. It does not, on its own, prove that a customer committed a crime or that the institution violated the law. An institution may file a report because activity is unusual or raises concerns, while investigators

later determine that there is a lawful explanation. Conversely, a SAR may lead investigators to other evidence that reveals a broader pattern.

SARs are confidential under federal law. People generally should not try to obtain or disclose a SAR itself outside authorized channels. A person with relevant knowledge can instead describe the underlying facts—such as transactions, dates, accounts, instructions, or control relationships—through an appropriate reporting process. FinCEN's website explains official reporting channels and related guidance.

Potentially Qualifying Conduct

The whistleblower program concerns certain violations of the BSA and related laws. The precise legal question depends on the facts and the statutory requirements. Examples of conduct that may be relevant include:

- **SAR-related violations:** A financial institution may have failed to file required reports, filed them late, or handled reporting duties improperly. The existence of a suspicious transaction alone does not establish that a reporting violation occurred.
- **Structuring:** A person may break up cash transactions to evade reporting requirements. Investigators examine the pattern and evidence of intent; a series of smaller transactions is not automatically illegal.
- **Customer due diligence:** Weaknesses involving customer due diligence (CDD), beneficial ownership, or ongoing monitoring may be relevant when they violate applicable requirements. A control failure and a customer's underlying crime are separate issues.
- **Recordkeeping:** Required records may be missing, inaccurate, or inadequately maintained. The relevant duty depends on the type of institution and the applicable rule.
- **Sanctions-related conduct:** Certain sanctions violations may fall within the expanded whistleblower framework. Sanctions law is separate from the BSA, so a potential reporter should verify the applicable rules and reporting route.

These are examples, not a checklist of guaranteed eligibility. The legal characterization of conduct depends on evidence, the responsible party, wrongful termination and the specific law that applies.

Eligibility and "Original Information"

"Original information" generally refers to information derived from a person's independent knowledge or analysis, rather than information already known to the government or obtained solely from public sources. The exact statutory standards and exceptions matter. A person does not necessarily need to have witnessed every transaction firsthand; useful information may come from analyzing records or connecting facts that were not previously understood together.

For example, an employee might know that several entities shared a decision-maker, saw recurring transfers that did not match stated business activity, and identified internal alerts that were repeatedly closed without investigation. Those concrete details may be more useful than a broad claim that "the bank is laundering money." Whether the information qualifies as original and whether a person is eligible are legal questions that depend on the facts.

Potential whistleblowers should also consider restrictions on who may receive an award and how information must be submitted. Duties tied to legal, compliance, audit, or government roles can affect eligibility. So can the source of the information and whether it was provided voluntarily and in the required manner. Do not assume that an internal report automatically satisfies federal program requirements—or that bypassing internal channels is always appropriate.

What to Do Next

1. **Write down what you know.** Record dates, entities, transaction types, decision-makers, and how you learned each fact. Separate direct observations from assumptions.
2. **Preserve information lawfully.** Do not access systems without authorization, remove confidential records, or send sensitive materials to a personal account. Avoid using a work laptop or work email for confidential legal communications.
3. **Do not disclose a SAR.** Describe the underlying activity rather than attempting to obtain or share a confidential report.
4. **Check official guidance.** Review FinCEN's website for current whistleblower information and reporting instructions.
5. **Consult qualified counsel.** A whistleblower lawyer can help assess eligibility, confidentiality, retaliation concerns, and the safest way to submit information.

Question Why it matters What specific conduct occurred? Investigators need facts that can be tested against a legal or regulatory requirement. Who controlled the accounts or entities? Ownership and decision-making may be obscured across multiple entities. Where did the money move? International components can require additional records and coordination. What is firsthand knowledge versus inference? Clear sourcing helps investigators evaluate reliability and helps counsel assess eligibility.

The Bottom Line

AML and BSA investigations can take years because complex transaction patterns, multiple entities, and international components create a large evidentiary puzzle. Investigators must gather records, identify who controlled the money, distinguish suspicious activity from proven violations, and coordinate across institutions and jurisdictions. A SAR can be an important lead, but it is not proof of wrongdoing or a guarantee of enforcement.

The whistleblower program gives eligible people a formal way to share information about certain violations, with the possibility of an award if statutory conditions are met. Anyone considering a report should focus on specific, lawfully obtained facts, check FinCEN's current guidance, and seek legal advice before sharing sensitive information.