

Tab 1

## [Design](#)

**Authors:** Alisa Abramova, Julia Andreeva

**URL:** /suspicious-transaction-report

**Meta title:** Suspicious Transaction Reports (STRs): A 2025 Guide for Regulated Businesses | The Sumsuber

# Suspicious Transaction Reports (STRs) in 2025: The Latest Guidance for Regulated Businesses

**Learn everything about Suspicious Transaction Reports in 2025—how they differ from other FIU reports, what businesses must do to stay compliant, and the penalties for getting it wrong**

Suspicious Transaction Reports (STRs) are an essential tool in the fight against money laundering, terrorist financing, and other criminal financial activity. They are also a regulatory requirement in most countries, with significant penalties for non-compliance.

In one recent case, a C\$1 million penalty (~US\$780,000) was [handed out to British Columbia Lottery Corporation by Canadian regulator FINTRAC](#) for compliance violations, including not reporting suspicious transactions. However, the penalties involved can be much higher. In 2024, TD Bank was fined a total of approximately \$3 billion by US regulators, including [FinCEN](#) and the [Department of Justice](#), for failing to prevent millions of dollars in transactions by criminals. This shows the scale of the potential risk to regulated firms that do not meet their obligations.

This is part of a wider trend of growing penalties for AML failings, with [over \\$55 billion in fines](#) being handed out since the 2008 global financial crisis.

Let's take a closer look at what STRs are and why they are essential for businesses (especially those with AML obligations).

## **What is a Suspicious Transaction Report (STR), and how is it different from other FIU reports?**

Suspicious Transaction Reports (STRs) are made by businesses and organizations when they spot potentially suspicious transactions involving their clients. These reports will be made to the appropriate government agencies in the relevant country, who will then decide what further action may be needed.

STRs are related to other types of [Financial Intelligence Units](#) (FIU) reports—for example, [Suspicious Activity Reports \(SARs\)](#) and these terms are sometimes used interchangeably. However, they are different things in most parts of the world.

Other FIU reports include:

- Threshold Transaction Report (TTR): A transaction exceeding \$10,000 or an equivalent amount in another currency.
- Suspicious Transaction Report (STR): Focuses on transactions that appear unusual in value or nature.
- Unusual Transaction Report (UTR): Used when a transaction does not fit the expected pattern. It may later be upgraded to an STR.
- International Funds Transfer (IFT): Filed when money is moved between countries, helping track cross-border flows.
- Cross-Border Report: Used for any transaction that moves funds in or out of a country.
- Additional Information File (AIF): Provides further information in response to analyst or authority requests.
- Terrorism Financing Report (TFR): Used when a transaction is believed to be connected to terrorist activity.

The type of report and the circumstances for filing it depend on the jurisdiction.

## When should STRs be filed?

Common reasons to file suspicious transaction reports include where transactions appear to be:

- Unusual for a particular client
- Lacking in an apparent lawful purpose
- Structured to hide another transaction

The goal of suspicious transaction reporting is to help identify and prevent various types of illegal activity, including money laundering, terrorist financing (ML/TF), fraud, and efforts to evade regulatory requirements.

## Who is required to submit STRs?

Most countries require financial institutions and other [AML-obliged](#) organizations and professionals to report suspicious transactions and activity.

Additionally, in many jurisdictions, unregulated businesses and individuals can report suspicious financial behavior through fraud reporting portals. For example, the FBI's Internet Crime Complaint Center (IC3) ([IC3.gov](#)) is used to report cybercrimes in the US, and other

scams can be reported through the Federal Trade Commission's (FTC) [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud). In Cyprus, it is the Cyprus Police's Cybercrime Reporting Platform ([police.gov.cy](https://police.gov.cy)). For reporting scams in the UK, Action Fraud ([actionfraud.police.uk](https://actionfraud.police.uk)) is used.

Exactly which organizations and professionals are covered by STR requirements will depend on the jurisdiction. Your national FIU, professional body, trade association, or legal advisors will be able to provide specific guidance.

In general, the following types of organizations will usually be required to submit STRs:

- Banks
- Lawyers
- Accountants
- Tax advisors
- Trust providers
- Real estate agents
- Casinos
- Dealers in high-value goods
- Individuals and businesses involved in the art market
- Cryptocurrency exchanges

## When should a business file an STR?

When to file a suspicious transaction report depends on the jurisdiction, but generally it is required when transactions suggest possible money laundering, terrorist financing, or other criminal activity by an employee or customer.

The Financial Action Task Force (FATF) recommends [a risk-based approach](#) to AML/CTF. Financial institutions and other regulated organizations should assess the specific risks they may be exposed to, then put in place risk management and mitigation measures appropriate for their level of risk.

