sumsub pismo

Complete Guide to Transaction Monitoring

Contents

Introduction

If companies don’t monitor transactions, they run the risk of money laundering, fraud, and other crime occurring on their platforms. That’s why governments have been toughening their AML regulations; and if companies fail to comply, they face heavy fines, reputational damage, and even license revocation.

$1.6 trillion

lost per year to money laundering according to the United Nations

$8.8 billion

lost on fraud in 2022 according to the Federal Trade Commission

Transaction monitoring is crucial for companies providing financial services, as it helps them perform risk assessments and detect suspicious activity.

This expert guide will help you spot transaction fraud, bolster your defenses, and optimize conversion rates at the same time.

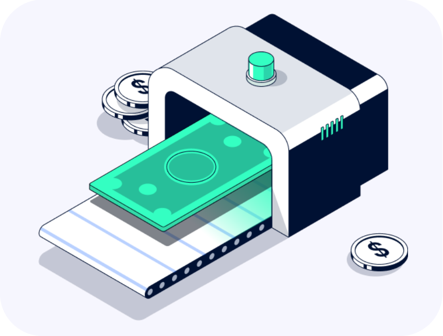
Summary

Transaction monitoring is helpful in preventing:

Fraud

Money laundering

Terrorist financing



Top 3 transaction monitoring challenges:

- False-positive cases
- Innovative fraud patterns
- Balancing protection & conversion rates

Industries that benefit from transaction monitoring the most:

- Fintech, banking
- Insurance
- Gambling and iGaming
- Crypto
- Ecommerce

> “Behavior is the first thing to monitor to see what’s really happening.”

Guilherme Chaddad, Software Engineer Specialist pismo

What is transaction monitoring?

Transaction monitoring is an ongoing process used to spot dubious transfers and transactions made in digital or fiat currencies. In terms of monitoring, a transaction could also be defined by other customer activity events, e.g boarding a rented vehicle or making a claim for an insurance payout.

Transaction monitoring is mandatory for regulated businesses, as both local and international ML/TF laws require businesses to perform customer due diligence (CDD).
CDD is a part of the FATF's (Financial Action Task Force) 40 recommendations successfully implemented in legislation of most countries. If businesses do not adhere to them, they risk regulatory penalties and fines.

FATF Recommendations include:

- Ongoing monitoring of transactions throughout the business relationship
- Source of funds checks for transactions above certain thresholds, e.g over $10,000
- Customer identity verification
- Understanding of the purpose of business relationships
- Verification of ultimate beneficial owners (UBOs) during business verification
- Reporting suspicious transactions to financial intelligence units (FIUs)

What is transaction monitoring?

Transaction monitoring can be split into two main categories:

AML transaction monitoring

Usually overseen by compliance departments, transaction monitoring helps prevent financial crime. According to the Guidance for the UK Financial Sector, there are two approaches to transaction monitoring: real-time and post-transaction.

Real-time

Monitoring occurs as the transaction takes place, which reduces the risk of breaching sanctions.

Post-transaction

Used to detect patterns and trends in criminal activity occurring after the initial transaction took place.

Anti-fraud transaction monitoring

Anti-fraud prevention is done by analyzing user behavior patterns, transaction details, and many other signals that help specialists make informed decisions.

As a part of transaction monitoring, other events related to the safety of the account are also considered transactions, such as login, password recovery, or money transfer operations. That way, the monitoring solution has more activity data points to determine fraud patterns or suspicious actions.

In the case of Sumsub, transaction monitoring algorithms use AI models to differentiate between legitimate and fraudulent activities by analyzing various signals.

What is transaction monitoring?

Generally, national AML legislation requires transaction monitoring to include:

- A risk-based approach driven by the nature, size, and complexity of a given business
- Reporting of suspicious transactions
- Holistic monitoring to detect politically-exposed persons (PEPs) or people belonging to other high-risk categories

Real-time transaction monitoring

By using algorithms, it’s possible to detect and block abnormal transactions when they happen.

For example:

An attempt is made to send a large sum of money to a foreign account that has not been used before. A real-time transaction monitoring system immediately flags this transaction as suspicious and sends an alert to the bank's compliance team for review. If there are signs of fraud or money laundering, the account will be frozen until the investigation is complete.

Post-event transaction monitoring

This type of monitoring is used when completed transactions don’t raise an immediate concern to then compare them against money laundering typologies.

