



# Transaction Monitoring Tactics:

Preventing Fraud and Meeting Higher AML Standards





## Johan Torgeby

CEO of SEB Group,  
[The Financial Times](#)



**The banks are spending \$20 billion a year to run the compliance regime, and we are seizing 1% of criminal assets every year in Europe.**

Does the above statement sound like good business to you? Because it does to criminals.

It's a well-known fact that money laundering and fraud rise annually, so improved countermeasures are essential.

This eBook will explain how to combat money laundering and fraud with the most up-to-date solutions, helping you fill your organization's transaction monitoring knowledge gaps.

If businesses don't monitor transactions, they risk money laundering, fraud, and other crimes occurring on their platforms. That's why governments have been tightening their anti-money laundering (AML) regulations, and businesses that fail to comply can face hefty penalties, reputational harm, and even license revocation.

**\$1.6 trillion**

lost per year to money laundering, according to the United Nations

**\$8.8 billion**

lost per year to fraud, according to the Federal Trade Commission

Transaction monitoring is the surveillance of transactions to provide a comprehensive picture of client activity, including transfers, deposits, and withdrawals.

The main challenge for transaction monitoring is the continual increase and complexity of financial transactions, which requires equally developed systems to monitor them.

**Case study #1:****The cost of Criminal Justice Act (CJA) breaches**

Problems arise when transaction monitoring solutions don't align with global requirements. More specifically, fines are issued when financial institutions breach specific acts that regulate the financial industry. That's what happened to Danske Bank in 2022, which was fined €1.82 million by the Central Bank of Ireland. In this case, Danske Bank was reprimanded for three breaches of the Criminal Justice Act (CJA) 2010.

Danske Bank's failures were linked to out-of-date data filters within its automated transaction monitoring systems, resulting in 348,321 transactions being processed without adequate AML and counter-terrorist financing (CTF) monitoring between 2015 and 2019.

Penalties for non-compliance get stricter year by year. However, Danske Bank could have avoided this fine with the correct countermeasures, and transaction monitoring offers a wide range of immediate and long-term benefits, such as:



### KYC/AML compliance

Know Your Customer (KYC) and due diligence measures are regulatory requirements that financial institutions must follow, and the correct implementation of transaction monitoring ensures that these regulatory requirements are met. KYC/AML compliance within transaction monitoring workflows reduce the overall risk of working with individuals or organizations involved in illegal activities.



### Customer confidence

Successful transaction monitoring helps maintain customer confidence by minimizing AML and fraud risks and safeguarding customer assets. This encourages customer loyalty, building a reputation for security and dependability.



### Time-saving

By automating the surveillance processes, transaction monitoring decreases the processing time needed to deal with suspicious clients and transactions by up to 60%.



Introduction .....	02
Key takeaways .....	06
What is transaction monitoring? .....	08
Part 1: AML transaction monitoring .....	09
Anti-money laundering (AML) rules .....	15
How to develop an AML program in six steps .....	25
Part 2: Anti-fraud transaction monitoring .....	28
Why is anti-fraud transaction monitoring important? .....	31
Summary .....	38

# Key takeaways

Stay ahead of fraud and AML risks with the following transaction monitoring best practices:

## Cover the full customer lifecycle

Use a platform that includes transaction monitoring within an end-to-end customer verification lifecycle. Platforms that combine user, business, and transaction monitoring solutions reduce the costs and time spent on managing multiple providers.

## Prioritize ease-of-use

Choose a transaction monitoring solution that can be easily customized with zero coding required, so you can start screening users faster. Having a dry-run mode is also important, so you can test your monitoring system before going live.

## Apply advanced rules

Match your transaction monitoring systems to specific client and industry requirements by creating custom rules based on historical data.

## Understand the latest methods

Make sure that your business is up to date on the evolution of transaction monitoring. This includes the transition from rule-based systems to AI and machine learning data aggregation-based approaches (see section: [The evolution of transaction monitoring](#)).

## Reduce legal and reputational risks

Consult with compliance experts in the KYC/AML space to help you avoid risks, fines, and penalties before they occur. Some, but not all, platforms offer Compliance-as-a-Service (CaaS), enabling you to consult with compliance experts as a part of your plan.



### Focus on accountability

Big fines and regulatory breaches can still occur even with the most advanced transaction monitoring systems if cross-departmental data sharing and accountability are not prioritized.



### Keep your systems up-to-date

Recognizing when your business has outgrown its current AML and anti-fraud technology is essential. Implementing new systems at the right time can also reduce corporate expenses and strengthen compliance.

# What is transaction monitoring?

Transaction monitoring can be split into two main categories:

## AML transaction monitoring

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

### Real-time

Monitoring occurs as the transaction occurs, reducing the risk of breaching sanctions.

