Possibly. Reporting suspected money laundering or another financial crime may be protected, but that does not automatically give you permission to copy, remove, or disclose every workplace document that might support your report. The answer can depend on what the records contain, how you accessed them, what you did with them, and whether special confidentiality rules apply.

This distinction matters especially in anti-money-laundering cases. Suspicious Activity Reports (SARs) and information revealing that a SAR exists are subject to strict confidentiality rules. Customer data, trade secrets, and records covered by a confidentiality agreement may raise additional concerns. A whistleblower lawyer can help you assess how to report what you know without creating avoidable legal or professional risks.

This article offers general information, not legal advice for your specific situation.

What Is the AML/BSA Whistleblower Program?

The Bank Secrecy Act (BSA) is a federal law that requires financial institutions to maintain certain records and help detect and report suspected money laundering and other financial misconduct. The Anti-Money Laundering (AML) whistleblower program allows people with relevant information to report certain violations to the U.S. Department of the Treasury, including through the Financial Crimes Enforcement Network (FinCEN).

FinCEN is the Treasury bureau that administers the program. Its website, fincen.gov, provides information about BSA and AML matters. The law may allow an eligible whistleblower to receive an award when original information leads to a successful enforcement action and the other statutory requirements are met. It also provides protections against certain forms of retaliation.

These provisions do not create a blanket license to take company records. A reporting right and a right to possess or disclose a particular document are different questions. A person may be allowed to report suspected misconduct while still facing legal or workplace consequences for obtaining or sharing records improperly.

Legal Origin and Timeline

The core BSA whistleblower provisions were established by the Anti-Money Laundering Act of 2020, which became law on January 1, 2021, as part of the National Defense Authorization Act for Fiscal Year 2021. Congress later amended and strengthened the program through the National Defense Authorization Act for Fiscal Year More help 2023, signed on December 23, 2022.

The later legislation addressed important features of the program, including potential awards and protections. The rules and procedures for making a claim can change, so check current FinCEN guidance and consult a lawyer familiar with whistleblower matters before submitting information or seeking an award.

Who May Qualify—and What Counts as “Original Information”?

In general, an individual may qualify if they voluntarily provide the Treasury Department with original information about a covered violation and that information contributes to a successful enforcement action meeting the program’s requirements. Eligibility is fact-specific; simply having documents or being the first person to raise a concern internally does not automatically qualify someone.

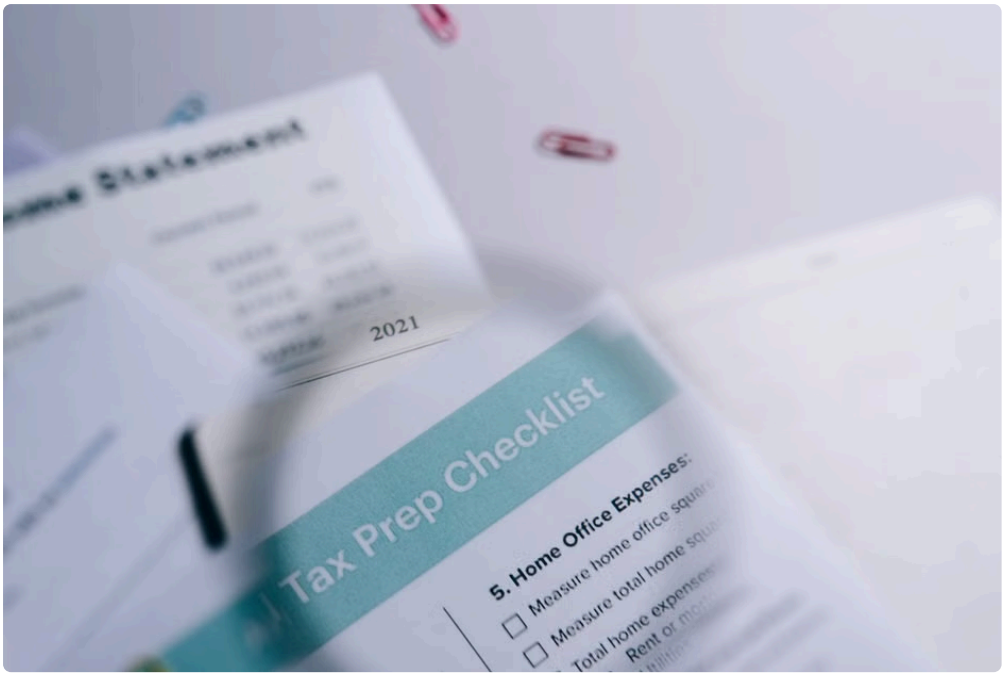
“Original information” generally means information derived from the person’s independent knowledge or analysis, not information already known to the government from another source. It may be based on documents, but a

whistleblower does not necessarily need to take documents to provide useful information. A clear account of what happened—who was involved, when it occurred, which controls failed, and where relevant records are maintained—may help authorities assess the allegation.

Some people may be excluded or face limits based on how they obtained the information or their role in the misconduct. Rules can also apply to information obtained through certain official duties, legal representation, or audits. Because the details matter, get individualized advice before assuming that you qualify.

What Violations Can Be Relevant?