For example:

A customer has a history of transactions just under local AML thresholds. Post-event monitoring uncovers this pattern and takes action: reassesses risk score, requests a source of funds document, and/or lowers the transfer limit until the nature of transactions is clarified.

Sumsub recommends using both real-time and post-event transaction monitoring for maximum protection.

Regulations for AML transaction monitoring

Businesses should follow these key AML regimes:

UK

Applicable AML legal framework

In the UK, firms must have effective policies and procedures in place to identify unusual transaction patterns as a part of their anti-money laundering and counter-terrorist financing obligations. AML obligations include submitting Suspicious Activity Reports (SARs).

The National Crime Agency (NCA) oversees the submission of SARs when unusual or exceptionally large transactions are identified.

Firms should include as much relevant information about the customer as possible in SARs, including transaction history, activity, occupation, company's business, and National Insurance number. While businesses are not required to collect this information for all customers, they should include it in SARs if they have obtained it in the course of normal business.

Recordkeeping requirements

The company is required to maintain records for at least five years. These records must include copies of all documents and information obtained to satisfy customer due diligence requirements, as well as supporting records related to any transactions subject to customer due diligence measures or ongoing monitoring.

By keeping these records, compliance officers can reconstruct transactions and provide evidence of their compliance with anti-money laundering and counter-terrorist financing regulations.

Maintaining records in a clear and organized manner for the required period ensures transparency and helps prevent illicit activities.

Regulations for AML transaction monitoring

Businesses should follow these key AML regimes:

USA

Applicable AML legal framework

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, is responsible for administering and issuing regulations under the **Bank Secrecy Act** (BSA). The BSA and its regulations require firms to implement and maintain an effective AML program.

AML programs must include policies, procedures, and internal controls that ensure ongoing compliance with customer identification, reporting, recordkeeping, and responding to law enforcement requests. BSA provisions apply to financial institutions such as banks, credit unions, casinos, brokers, and dealers in securities, and money services businesses.

Suspicious activity reports must be filed for unusual transactions over $5,000, and the filing must occur within 30 days after suspicion arises.

Recordkeeping requirements

BSA records must be retained for a period of five years.

Upon request, obliged entities must make all supporting documentation (such as CDD information, SARs, transaction reports, and other financial or business correspondence) available to FinCEN or any other law enforcement or supervisory agencies (including the IRS).

BSA reporting and recordkeeping requirements result in paper trails of transactions that law enforcement and others can use in criminal, tax, and regulatory investigations.

Regulations for AML transaction monitoring

Businesses should follow these key AML regimes:

EU

Applicable AML legal framework

The European Directive on Anti-Money Laundering provides that obliged entities shall apply customer due diligence requirements when entering into a business relationship (i.e. identifying and verifying the identity of clients, monitoring transactions, and reporting suspicious transactions).

One of the pillars of the European Union's legislation to combat money laundering and terrorist financing is Directive (EU) 2015/849.

According to this Directive, banks and other regulated institutions are required to apply enhanced due diligence in business relationships and transactions involving high-risk third countries.

Reporting requirements vary from country to country.

Recordkeeping requirements

Recordkeeping requirements vary. The average retention period is 5 years.

Transaction monitoring challenges

There are countless transaction fraud schemes, with new vectors of attack emerging often. Here are the risks of running an insufficient transaction monitoring solution:

False positives

Occurs when the monitoring system is imprecise and places false flags on otherwise legitimate cases. Manual review is required as a result, which is time-consuming and annoying for customers.

Complex rules

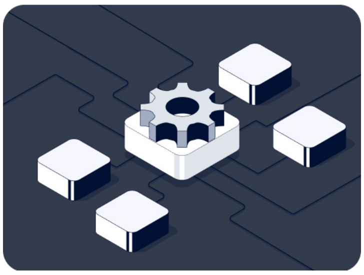
With a lot of complex rules in place, monitoring cases gets difficult and scaling becomes a challenge as the system will not be able to keep up with demand.

Unusual transactions

Fraudsters will go to lengths to conceal their activity. Detecting sophisticated fraud or ML/TF patterns requires a well-designed detection system.

Risk-based optimization

Finding the sweet spot between strong protection and optimal conversion rates is difficult, as the process has to be customized for various risk levels, user groups, and regions.