### Post-transaction

Monitoring occurs after the initial transaction to detect patterns and trends in criminal activity.

## Anti-fraud transaction monitoring

Anti-fraud transaction monitoring is done by analyzing user behavior patterns, transaction details, and other signals that help fraud specialists make informed decisions about the legitimacy of user activities and processes. This includes logins, password recovery, or money transfer operations—data points used to determine fraud patterns or suspicious actions.

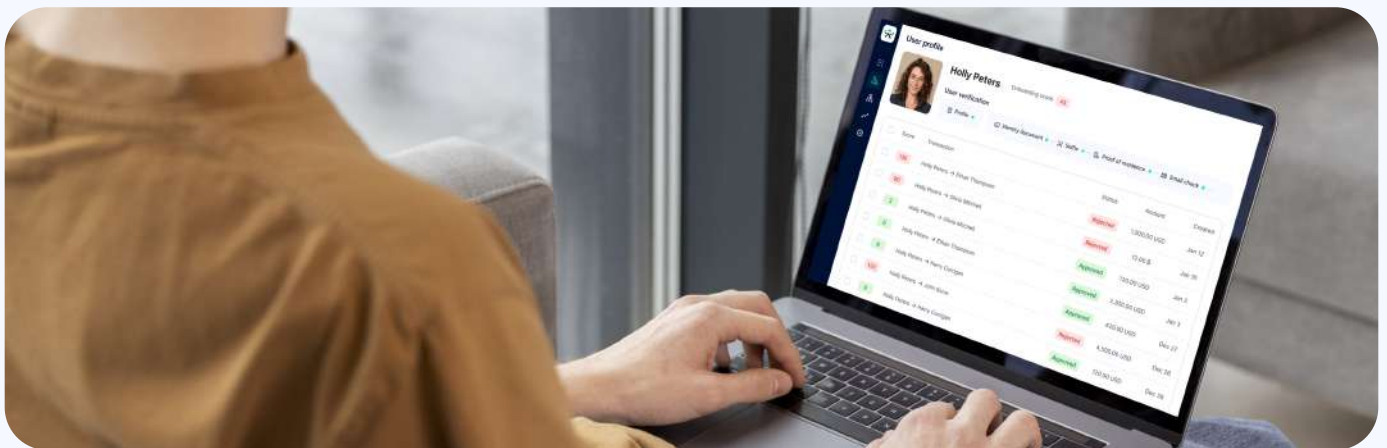
Sumsu's transaction monitoring algorithms use AI models to differentiate between legitimate and fraudulent activities by analyzing a wide array of user data.

The main difference between these two is that AML transaction monitoring aims to comply with AML requirements, while anti-fraud transaction monitoring attempts to shield companies from financial losses.



## What is AML transaction monitoring?

AML transaction monitoring is used to detect money laundering operations by studying financial transactions. AML transaction monitoring scans and analyzes financial transaction data, including bank transfers, credit card payments, and other financial activities. The process is designed to spot trends and discrepancies that might indicate money laundering or other financial crimes like terrorism financing.



## What is money laundering?

Money laundering involves disguising illegally obtained money as legitimate income. The process can be broken down into three basic stages:



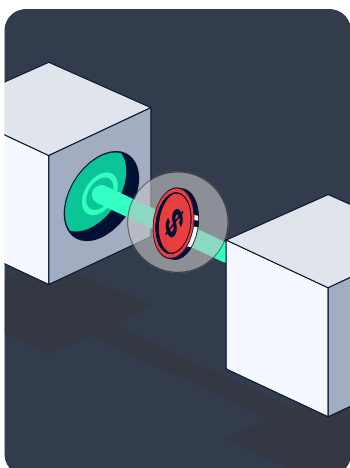
### 1. Placement

This stage involves introducing illicit funds into the financial system. Criminals may deposit cash into banks, purchase assets such as real estate or luxury goods, or convert cash into other forms such as digital currency. The aim is to make the illegal funds appear legitimate and difficult to trace.



## 2. Layering

The layering stage is about making it even more challenging to trace the origin of the illicit funds. Criminals may conduct multiple financial transactions, move funds between different accounts or jurisdictions, and create complex webs of transactions to obscure the money's source. This can involve using shell companies, offshore accounts, or conducting transactions through intermediaries.



## 3. Integration

In this final stage, the laundered funds are integrated back into the legitimate economy, where criminals may use it to invest in legitimate businesses. The aim is to make the illicit funds blend in with legal assets and income, making it difficult for authorities to distinguish between intentionally obscured money and legitimate funds.

## The current state of global money laundering

The United Nations Office on Drugs and Crime (UNODC) estimates that around 1.87 trillion Euros are laundered every year, with the number of cases increasing every year. However, this global rise can be reduced if advanced transaction monitoring processes are applied correctly.