[The FATF Recommendations](#) provide an international standard for anti-money laundering and countering terrorist financing that is endorsed by [more than 200 countries and jurisdictions](#).

[FATF Recommendation 20](#) provides specific guidance on the reporting of suspicious transactions, which are a key reporting obligation in any financial risk management framework. It states:

“If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).”

## Examples of suspicious transactions

The 2024 [case against Canada's TD Bank](#) by the US Financial Crimes Enforcement Network (FinCEN) involved a number of examples of suspicious transactions that the bank failed to identify and act upon. This resulted in [a penalty of over \\$3 billion](#) with \$1.3 billion going to FinCEN and a further \$1.8 billion to the US Justice Department.

Transactions featuring a number of suspicious characteristics were at the heart of [a recent prosecution](#) by Canada's Financial Investigation Unit, [FINTRAC](#). British Columbia-based Crystal Currency Exchange Inc. was fined C\$340,000 (~US\$252,000) for compliance issues, including failure to submit Suspicious Transaction Reports where legally required to do so.

The most serious regulatory breaches FINTRAC uncovered involved [three cases where Suspicious Transaction Reports were not made](#) when there were "reasonable grounds" to suspect transactions were related to money laundering activities. Those reasonable grounds included that the transactions involved large quantities of foreign cash, they were not consistent with the account holders' finances, and they were connected to high-risk jurisdictions.

These examples of suspicious transactions not being identified and reported correctly could likely have been avoided with measures, including [effective transaction monitoring](#).

## Situations where an STR may be required

Examples of when an STR may be required include:

- When an unusually large transfer is made into or out of a customer account → **Then file an STR**
- When a large deposit or withdrawal is made in cash that does not fit a customer's usual pattern of behavior → **Then file an STR**
- When a number of small transactions are carried out that may be an attempt to disguise a larger transaction → **Then file an STR**
- When a transaction does not appear to have a clear business or lawful purpose, and the customer will not provide information on the purpose → **Then file an STR**
- When a transaction involves a high-risk jurisdiction → **Then file an STR**
- When account activity is inconsistent with the account holder's normal behavior → **Then file an STR**
- When a transaction seems unnecessarily complex (e.g., involving numerous accounts and/or financial institutions) → **Then file an STR**

This is not intended to be an exhaustive list and identifying which activity should trigger an STR should be part of an organization's risk and compliance framework.

## Regulatory triggers for STRs in different regions

| Region | Reporting trigger | Key relevant legislation | Regulatory body | Source |
|--------|-------------------|--------------------------|-----------------|--------|
|--------|-------------------|--------------------------|-----------------|--------|

|           |                                                                                                                          |                                                                                                            |                                                                                                     |                                                                                                     |
|-----------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Canada    | Reasonable grounds to suspect money laundering or terrorist financing                                                    | <a href="#">Proceeds of Crime (Money Laundering) and Terrorist Financing Act</a>                           | <a href="#">Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)</a>              | <a href="#">FINTRAC STR Compliance Guidance</a>                                                     |
| Germany   | Suspicion that an asset or transaction is connected to a criminal act related to money laundering or terrorist financing | <a href="#">Act on the Detection of Proceeds from Serious Crimes (GwG)</a>                                 | <a href="#">Federal Financial Supervisory Authority (BaFin)</a>                                     | <a href="#">BaFin guide to their Suspicious Transaction Reporting System</a>                        |
| Australia | Any transaction or interaction that raises suspicion of illegal activity                                                 | <a href="#">Anti-Money Laundering and Counter-Terrorism Financing Act 2006</a>                             | <a href="#">Australian Transaction Reports and Analysis Centre (AUSTRAC)</a>                        | <a href="#">AUSTRAC guide to the obligations of designated service providers</a>                    |
| Japan     | Suspicion that a transaction may be related to criminal activity or that a customer could commit a crime                 | The Act on Prevention of Transfer of Criminal Proceeds (APTCP); the Foreign Exchange and Foreign Trade Act | <a href="#">Japanese Financial Intelligence Centre (JAFIC)</a>                                      | <a href="#">JAFIC Annual Report 2023</a>                                                            |
| France    | Suspicious transactions relating to offences punishable by one year's imprisonment and/or terrorist financing            | The Monetary and Financial Code                                                                            | <a href="#">Intelligence Processing and Action Against Clandestine Financial Circuits (Tracfin)</a> | <a href="#">Financial Markets Authority (AMF) Guidelines on the Obligation to Report to Tracfin</a> |