Integrating different vendors

Integrating and managing multiple vendors is a time-consuming process that requires constant upkeep and is prone to errors and unexpected downtime.

Insufficient case management

Poor delegation of casework, low-quality inspection tools, and inconclusive data analysis leads to missed cases, incorrect decisions, and wasted time.

Transaction monitoring challenges

Guilherme Chaddad

Software Engineer Specialist at Pismo

When monitored behavior changes, it may not be a fraud-related problem, but rather an issue with the network or the acquiring service. It can also indicate some fraudulent activities, which is why having all available data for case reviews is important.

One situation we heard of was a person who found a way to surpass set bank limits and spend more than R$100,000 ($20,000). As a result, the item was purchased on the acquiring side and canceled on the issuer side. That could be prevented if both the business and the acquiring side had a transaction monitoring rule for this situation. An example would be: if the same person makes many transactions and cancels them during the same day, they are flagged as suspicious.

Who benefits from transaction monitoring?

Every industry benefits from transaction monitoring in different ways:

Fintech, Banking, or Payments

- Reduced false positive cases
- Improved team efficiency
- Risky users and transactions flagged
- Controlled transaction limits
- AML compliance
- Payment/chargeback fraud prevention
- Balanced onboarding speed and fraud protection

By utilizing customer onboarding data and taking a risk-based approach, banks can automatically detect signs of suspicious activity, such as income drastically higher than in the source of funds statement.

Gambling, iGaming

- Reduced false positive cases
- Elimination of promo or bonus abuse
- Adherence to responsible gaming laws
- Prevention of multi-accounting
- Prevention of account takeovers
- AML compliance
- Prevention of bot attacks
- Protection of customers throughout the entire lifecycle

A gambling or iGaming service can easily detect if a customer is spending more money than declared in their income statement, or curb arbing by detecting multi-accounters.

Who benefits from transaction monitoring?

Every industry benefits from transaction monitoring in different ways:

Crypto services

- Detection of suspicious profiles and synthetic IDs
- Decreased chargeback rates
- Reduced in false positives
- Maximized revenue
- AML compliance
- Travel Rule compliance

With transaction monitoring in place, outbound transactions to dark web wallets or multiple exchanges can easily be detected.

Insurance

- Reduced false positive cases
- AML compliance
- Prevention of fraudulent insurance claims
- Maximized revenue
- User, business, and transaction verification in a single platform

By looking at suspicious financial history, such as multiple insurance payments requested in one month, illegitimate claims and fraud patterns can be detected.

Ecommerce

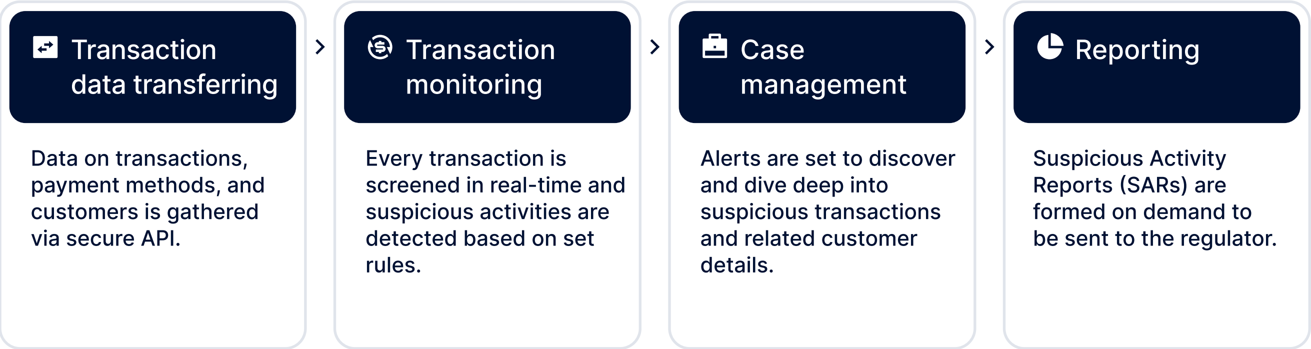
- Frictionless shopping experience
- Reduced chargebacks and false refunds
- Elimination of gift card and coupon abuse
- Automatic flagging of suspicious transactions

Transactions made at night from multiple countries, purchases over AML thresholds, and unusual spending patterns should automatically raise alarm bells and be prevented based on set rules in place.

