

EMPLOYEE ANTI-FRAUD REPORTING GUIDE

veriff 

How to File a Suspicious
Activity Report (SAR)



Introduction

You have a critical role in protecting your company, your users, and safeguarding the financial system from fraud and illicit activities. This guide provides a non-exhaustive step-by-step process example for identifying and reporting suspicious activity, ensuring compliance with anti-money laundering (AML) regulations.



STEP 1 UNDERSTAND WHY REPORTING MATTERS

- **Protect the Company:** Prevent financial crimes, reputational damage, and regulatory penalties.
- **Protect the Financial System:** Safeguard the integrity of global financial markets and your business.
- **Meet Legal Obligations:** Most jurisdictions require financial institutions to report suspicious activity to authorities.

STEP 2 RECOGNIZE RED FLAGS

Suspicious activity often reveals itself through warning signs that deviate from a customer's normal behavior.

Examples of Red Flags:

- **Unusual Transaction Patterns:** Large cash deposits or withdrawals inconsistent with the customer's profile; frequent transactions just below reporting thresholds; sudden unexplained changes in behavior.
- **Suspicious Customer Behavior:** Reluctance to provide identification; nervous, evasive, or overly secretive demeanor; inconsistent or vague explanations about source of funds.
- **Complex or Unnecessary Transactions:** Use of multiple accounts or intermediaries without clear purpose; reliance on shell companies or offshore accounts.
- **Other Indicators:** Transactions involving high-risk countries or industries; attempts to avoid compliance procedures (e.g., refusing to complete forms)

STEP 3 DOCUMENT AND REPORT

- Record the suspicious activity clearly and factually.
- File a Suspicious Activity Report (SAR) following company procedures.
- Submit promptly to the designated compliance officer or regulatory authority.

THE 5 STEPS FOR REPORTING SUSPICIOUS ACTIVITY

Follow these steps carefully and take into account specific steps and reporting channels outlined in applicable Anti-Money Laundering law. Do not investigate on your own. Your role is to Detect, Document, and Report internally.



STEP 1 DETECT AND IDENTIFY

Your first responsibility is to stay vigilant. Trust your instincts—if something feels “off,” it’s worth a closer look.

What to Look For:

- Does the transaction align with the customer’s usual behavior?
- Is the customer acting secretive, nervous, or evasive?
- Are the provided documents (e.g., IDs, business records) unclear, incomplete, or potentially fake?
- Is the activity unnecessarily complex or inconsistent with the customer’s profile?

Practical Example:

A customer who typically deposits \$1,000 per month suddenly deposits \$50,000 in cash, claiming it’s a “gift from a friend” but cannot provide supporting documentation.

STEP 2 DOCUMENT THE “NARRATIVE”

Immediately and privately, write down everything you observed. This internal “narrative” is critical for regulatory authorities to assess the situation. Be objective, factual, and thorough.

How to Document:

- Use the “**5 Ws**” Framework:
 - **Who:** Who conducted the activity? (Include customer name, account number, etc.)
 - **What:** What was the activity? (Transaction type, amounts, dates.)
 - **When:** When did it occur? (Date and time.)
 - **Where:** Where did it happen? (e.g., Online, in-person, at which branch.)
 - **Why:** Why did it seem suspicious to you? (This is the most important part. For example: “Customer claimed to be unemployed but attempted to deposit \$50,000 in cash, stating it was a ‘family gift.’”)

Pro Tip:

Stick to facts. Avoid assumptions or personal opinions.

STEP 3 REVIEW AND ESCALATE

Do not attempt to investigate further or ask the customer probing questions without being directed to do so by regulatory authorities. Your next step is to escalate your documented findings to relevant authority immediately.

Action Steps:

- Send your documented narrative directly to:
 - [Your Company's AML/Compliance Officer Name or Department]
 - [Compliance Email Address or Reporting Portal Link]
- Ensure the report is submitted securely and confidentially.

What Happens Next: Once you've submitted your report, your role in the initial alert is complete. Your company's compliance team should take over from here.