The program covers certain violations of the BSA and related AML requirements. Potentially relevant conduct may include:



- **SAR-related failures:** A financial institution may fail to file required Suspicious Activity Reports, file them late, or submit reports that omit important information.
- **Structuring:** People may divide transactions into smaller amounts to evade reporting or recordkeeping requirements. A report might describe an institution's role in facilitating, ignoring, or failing to identify suspected structuring.
- **Customer due diligence (CDD):** CDD refers to steps financial institutions take to understand customers and assess risk. Potential issues may include inadequate customer identification, weak beneficial-ownership information, or failures to monitor risk as required.
- **Recordkeeping and reporting:** This can include failures to maintain required records, monitor transactions, or meet applicable BSA reporting obligations.
- **Sanctions-related conduct:** Facts about possible sanctions evasion or related financial activity may be relevant to authorities. Whether a particular matter falls within the whistleblower program depends on the law and the enforcement route.

A suspicious transaction is not automatically proof of a violation. Your report should distinguish what you personally observed from what you infer, and should avoid overstating what the evidence shows.

Why Taking Documents Can Create Risk

There is no universal answer to whether copying a document is lawful. Relevant factors include your job duties, the system you used, your access permissions, the type of information, the reason for copying it, and what you did with the copy. A lawyer can help evaluate applicable federal and state laws, employment agreements, and internal policies.

Record or conduct Why it may be sensitive Safer first step SAR or information revealing a SAR's existence Federal law generally restricts disclosure of a SAR and information that would reveal one exists. Do not copy, forward, or attach it without specific legal guidance. Describe the concern to counsel without disclosing the SAR itself. Customer records or account data May contain personal, financial, or confidential information. Record what you observed and where the information is kept; ask counsel how to handle any supporting material. Trade secrets or internal business material Trade secret obligations and confidentiality agreements may restrict use or disclosure, though they may not prevent lawful reporting to government authorities. Do not send broad files or unrelated proprietary material. Get advice on a narrow, appropriate disclosure. Records obtained through unauthorized access Accessing systems or files outside your authorization can create separate legal and employment issues. Do not bypass controls, use another person's credentials, or continue accessing material. Seek legal advice promptly.

SAR Confidentiality Is a Special Concern

Federal law generally prohibits a financial institution and its employees from disclosing a SAR or information that would reveal the existence of a SAR, except in authorized circumstances. This rule is not simply another confidentiality clause. It can apply even when a person believes the SAR is evidence of wrongdoing.

That does not mean you should stay silent about suspected misconduct. It means you should avoid casually copying or sharing the SAR itself, naming a SAR's existence to unauthorized people, or attaching SAR material to an email or submission without legal advice. A lawyer can help you describe the underlying conduct and determine whether, and how, relevant information may be provided through an authorized channel.

Confidentiality Agreements and Trade Secret Obligations

Confidentiality agreements do not necessarily prohibit lawful reporting of possible violations to the government. But they also do not give you unlimited permission to use or distribute company information. Trade secret obligations, privacy rules, customer-confidentiality requirements, and other legal duties may still matter.

Do not assume that labeling a file "evidence" or sending it only to a personal account makes the disclosure lawful. Nor should you assume that an employer's policy can override every legal whistleblower protection. The safest course is to have counsel review the specific agreement, records, and proposed reporting method.

How to Prepare a Report Without Taking Unnecessary Risks

1. **Write a factual timeline.** Note dates, people or roles involved, transactions or control failures, and what you personally observed. Separate firsthand knowledge from assumptions.
2. **Preserve what you are authorized to retain.** Do not delete, alter, conceal, or destroy records. Do not remove original files or create a large personal archive.
3. **Do not expand your access.** Avoid bypassing permissions, using another employee's login, or searching for records outside your normal duties.
4. **Get independent legal advice.** A whistleblower attorney can discuss eligibility, confidentiality agreements, trade secret obligations, SAR restrictions, and safe ways to present information.
5. **Use appropriate reporting channels.** Counsel can help determine whether to contact FinCEN or another agency and how to submit information without exposing restricted records.

6. **Keep the matter private.** Avoid discussing the report with coworkers, posting details online, or sending sensitive files through personal email or messaging apps.

What If You Already Took or Sent Documents?

Do not panic, but do not make the situation worse. Do not forward the material to additional people, upload it to a public or shared service, or destroy it to hide what happened. If a SAR or information that could reveal a SAR is involved, tell your lawyer promptly and avoid further disclosure. Explain what was copied, when, how it was accessed, and who received it. Preserve relevant communications and follow counsel's advice about the next steps.



Also, do not use a work laptop, work email, or employer-managed device to seek confidential legal advice. If you are concerned about monitoring, use a personal device and account, while avoiding the transfer of company records to them. Ask your lawyer how to communicate securely.

What to Do Next: Quick Checklist

- Write down the key facts from memory, with dates and specific examples.
- Do not access new files or take additional records to strengthen your case.
- Do not disclose a SAR, or information revealing that one exists, without legal guidance.
- Review the issue with an independent lawyer before submitting documents or contacting coworkers about the report.
- Check current whistleblower information on FinCEN's website.

The Bottom Line

You may have a protected right to report suspected BSA or AML violations, and confidentiality agreements do not automatically erase that right. But whistleblower protections are not blanket immunity for taking documents. SARs carry particularly strict confidentiality rules, while customer data, trade secrets, and unauthorized access can create other risks.

Focus first on recording what you know, preserving records you are authorized to retain, and getting legal advice before copying or sharing sensitive material. That approach can help you report responsibly while limiting avoidable exposure.