How transaction monitoring works

Any regulated business is obligated to have transaction monitoring in place. The best solutions ensure that transaction monitoring is integral to the entire verification flow, meaning that user, business, and transaction verification are connected. This way you can use every single available data point to assess users, risks, and suspicious patterns.

The structure of a transaction monitoring solution



Transaction data transferring

Data on transactions, payment methods, and customers is gathered via secure API.

Transaction monitoring

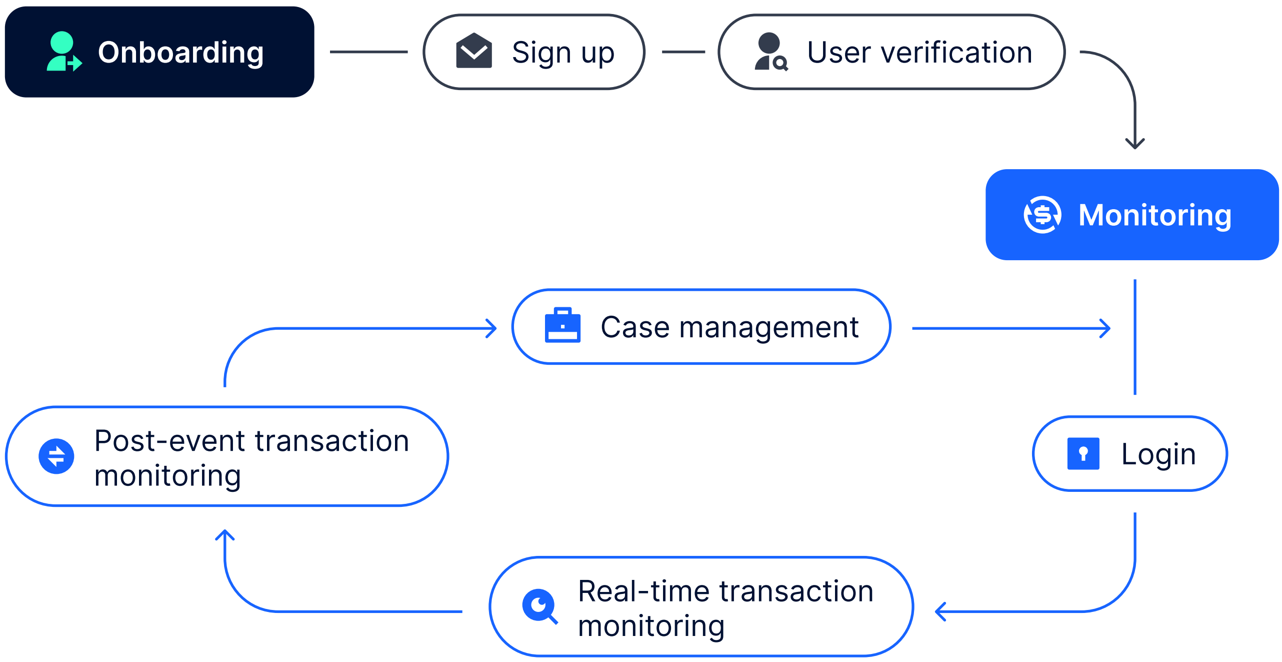
Every transaction is screened in real-time and suspicious activities are detected based on set rules.

Case management

Alerts are set to discover and dive deep into suspicious transactions and related customer details.

Reporting

Suspicious Activity Reports (SARs) are formed on demand to be sent to the regulator.

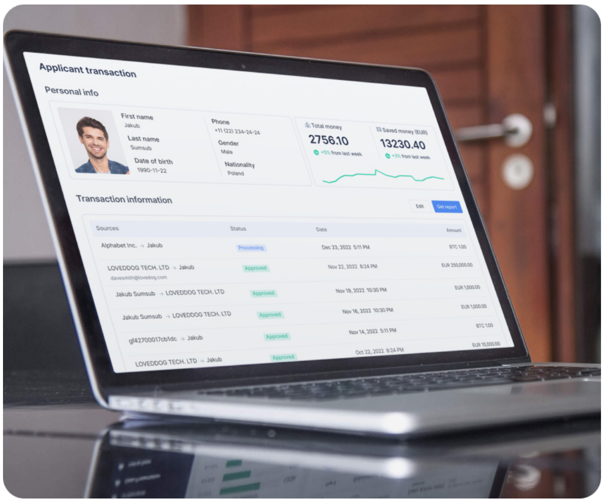

Onboarding
Sign up
User verification
Monitoring
Case management
Login
Post-event transaction monitoring
Real-time transaction monitoring

How transaction monitoring works

Transaction monitoring systems come in different forms.