STEP 4 FILING (COMPLIANCE OFFICER'S DUTY)

This step is for your awareness. Usually a Compliance Officer or designated team within your company should be trained to handle the next steps.

- **Investigation:** The Compliance Officer will review your narrative, analyze the account holistically, and determine if the activity meets the legal threshold for reporting.
- **Filing:** If confirmed, the Compliance Officer will file a Suspicious Activity Report (SAR) or equivalent report with the appropriate regulatory authority in your country. Filing timelines and requirements vary by jurisdiction, but this is typically required within a specific timeframe (e.g., 30 days).

STEP 5 RETAIN (OUR LEGAL OBLIGATION)

Your company is typically required by law to securely maintain all records related to the SAR.

Requirement:

- All documentation, including your initial narrative and the SAR itself, should be securely stored for a minimum period as required by local regulations (e.g., 5 years from the date of filing).

CRITICAL: DO NOT “TIP OFF” THE CUSTOMER

It is a criminal offense in most jurisdictions to “tip off” any person involved in the transaction that a SAR has been, or is about to be, filed. This is the most important rule to remember.

DO NOT:

- Tell the customer (or any other employee not involved in compliance) that you are filing a suspicious activity report.
- Make copies of your narrative or the SAR for personal records.
- Allude to the report in any way (e.g., “I have to report this to my manager” or “This transaction is being flagged”).

Why This Matters: Tipping off a customer can compromise investigations and is punishable by law.

WHAT TO DO AND SAY INSTEAD:

Your goal is to remain calm, professional, and non-confrontational.

If a customer asks	Do not say Tipping Off	Do say Safe & Professional
1. "Why is this taking so long?"	"I have to get this large transaction approved by my compliance team"	"We just need to follow our standard processing procedures. Thank you for your patience"
2. "Why do you need all this information?"	"We have to report this to the government"	"To protect our customers, we are required to collect and verify this information for all transactions. It's a standard regulatory requirement"
3. If you must decline the transaction	"I can't complete this; it's too suspicious"	"I am unable to complete this transaction at this time." [If pressed, you may say, "This transaction does not meet our firm's current processing policies"]

Question 01: What if I'm not sure if something is suspicious?

A: **When in doubt, report it.** It is not your job to be 100% certain. It is your job to report anything that seems suspicious. Your Compliance team will determine if it's truly reportable. You are protected for reporting in "good faith."

Question 02: What if I'm wrong and it's a "false alarm"?

A: There is **no penalty** for reporting something in good faith that turns out to be legitimate. You need to be cautious. It is safer for business to report 10 "false alarms" than miss one real threat.

Question 03: What if it's a long-time, friendly customer?

A: The rules and your legal obligation apply to **all customers** equally, regardless of how long you have known them. Reporting can even protect a good customer if their account has been compromised by a fraudster.

CUSTOMIZING FOR YOUR COUNTRY

To make this guide fully compliant with your country's regulations:

- Replace "[Your Company's AML/Compliance Officer Name or Department]" with the appropriate contact details.
- Update "[Compliance Email Address or Reporting Portal Link]" with your reporting system used in the country where you are licensed.
- Confirm the SAR filing timeline and record retention period for your jurisdiction (e.g., 30 days for filing, 5 years for retention; as may differ from country to country).

Questions?

If you have any questions or need further guidance, contact the Compliance Department

Disclaimer:

This guide is an informational template, not legal advice. Anti-Money Laundering (AML) and Suspicious Activity Report (SAR) laws differ significantly by country.

You must consult your own legal and compliance teams to ensure this guide is fully adapted to your company's policies and all applicable laws in your jurisdiction. This document is not a substitute for professional legal counsel.



Veriff is a global identity platform helping businesses build trust online. Our AI-native technology combines automation and human expertise to quickly and accurately verify users worldwide with minimal friction.

Our trust infrastructure helps businesses stay compliant, prevent fraud, protect users, and scale globally, enabling a safer, more transparent internet for everyone.

Speak to one of our fraud experts today to discover how we can create customizable fraud protection for your business:

veriff.com