Submitting information to the Financial Crimes Enforcement Network (FinCEN) can feel like the end of a long process. It is better to treat it as the beginning of a careful recordkeeping process. A clear record of what you sent, when you sent it, and what supporting material you included can help you answer questions later and avoid confusion about what your submission actually said.

This guide explains how to document a FinCEN whistleblower submission, organize relevant information, and prepare for possible follow-up. It is general information, not legal advice. If you are considering a submission involving confidential business information, a suspicious activity report (SAR), or records you accessed through work, consider speaking with a qualified attorney before sharing anything.

What FinCEN Is and What It Does

FinCEN is a bureau of the U.S. Department of the Treasury. It administers and enforces parts of the Bank Secrecy Act (BSA), collects and analyzes financial data, and supports law enforcement and other authorities working to identify and investigate financial crime. Its work includes combating money laundering, terrorist financing, sanctions evasion, and other illicit activity.

FinCEN's whistleblower program provides a way for eligible individuals to report certain violations of the BSA and related laws. The program page explains how to submit information and provides current program details. Read the instructions on FinCEN's whistleblower program page before submitting; procedures and requirements can change. Do not assume that a particular submission qualifies for an award or that an award is guaranteed.

BSA and SAR Reporting Basics

The BSA requires certain financial institutions and other covered businesses to maintain records, establish compliance programs, and report specified activity. One important reporting tool is the SAR. Financial institutions file SARs with FinCEN when they know, suspect, or have reason to suspect that a transaction involves unlawful activity, is designed to evade BSA requirements, lacks an apparent lawful purpose, or otherwise meets applicable reporting standards.

A SAR is generally a regulated institution's report—not a public complaint form for an individual to fill out. If you are an employee or contractor, do not assume you may copy, keep, or disclose a SAR or information identifying its existence. SAR confidentiality rules are strict. Follow your organization's policies and get legal advice before handling or sharing SAR-related material.

A whistleblower tip and a SAR serve different purposes. A tip may describe suspected misconduct or a pattern of violations for FinCEN to assess. It does not replace an institution's reporting obligations, and making a tip does not authorize you to access records you are not permitted to access.

What Conduct May Be Reportable?

Relevant conduct can include suspected BSA violations, such as failures to maintain an effective anti-money laundering program, inadequate customer due diligence, failures to file required reports, or efforts to evade reporting and recordkeeping rules. A concern may also involve activity such as money laundering, the use of shell companies to obscure ownership, or transactions designed to hide the source or destination of funds.

Examples can help explain the difference between a specific factual concern and a general suspicion:

- **Observed:** You personally reviewed transaction records through an authorized role and saw repeated transfers structured just below a reporting threshold.
- **Heard:** A colleague told you that a manager directed staff to avoid filing reports. You did not witness the instruction yourself.
- **Observed:** You saw a documented control failure, such as a required review being marked complete without the review taking place.
- **Heard:** Someone outside your team said a customer was involved in laundering, but provided no records or first-hand details.

These examples are not legal conclusions. Whether conduct is a violation depends on the facts, applicable rules, and context. Be precise about the source of each statement: what you saw, what you heard from someone else, and what you inferred. Do not present an inference or second-hand account as personal knowledge.

Prepare a High-Quality Tip Before You Submit

A useful tip is understandable, specific, and candid about uncertainty. It should help a reader identify the people or entities involved, the relevant activity, the approximate timeframe, and why you believe the conduct may matter. Avoid exaggeration, speculation presented as fact, or long narratives that bury the central issue.

Build a factual outline

1. **Describe the concern.** State the suspected conduct in plain language and identify the main issue.
2. **Give the timeframe.** Use dates or ranges where possible. Mark estimates as estimates.
3. **Identify the source.** For each important fact, note whether you observed it directly, learned it from another person, or inferred it from records.
4. **Explain the significance.** Connect the facts to the possible reporting or compliance concern without claiming certainty you do not have.
5. **List supporting material.** Describe relevant records and where they came from, but do not collect or transmit material you are not authorized to possess or disclose.

Before sending anything, review FinCEN's current instructions and any applicable confidentiality obligations. Be especially careful with customer data, personal information, privileged communications, internal investigations, and SAR-related information. Limit copies and access to what is necessary, use secure storage, and ask counsel about safe handling when in doubt.

Keep a paper trail: Maintain a dated note of the steps you took to prepare the submission, including what you reviewed, what you excluded, and any advice you received. Keep it factual and avoid adding sensitive information unnecessarily.