Manual

Monitoring is performed by compliance officers using case management tools for detecting suspicious activity. Decision-making is always done by a person. This approach is highly time-consuming, and scaling up verification efforts can be challenging.



Applicant transaction

Personal info

First name: Jakub
Last name: Sumsub
Date of birth: 1990-11-22
Phone: +11 (22) 234-24-24
Gender: Male
Nationality: Poland

Total money: 2756.10 (+5% from last week)
Saved money (EUR): 13230.40 (+3% from last week)

Transaction information

Sources	Status	Date	Amount
Alphabet Inc. → Jakub	Processing	Dec 23, 2022 5:11 PM	BTC 1.00
LOVEDDOG TECH. LTD → Jakub davesmith@lovedog.com	Approved	Nov 22, 2022 8:24 PM	EUR 250,000.00
Jakub Sumsub → LOVEDDOG TECH. LTD	Approved	Nov 19, 2022 10:30 PM	EUR 1,000.00
Jakub Sumsub → LOVEDDOG TECH. LTD	Approved	Nov 16, 2022 10:30 PM	EUR 1,000.00
gf42700017cb1dc → Jakub	Approved	Nov 14, 2022 5:11 PM	BTC 1.00
LOVEDDOG TECH. LTD → Jakub	Approved	Oct 22, 2022 8:24 PM	EUR 10,000.00

Automated

Transactions are automatically monitored in real-time, and only some suspicious cases are assigned to the compliance team. Sometimes, a combination of both is necessary, especially in firms with a high volume of transactions.

With new technologies, it’s possible to improve the speed, quality, and efficiency of money laundering and terrorist financing prevention. This helps financial institutions assess risks more accurately, quickly, and comprehensively.

How transaction monitoring works

Guilherme Chaddad

Software Engineer Specialist at Pismo

Avoid giving guidelines to the fraudsters. If we show them that the card is not valid, then they know that the account number they are trying to use isn't valid. When they find a real card, they will know they can try again. We change the available data often. In Brazil, we have an entity that controls response codes. Instead of responding that the card is not valid, we respond that the transaction was declined.

Building a transaction monitoring workflow

How you build your transaction monitoring workflow depends on your industry, customer type, and many other factors. Below you'll find recommendations on how to do it right.

The essentials of any transaction monitoring system include:

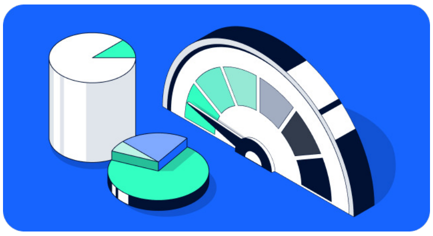
- Flagging transactions and/or activities for review
- Prompt reviews of suspicious activity by compliance officers
- Appropriate action taken when suspicious activity is uncovered

Preparing transaction monitoring rules

When it comes to arranging transaction monitoring, businesses should take the following points into account:

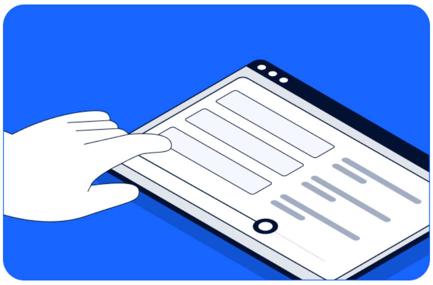
- The frequency, volume, and size of transactions with customers
- Customer and product risk scoring
- The scope of the firm's business activities and size
- Up-to-date customer information
- Awareness of evolving financial crime risks and typologies
- Investigation into the reasons for unusual transactions or activities
- Thresholds and parameters set to the firm's risks and context
- Back-testing to ensure proper operation and effectiveness of monitoring

Building a transaction monitoring workflow



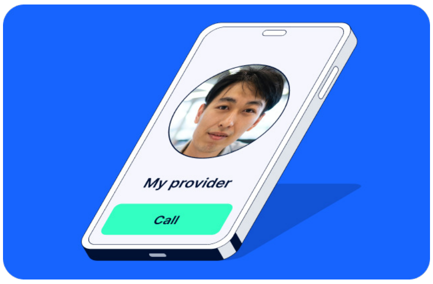
Analyze your risk policy

Get a clear idea of what data you need to screen and why. This will determine the basis for the rules to be set later.



