"Original information" is a central concept in the Anti-Money Laundering (AML) whistleblower program. It can determine whether a report may help authorities investigate a financial institution or other business—and whether the person who provided it may qualify for an award. But original does not necessarily mean secret, never-before-seen, or based on a document you personally created.

In general, the key question is whether you can provide useful information based on your **direct knowledge** or **independent analysis**, rather than simply repeating allegations already available to regulators or the public. The details matter: what you observed, how you learned it, when you reported it, and whether officials already knew it can all affect eligibility.

This guide explains the program, the legal timeline, the meaning of original information, and the kinds of conduct that may matter. It is general information, not legal advice. Whistleblower rules are technical, and people considering a report should get advice from a lawyer experienced in whistleblower matters.

What Is the AML/BSA Whistleblower Program?

The Bank Secrecy Act (BSA) is a federal law that requires financial institutions and certain other businesses to maintain records and help detect and report potential money laundering and other financial crime. FinCEN, the Financial Crimes Enforcement Network, administers key parts of the BSA and receives many reports about suspicious activity.

The BSA whistleblower program provides a way for people to give information to the government about possible violations. Under the law, a person who provides qualifying information may be eligible for an award if that information leads to a successful enforcement action resulting in sufficiently large monetary sanctions. The program also includes protections against retaliation for certain lawful whistleblower disclosures.

It is not a private lawsuit system in which a whistleblower automatically receives a share of money simply for submitting a tip. Authorities decide whether to investigate, whether to bring an action, and whether the statutory requirements for an award have been met. An award is not guaranteed.

Legal Origin and Timeline

The BSA's whistleblower provisions were expanded by the Anti-Money Laundering Act of 2020, which was enacted as part of the National Defense Authorization Act for Fiscal Year 2021. The law created an award framework and protections for certain whistleblowers *aml whistleblower* who report BSA violations.

Congress later strengthened and clarified that framework in the Anti-Money Laundering Whistleblower Improvement Act, included in the National Defense Authorization Act for Fiscal Year 2023. President Biden signed that act on **December 23, 2022**. Among other changes, the law addressed award funding and increased the potential reward structure for qualifying whistleblowers.

The statute generally provides for an award of 10% to 30% of monetary sanctions collected in qualifying actions when the statutory conditions are satisfied, including the applicable threshold for sanctions. The amount is not automatic: the government determines eligibility and award amounts under the law. Consult current FinCEN guidance and a lawyer for the rules that apply to a particular report.

Who May Be Eligible?

The program is not limited to bank employees. Depending on the facts, a person with information about a possible BSA violation may be able to report it. That could include an employee, contractor, former employee, customer, business partner, or another person with relevant knowledge.

Eligibility depends on more than a person's job title. The information generally must be provided voluntarily and in the manner required by the program. It must also relate to a violation within the program's scope and contribute to a successful enforcement action. Statutory exclusions and other limits may apply—for example, in circumstances involving a person's role in the misconduct or information obtained through certain restricted channels.

People who believe they may have participated in conduct under investigation should not assume they are either eligible or ineligible. Their role, the timing of their disclosure, and other legal issues can be significant. A lawyer can assess those questions before a submission is made.

What Does "Original Information" Mean?

For whistleblower purposes, original information generally means information derived from a person's **independent knowledge or independent analysis** that is not already known to the government from another source, subject to exceptions and detailed rules. It must also be provided in a way that satisfies the law and applicable procedures.

Direct knowledge

Direct knowledge is information you learned through your own experience, work, or observations—not merely something you heard repeated by someone else. For example, a compliance analyst who reviewed a transaction alert may have direct knowledge of the alert, the review steps taken, and the decision to close the case. A person who only heard a colleague say that "the bank ignores suspicious activity" may have an allegation worth looking into, but that statement alone is less likely to provide a solid factual basis.

Direct knowledge does not require witnessing a crime. An employee may have first-hand knowledge of a process, control failure, instruction, or record that helps authorities understand whether a violation occurred.

Independent analysis

Independent analysis means drawing a new insight from information that may be available to others. It can involve connecting records, identifying a pattern, or explaining why separate facts indicate a potential violation. The analysis should reflect your own reasoning, not simply reproduce a conclusion already published by someone else.

For example, suppose a person reviews transaction data they were authorized to access and identifies repeated transfers just below a reporting threshold, involving related customers and the same business. The records may not be secret individually, but the pattern and explanation may be an independent analysis. Whether it qualifies depends on the facts, the source of the data, and what the government already knows.