How to Keep a Record of Your Submission

Your goal is to create a reliable record without creating an unnecessary second collection of sensitive data. Keep a record of the submission itself and enough information to identify its contents. Do not assume that every attachment should be copied to a personal device or personal email account. Follow the submission instructions, your legal advice, and any security or confidentiality rules that apply to you.



Record What to note Handling reminder Save submission copy A copy of the final narrative, answers, and any permitted attachments, if you can lawfully retain them. Store securely; do not keep restricted material in an unapproved location. Submission date log Date and time, time zone, method used, and any confirmation or reference number displayed. Record what the system actually showed; do not infer that a submission was accepted unless confirmed. Evidence inventory Attachment name, brief description, date range, source, and whether it was included. Inventory is not permission to retain or disclose the underlying records. Follow up readiness A secure way to receive messages, the contact details you provided, and a note of any response deadline. Check the contact method you supplied, while avoiding unsolicited disclosure of sensitive information.

Make a submission date log

As soon as you submit, record the date and time, including the time zone. Note the submission method, the page or portal used, and any confirmation number, receipt, or on-screen message. If you do not receive a confirmation, write that down too. Keep the log factual: “No confirmation appeared” is more useful than guessing whether the submission went through.

Keep a paper trail: Save the log in a secure location and note when you created or updated it. If you later correct an entry, preserve the original note and add a dated correction rather than silently replacing it.

Save a submission copy safely

If permitted, save the final version of your narrative and the materials actually submitted. If retaining a full copy would create a confidentiality, employment, privacy, or security concern, ask an attorney how to document the submission without keeping prohibited records. A brief index or factual log may be safer than duplicating underlying documents.

Use a secure, access-controlled location. Avoid forwarding sensitive material to a personal account or storing it on a shared device unless you have confirmed that doing so is allowed and safe. Restrict access to people who have a legitimate need to know. Do not alter the saved submission; if you need to make a later version, label it clearly and keep the dates distinct.

Keep a paper trail: Record where the copy or index is stored, who can access it, and any later transfer or deletion required by applicable policy or legal advice.

Create an evidence inventory

An evidence inventory is a concise index—not a substitute for the evidence itself. It can record an item's name, general description, date range, source, and whether it was submitted. Note whether you observed the item directly or learned about it from someone else. If you know how a record was obtained, describe that accurately; do not guess or conceal a questionable source.

For example, an inventory entry might say: "Spreadsheet, transactions from March–June, viewed in authorized work system, summary information included in tip; original not retained." That is clearer than a vague entry such as "proof of transfers." Keep customer names and account details out of the inventory unless they are necessary and you are authorized to retain them.

Keep a paper trail: Date the inventory and note who prepared it. If it changes, record what changed and why.

Be Ready for Follow-Up

Follow up readiness means being able to understand and respond to a legitimate request without scrambling to reconstruct your account. Keep your factual timeline, submission date log, and evidence inventory organized. Note the contact details you provided and check that channel periodically, while following any instructions about secure communications.

If someone contacts you claiming to represent FinCEN, verify the request through an appropriate official channel before sending sensitive information. Do not send additional documents merely because someone asks. Confirm what is requested, whether you are authorized to provide it, and how it should be transmitted. Keep a lexinter.net record of the request and your response.



ACAMS offers anti-money laundering training resources that may help readers understand BSA concepts and compliance practices. Explore the resources at ACAMS. Training can provide useful background, but it does not determine whether a specific event is reportable or replace advice from a qualified lawyer.

Keep a paper trail: Log follow-up contacts, dates, the method used, what was requested, what you provided, and any next steps. Distinguish your own conversation or observation from what another person told you.

Common Recordkeeping Mistakes to Avoid

- Relying on memory instead of making a dated log promptly.
- Keeping restricted records, including SAR-related material, in a personal account or device without authorization.
- Calling second-hand information “something I saw.”
- Changing the saved version of a submission without preserving the original or noting the revision date.
- Sending extra sensitive documents without confirming that they are relevant, permitted, and securely transmitted.
- Assuming a submission guarantees an investigation, a response, or an award.

A Practical Closeout Checklist

- Read FinCEN’s current whistleblower instructions.
- Separate direct observations, information heard from others, and your own inferences.
- Record the submission date, time, method, and any confirmation.
- Save a permitted copy or a safe index of what was submitted.
- Prepare an evidence inventory that identifies sources and limits unnecessary sensitive details.
- Store records securely and restrict access.
- Keep dated notes of preparation and follow-up, and seek legal advice about confidentiality or document handling concerns.

Good records make your account easier to explain and help you remember exactly what you sent. The central discipline is simple: document what you personally know, label what you learned from someone else, and keep a careful paper trail without creating unnecessary copies of protected information.