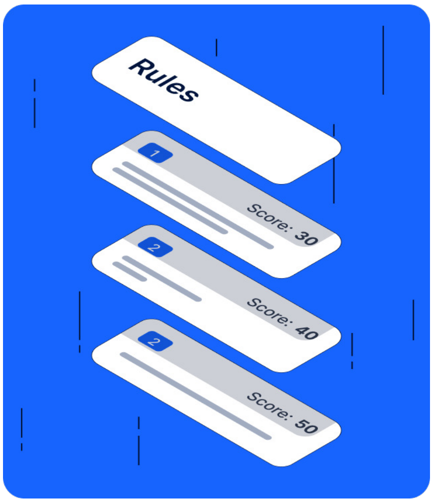
Determine data types

Take a hard look at all available data and decide what can be useful for your decision-making process during user, business, and transaction verification.



Consult your verification provider

If you're unsure where to start or get stuck, it's always a good idea to approach your vendor and ask for rule examples for your industry and best practices on how to use them.



Start creating rules

Many verification providers, including Sumsub, have pre-made rules that include conditions, risk scores, tags, and actions. Rules created for various industries can be mixed and matched together as well. Sumsub enables using an unlimited number of rules simultaneously.

For example: demanding a source of funds statement for transactions over $5,000.

Building a transaction monitoring workflow

Testing and debugging rules

Once you set up your rules, it's very likely you'll need to adapt them to new changes or markets. It's crucial to have the ability to safely test new rules on an existing database of customers in a dry-run mode before using them in a live environment.

Alert system

With an alert system in place, you can quickly react to new events. Automatic actions based on alerts, such as requesting source of funds, redoing verification, or adding risk labels, are also important.

Examples of suspicious and unusual transactions

- Transactions with no apparent purpose or of unnecessary complexity
- Use of non-resident accounts, companies, or structures without purpose
- Transfers to and from high-risk jurisdictions without reasonable explanation or business purpose
- Range of services inconsistent with the company's relation to the customer
- Dealing with customers that seem out-of-place in a given industry
- A series of transactions structured just below a regulatory threshold

Building a transaction monitoring workflow

Guilherme Chaddad

Software Engineer Specialist at Pismo

> For e-commerce transactions, a valid credit card and CVV2 code is redirected to the bank institution for processing when a purchase is made. When a card is not found in the database, it may be hedged using a valid BIN (Bank Identification Number) code. Then, if the response is "invalid password", a brute-force attack may be attempted to guess both the correct PIN and CVV2 codes of the card.

Case management

Some corner cases will require human attention, and it’s important to have a workflow that allows for systematic and careful review. We recommend opting for a solution with the following functionality:

Analytics

An analytics suite will help you find bottlenecks, assess compliance team performance, and gain insights into your customer base patterns.

Casework logging

Attaching necessary documents and notes to a particular case will help structure information. Audit logs are also mandatory.

Scalability

For businesses with hundreds of compliance officers, delegation of casework and customized alerts will help to improve productivity.

Building a transaction monitoring workflow

Guilherme Chaddad

Software Engineer Specialist at Pismo

Teams monitoring transactions need dashboards and alerts to monitor the behavior of the transactions being processed. The response time, number of requests, number of approvals, and number of denials—all matter. Those dashboards help to measure the system's health and identify anomalies in the graph that could indicate an attack attempt like a peak of declined transactions, an unexpected increase in a load of transactions being processed, or an unexpectedly high volume of requests coming from a single acquirer.

An alert system must be in place for the responsible teams to see the incoming requests and take actions like blocking transactions for a specific acquirer, merchant, account, card, or any other action that may be necessary in order to avoid a fraudulent transaction to be approved.

Building a transaction monitoring workflow

Forming reports

Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs), are basically the same. The FATF calls them STRs, while the U.S. calls them SARs. These are one of the key weapons used by governments in the battle against money laundering and other financial crimes.