## Penalties for failing to report suspicious transactions

The following is a breakdown of the penalties for failing to report suspicious financial activity in some of the world's top economies:

| Country   | Penalty                                                                                                                                                                                                               | Relevant legislation                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Canada    | Fine of up to C\$2 million (~US\$1.45 million) and/or up to 5 years' imprisonment                                                                                                                                     | Proceeds of Crime (Money Laundering) and Terrorist Financing Act |
| Germany   | A fine of up to €150,000 (~\$176,000) for most offences. For particularly serious and systematic offences, a fine of up to €1-5 million (~\$1.2-5.7 million) or 10% of an organization's gross income can be imposed. | Act on the Detection of Proceeds from Serious Crimes (GwG)       |
| Australia | For individuals: Up to 20,000 penalty units (currently equal to AU\$6.26 million or ~\$4.1 million)<br><br>For corporate bodies: Up to 100,000 penalty units (currently AU\$31.3 million or ~\$20.5 million)          | Anti-Money Laundering and Counter-Terrorism Financing Act 2006   |

## How to file a Suspicious Transaction Report (Step-by-Step)

When an organization has identified a suspicious transaction or pattern of activity, it will need to follow the reporting process for the Financial Investigation Unit in the relevant jurisdiction. For example, in Canada, this is covered in [FINTRAC's compliance guidance for reporting suspicious transactions](#).

The exact process involved will vary from country to country, but the general steps should include:

## **Step 1. Establish the basis for making the report**

The organization must identify which transaction or transactions are suspicious and why they are suspicious.

## **Step 2. Carry out Enhanced Due Diligence**

Enhanced Due Diligence will allow the organization to identify potentially relevant information, including whether the customer account may have been opened fraudulently or taken over by criminals. EDD can also demonstrate that the organization has taken all appropriate steps to determine if there is a legitimate reason for a suspicious transaction.

## **Step 3. Collect all relevant information, including details of any previous related STRs**

The STR should include all relevant information that the organization holds, including around the customer's identity and previous patterns of behavior. If a previous STR has been made about the same customer, details of this should be included.

## **Step 4. Prepare the report**

The report should be prepared by the appropriate person, such as the organization's Nominated Officer or Money Laundering Reporting Officer (MLRO). Input should be sought from all relevant people within the organization, such as financial and legal risk experts.

## **Step 5. Have the report checked by all relevant people within your organization**

Before submitting the report, it should be checked and signed off by all appropriate people within an organization. Who this is and what level of sign-off is required will depend on the organization and level of risk involved.

## **Step 6. Submit the report**

The report should be submitted through the proper channels. In most cases, STRs can now be submitted online but some jurisdictions will still allow paper reports where required.

## **Step 7. Notify any other relevant authorities**

If an organization has reason to believe that a crime has occurred, then it will likely need to report the matter separately to the relevant authorities.

## **How STRs fit into an AML compliance program**

Suspicious Transaction Reports (STRs) can help with key requirements of an [Anti-Money Laundering \(AML\) compliance program](#), including:

- Facilitating early detection and prevention of criminal activity
- Supporting intelligence gathering for financial intelligence units and law enforcement agencies
- Demonstrating compliance with regulatory requirements
- Assessing and managing risks effectively

AML tools should incorporate systems for identifying any suspicious transactions in a potential money laundering scenario.

### How STRs align with key elements of an AML compliance program

| AML compliance process                                    | Purpose                                                                                                                                                             | Role of STRs                                                                                                                                                                                                   |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Taking a risk-based approach                              | Identify specific risks related to money laundering and terrorist financing, then create a risk management framework with measures appropriate to the level of risk | STRs are a key obligation of a risk-based approach to AML and the prevention of terrorist financing as good transaction monitoring and flagging suspicious transactions will be required for any level of risk |
| Know Your Customer (KYC) and Customer Due Diligence (CDD) | Verifying the identity of customers                                                                                                                                 | STR may be required if the verification process raises concerns about suspicious transactions                                                                                                                  |
| Customer Due Diligence (CDD)                              | Investigating, assessing and monitoring customers' behavior to assess their risk profile                                                                            | STR may be required where the CDD process uncovers suspicious activity                                                                                                                                         |
| Transaction Monitoring (TM)                               | Tracking and monitoring transactions for signs of money laundering or terrorist financing                                                                           | STR is required where a suspicious transaction or pattern of transactions is identified                                                                                                                        |
| Enhanced Due Diligence (EDD)                              | Investigating customers' backgrounds, activity and risk profile in higher risk situations                                                                           | Where a suspicious transaction or pattern of behavior is identified, EDD will normally be carried out before an STR is made                                                                                    |

|                      |                                                             |                                                                                                                 |
|----------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Regulatory reporting | Reporting suspicious transactions to the relevant authority | STRs are used to report suspicious transactions to the relevant authorities in line with regulatory obligations |
|----------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|

## Best practices for STR compliance in 2025

The following is a checklist of best practices for STR compliance in 2025 drawing from sources like the UK's National Crime Agency [Guidance on submitting better quality Suspicious Activity Reports \(SARs\)](#).