Not public sources is not the whole test

Information that comes entirely from public sources—such as news stories, public court filings, or government reports—may face limits under the original-information rules. But "not public sources" is not a complete legal test. Information is not automatically disqualified just because some of the underlying facts are public. A person's independent analysis may add something meaningful, and there are exceptions where a whistleblower's contribution helps authorities in a significant way.

Conversely, nonpublic information is not automatically original. A confidential rumor, a copied internal report, or information already in the government's possession may not qualify simply because it was not published online. The source, originality, timing, and value of the information all matter.

How Suspicious Activity Reports Fit In

A Suspicious Activity Report (SAR) is a report that certain financial institutions and other covered businesses must file with FinCEN when activity meets applicable reporting requirements. SARs can be important to law enforcement and regulators, but they involve strict confidentiality rules.

A whistleblower should not assume that they may take, copy, or disclose a SAR—or confirm that one exists. SAR confidentiality can apply to the report and information that would reveal its existence. A person who encountered suspicious activity through their work may be able to report the underlying facts through an authorized channel, but how to do so safely depends on the person's role and the information involved.



For example, an employee might describe transactions, customer behavior, internal instructions, or a decision not to escalate a concern, without attaching a SAR or disclosing its contents. Before sharing internal materials, get legal advice about confidentiality, privacy, employment obligations, and the proper reporting process. Do not remove records you are not authorized to take.

What Types of Violations May Qualify?

Potentially relevant conduct can involve more than a failure to file a SAR. The details and applicable law determine whether conduct is a BSA violation or another matter within the program's scope. Examples may include:

- **SAR-related failures:** Failing to file a required report, filing it late, or using a process that prevents meaningful escalation of suspicious activity.
- **Structuring:** Breaking up transactions to evade reporting or recordkeeping requirements. A pattern of deposits just below a threshold may warrant review, although a transaction pattern alone does not prove intent or a violation.
- **Customer due diligence:** Failures in customer due diligence (CDD), such as deficiencies in identifying or understanding customer relationships and risks where the law requires those controls.

- **Records and reporting:** Missing, inaccurate, or improperly maintained records or other failures to meet BSA recordkeeping and reporting obligations.
- **Sanctions-related conduct:** Transactions involving prohibited parties or jurisdictions may raise sanctions issues, which can involve laws and agencies beyond the BSA program. A report may need to identify the relevant legal regime rather than assume every sanctions concern is a BSA violation.

A strong report distinguishes observed facts from conclusions. “I reviewed these five transactions on these dates and found the same customer identifier” is more useful than “the company is laundering money.”

Examples: Original Information or Not?

Situation Why it may matter An employee describes a specific alert they reviewed and an instruction to close it without required follow-up. First-hand detail about a review and an internal decision may provide direct knowledge. A person identifies a new pattern by connecting transaction records they lawfully accessed. The pattern may reflect independent analysis, even if some underlying facts are available elsewhere. A tip repeats allegations from a news article without adding facts or analysis. Information derived solely from public reporting may not meet the original-information standard. A person forwards a SAR or reveals that a specific customer was the subject of one. This can raise serious confidentiality concerns. The person should seek legal advice before disclosing SAR-related information.

What to Do Before Reporting

Careful preparation can help a person explain what they know without creating avoidable risks. Consider these steps:



1. **Write down the facts.** Note dates, events, people involved, systems or processes, and what you personally observed. Separate facts from assumptions.
2. **Identify your source.** Explain whether each point comes from direct knowledge, documents you lawfully accessed, or independent analysis.
3. **Keep the chronology clear.** Record when you first learned the information and whether you raised it internally or with a regulator.

4. **Preserve information lawfully.** Do not access systems without authorization, alter records, or take documents you are not entitled to possess. Do not put sensitive material on a personal device without legal advice.
5. **Protect SAR confidentiality.** Do not disclose a SAR or information that could reveal its existence without advice about the rules and an appropriate reporting channel.
6. **Consult an experienced lawyer.** Ask about eligibility, reporting procedures, confidentiality, retaliation protections, and possible conflicts before submitting sensitive information.
7. **Check official guidance.** Review current materials on the FinCEN website at fincen.gov. Procedures and guidance can change.

The Bottom Line

Original information is not simply information no one has ever seen. It is generally information grounded in a whistleblower's direct knowledge or independent analysis that adds value beyond what authorities already know, subject to specific legal rules. A person may contribute by explaining how a control failed, documenting what they personally observed, or uncovering a meaningful pattern in records they were authorized to review.

At the same time, a report does not guarantee an investigation, an award, or protection in every circumstance. SAR confidentiality and limits on handling internal records deserve particular care. Focus on accurate, specific facts; distinguish what you know from what you suspect; and get legal advice before sharing sensitive information.