Firms are obligated to file such reports when illegal activity takes place or when the suspicious activity has met the relevant reporting threshold (which varies from country to country).

A quick and easy suspicious activity reporting tool is a must-have. Not every verification platform is equipped to send reports directly to financial authorities, but a prepared file is easy to generate. That’s why Sumsub lets companies prepare transaction data in Excel format at any time.

It is illegal to inform anyone involved in a transaction that a SAR has been filed.

SARs must only be provided to law enforcement when required. If an employee suspects money laundering, AML violations, or a suspicious transaction, they should report it to their manager or AML compliance officer. If a SAR is deemed necessary, it must be kept for a specific number of years along with any supporting documentation.

Building a transaction monitoring workflow

SARs typically include detailed information about the relevant customer or company, as well as the incident itself:

- The activity of the company or customer
- The contacts of the responsible compliance officer
- The person who (allegedly) conducted the suspicious transaction
- The type of suspicious transaction (currency exchange, cash conversion, remittance, use of foreign bank accounts, purchase of goods, gaming activities, use of shell companies and so on)
- The volume and currency of the transaction
- The alleged jurisdiction where the money came from
- The suspected origin of the money (money laundering, terrorist financing, drug trafficking, fraud)
- Who and under what circumstances discovered a suspicious transaction
- The security measures taken

The AML laws on filing such reports vary across countries, depending on the nature of the suspicious activity and the details of the customer or company involved. However, the core of a SAR report mirrors the parameters above.

Building a transaction monitoring workflow

Recordkeeping

AML-obligated firms are required to keep records of CDD information for a specific number of years (which may vary from country to country). In the past, government efforts to combat money laundering primarily focused on identifying suspicious activities, but now they also stress the importance of properly documenting large or questionable transactions. Maintaining accurate records is crucial for investigating potential money laundering cases.

Additionally, recordkeeping helps identify red flags in a customer's activity that may indicate illicit behavior.

How recordkeeping can help identify ML/TF attempts:

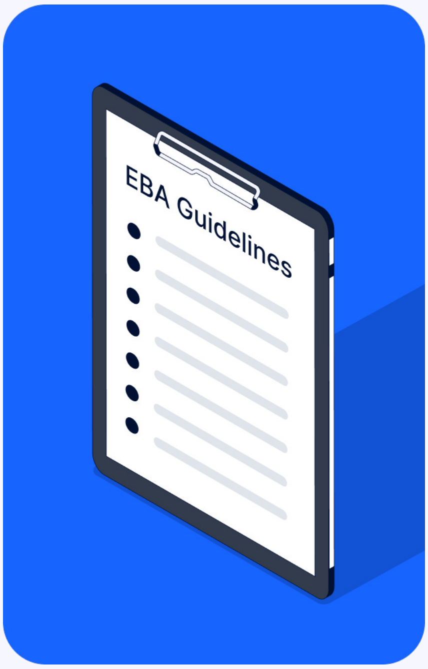
Customers may try to keep their transactions just below the reporting or recordkeeping thresholds by:

- Attempting to hide the size of a large cash transaction by breaking it into multiple, smaller transactions
- Being reluctant to provide the information needed for a reporting or recordkeeping requirements
- Being reluctant to proceed with a transaction after being informed that a report must be filed first

Building a transaction monitoring workflow

EBA Requirements

The European Banking Authority (EBA) has established specific provisions for recording transaction monitoring, including requirements for AML/CFT officers to produce an annual activity report. The report should be proportionate to the credit or financial institution's activities' scale and nature. If applicable, the activity report can be based on information already submitted to authorities in other reports.



The activity report should contain at least one of the following:

- The number of unusual transactions detected
- The number of unusual transactions analyzed
- The number of reports of suspicious transactions or activity to the FIU (distinguished by country of operations)
- The number of customer relationships ceased by the credit or financial institution due to AML/CFT concerns
- The number of requests for information received from the FIU, courts and law enforcement agencies

Checklist: how to choose a transaction monitoring solution

When it comes to picking the right transaction monitoring vendor, we recommend opting for a platform with every check you need available in one flow. Transaction monitoring works best if coupled with user and business verification.

Below are features that set apart highly effective verification platforms from the rest.