### STR best practice checklist:

- ☐ Does your organization have a Nominated Officer or Money Laundering Reporting Officer (MLRO) responsible for Suspicious Transaction Reports?
- ☐ Do you have an AML compliance program that includes STRs?
- ☐ Does your AML compliance framework show how STRs should be integrated into different aspects of your compliance program?
- ☐ Do you have reliable, AI-powered transaction monitoring systems?
- ☐ Are the criteria for suspicious transactions correctly defined in your monitoring systems?
- ☐ Do you have automatic alerts for suspicious transactions set up in your monitoring systems?
- ☐ Are Politically Exposed Persons (PEPs) and sanctions screening systems part of your AML program?
- ☐ Do relevant staff have up-to-date training on identifying suspicious transactions?
- ☐ Do you have appropriate documentation and training for how to create and submit an STR and what information to include?
- ☐ Do your processes include how to check whether a customer has previously been the subject of an STR?
- ☐ Do you have a clear review process to follow before an STR is submitted, including who must provide sign-off?
- ☐ Do you have regular audits of your AML compliance program that includes STRs?

Please note: Organizations should always refer to the reporting requirements for their own country when creating an AML compliance program.

## Staying proactive with STRs

Suspicious transaction reporting obligations are not something regulated entities can ignore or do haphazardly. As the various examples above show, **the penalties for getting it wrong can be devastating**. STRs must form a core part of an organization's risk-based approach to AML and preventing terrorist financing, and this can only happen with effective, proactive transaction monitoring.

Sumsu's AI-powered [Transaction Monitoring](#) solution flags and blocks suspicious transactions, cuts the need for manual reviews, and automates report building for faster, simpler compliance with STR obligations.

As regulatory requirements and the tactics criminals use change all the time, we can help organizations to make sure they always stay on top of the latest developments and their regulatory obligations.

## FAQ

### What triggers a Suspicious Transaction Report?

An STR should generally be triggered where a transaction or pattern of transactions suggests the possibility of money laundering, terrorist financing, or other criminal activity.

There are different [reporting triggers for different jurisdictions](#), so it is important that your AML compliance program and transaction monitoring are tailored to your regulatory regime.

### What are examples of suspicious activity in banking?

The following are common examples of suspicious activity in banking:

- **Transactions that do not match the customer profile** (e.g., higher than normal deposits and withdrawals)
- **Unusual transaction patterns** (e.g., a sudden increase in the number of transactions)
- **Transactions that lack a clear, legitimate purpose** (e.g., multiple transactions on the same day in different locations)
- **Smurfing or structuring** (where a transaction is broken down into smaller ones to avoid reporting thresholds)
- **Unexplained international transfers** (e.g., transfers to or from high-risk countries)

### Who is responsible for filing an STR?

An organization covered by suspicious transaction reporting requirements should have a designated person responsible for making these reports. They will typically be an employee

of the organization with a designation such as 'Nominated Officer' or Money Laundering Reporting Officer (MLRO).

Any individual can also submit a Suspicious Transaction Report if they believe they have good reason for doing so.

## **How do you write a Suspicious Transaction Report?**

To write an STR, you should:

1. Familiarize yourself with the reporting requirements for your reporting body
2. Provide a clear basis for why the report is being made
3. Include all relevant information (including all CDD and EDD data as well as whether an STR has previously been made about the same account holder)
4. Clearly indicate if there is any required information that you are unable to provide
5. Keep the report clear and concise with short paragraphs and a logical structure
6. Avoid jargon and acronyms wherever possible (and explain them if they are required)
7. Secure sign-off from all relevant parties before submitting the report

When providing the basis for the report, make sure to include who is involved, how they are involved, what assets are involved, where the assets are located, when the suspicious transaction/s took place, and why you consider the transaction/s suspicious.

## **What happens if a suspicious transaction isn't reported?**

If a suspicious transaction is not reported, then there is the obvious risk of investigation and prosecution by the relevant FIU or other government agency for failing to meet regulatory obligations. This can lead to both criminal and civil penalties, as covered in the above section [Penalties for Failing to Report Suspicious Activity](#).

Failing to raise an STR also means that criminal activity may be allowed to carry on unchecked. Criminals could then decide that an organization is a "soft touch" and begin to use it more frequently for illicit transactions.

There is also the reputational risk to consider, especially if significant wrongdoing is uncovered.