One solution for the entire customer lifecycle

Choosing a platform that combines user, business, and transaction monitoring can increase team efficiency, as well as reduce costs and time spent managing multiple providers.

Case management

User-friendly case management capabilities will spur collaboration among team members, including assigning cases, leaving comments, and logging all actions.

Compliance and risk management tools

Onboarding, monitoring, case management, investigation, and reporting capabilities should be available. There will be a moment when reporting is necessary and it's best to have everything ready by then.

Checklist: how to choose a transaction monitoring solution

Rules based on historical data

Advanced rule creation based on historical data will help you create complex rules and mix multiple rules together. That way, you can improve fraud protection significantly.

Real-time and post-transaction monitoring

Both monitoring modes help to detect every potential fraudster attack vector and uncover suspicious patterns easily.

Quick start during integration

Fast integration, no-code rule customization, and rule templates save time and help you screen users faster. A dry-run mode for rule testing on historical data will help to see how screening works before starting live monitoring.

Industry expertise

An important factor when selecting a provider, especially in regulated industries. A provider's expertise will help approach tough situations and jurisdictions effectively.

Transaction monitoring with Sumsub

Sumsub is one platform that incorporates transaction monitoring in a single, customizable flow.

Main benefits:

One verification platform

Screen users, businesses, and transactions while complying with regulations like the Travel Rule. Any kind of onboarding data can be used as a trigger for additional checks or actions.

Advanced rules

Unique rules based on custom data sources can be set up, including historical data. Dry-run mode will let you test your rules before going live.

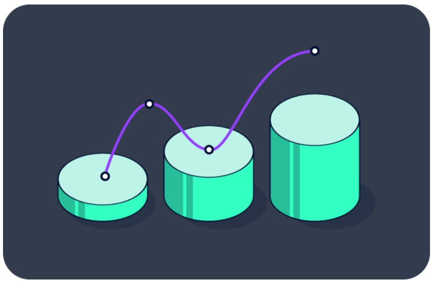
Customization & fast integration

Your own solution architect will build and customize the rules for you. You can make adjustments on your own as well, thanks to the no-code visual interface.

Increased team productivity

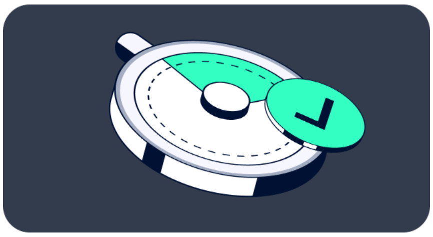
Easier casework, collaboration between departments, KPIs and analysis, and one flow for all types of checks to help you maximize efficiency and case processing speed.

Transaction monitoring with Sumsub



Analytics & reporting

Dive deep into all available data on suspicious cases to identify fraud patterns and easily generate reports for regulators as soon as you need them.



Real-time screening

Monitor faster than you can read this. It takes seconds to screen a transaction and perform an AML check.

Travel rule for crypto

It’s mandatory to monitor crypto transactions. With Sumsub, you can easily adhere to the crypto Travel Rule and ensure full compliance. Travel rule monitoring is an integral part of Sumsub’s transaction monitoring solution.

Transaction monitoring with Sumsub

Vyacheslav Zholudev

Co-founder and CTO at Sumsub

At Sumsub, we don't settle for being good at just one thing. Sumsub is one verification platform providing every type of check, case management, and continuous screening. What sets Sumsub apart is the seamless integration of our transaction monitoring, user verification, and business verification in a single flow. This way, you get a complete picture of user profiles and can intercept even the most sophisticated fraud attack vectors and patterns. Our clients rest easy knowing that Sumsub prevents fraud on all fronts—effortlessly—and helps them stay compliant worldwide.

About Sumsub

Sumsub is one verification platform that combines all types of checks, case management, and continuous screening. With AI-powered fraud detection and pattern recognition, you can be sure that nothing slips past. Every single user, business, transaction, and less tangible matter like crypto is fully secured—even from the advanced threats of tomorrow.

About Pismo

Pismo is a banking and payments technology specialist offering a highly flexible and modular cloud-native platform for financial services. Banks and fintech companies use the Pismo platform to build core banking, card issuing, payment processing, digital wallets, lending, and corporate banking solutions. It enables financial institutions to innovate and launch new products and services quickly.

Ready to start monitoring transactions worldwide?

Get a free demo →

sumsub