### Increase in money laundering cases



Source: [Europa.eu](https://europa.eu)



### The shell company problem

Identifying the beneficial proprietor of criminal assets is a significant obstacle in many money laundering cases due to the use of shell companies or aliases. However, it is possible to identify unusual transaction patterns using transaction monitoring, allowing companies to identify money laundering-related actors.

## AML policies

AML policies are a company's internal measures and procedures for preventing ML/TF. Implementation is mandatory for financial institutions and is overseen by regulatory authorities. Policies should determine AML risk appetite, unacceptable customer types, forbidden actions, employee responsibilities, employee rights, and qualification levels, among other areas.



Although the terms AML policy and AML program are often interchanged, the former is technically a component of the latter.

## How AML policies prevent money laundering

AML programs prevent money laundering through customer due diligence (CDD), transaction monitoring, and suspicious activity reporting.

An AML policy should be reviewed and adjusted to new money laundering attempts since criminals constantly upgrade their approaches. If policies are not continually updated, businesses may face unnecessary financial risk and reputational damage.



**Case study #2****The cost of AML failures**

Between 2012 and 2017, Santander neglected to effectively monitor and maintain its AML processes, severely impacting account monitoring for more than 560,000 corporate clients.

After an investigation, the FCA fined Santander UK Plc £107,793,300.

It was found that Santander needed more appropriate mechanisms to sufficiently validate the data supplied by clients regarding the business they would be conducting. Additionally, the company failed to effectively monitor discrepancies in the funds that clients had claimed would be passing through their accounts compared to what was actually deposited.

In one instance, a new customer opened an account for a small translation company with expected monthly deposits of \$5,000. Within six months, the company received millions in deposits and promptly transmitted the funds to other accounts. Before the bank terminated the accounts, more than £298 million had passed through.

Santander is entitled to a 30% discount on its fine because it did not contest the FCA's conclusions and decided to settle. The cost of the fine would have been £153,990,400 without the reduction.

## How Sumsub's transaction monitoring prevents AML failures

Implementing an automated transaction monitoring system is just one part of the AML challenge. In the previous case study, the Financial Conduct Authority (FCA) found examples where red flags linked to suspicious activity were not actioned correctly. This highlights that automated transaction monitoring alerts are only helpful if an organization knows how to use them.

Here are several areas where Sumsub's end-to-end solution can help reduce gaps in AML transaction monitoring controls:

### Know Your Customer (KYC)

Know Your Customer (KYC) and Customer Due Diligence (CDD) are essential components of an AML program. The information collected during the KYC process in particular provides a foundation for effective AML transaction monitoring throughout the entire lifecycle.

### Rules testing

The availability of Sumsub's dry-run mode allows businesses to test preset and custom rules before implementation, so you can detect how newly created rules may affect your transactions. This function enables companies to check if new rules are set up correctly, which helps properly detect suspicious activity in different scenarios.

### Suspicious pattern detection

The problem with standard suspicious pattern detection tools is that they do not go beyond generic screening parameters. Sumsub's AI actively trains pattern analysis to detect illicit activity outside of industry norms, so it is possible to uncover criminal groups performing fraud and money laundering despite their best efforts to conceal it. Plus, the zero-code visual interface allows you to quickly build and customize rules based on your specific industry needs.

# Anti-money laundering (AML) rules

Transaction monitoring can analyze user behavior patterns, transaction details, and many other signals to help your compliance specialists make informed decisions. Pre-set and customizable rule building is a crucial component of transaction monitoring, and rule designs must differ depending on customer profiles.

This section reveals how AML rules and Financial Action Task Force (FATF)<sup>1</sup> guidelines can be applied to monitor customer activity in different scenarios.



Three components define rules:

An illustration showing three overlapping cards representing rule building components. The top card is titled 'Conditions' and shows an 'If' dropdown menu, a right-pointing arrow, and an 'Add condition' button. The middle card is titled 'Rules' and shows 'Put on hold' buttons and a 'Score: 30' indicator. The bottom card is titled 'Actions' and shows 'Put on hold' buttons, a 'Reject' button, and a 'Score: 40' indicator.

<b>Title</b>
Rule name
<b>Condition</b>
The data that triggers the rule (i.e., the transaction amount exceeding the specified threshold)
<b>Action</b>
The event that follows the rule if it is matched

<sup>1</sup> The Financial Action Task Force (FATF) is a global money laundering and terrorist financing watchdog. The inter-governmental body provides international standards that aim to prevent illegal activity and their impact on society at all levels.

## AML rules

Used to initiate watchlist and adverse media screening of the transaction counterparty and act on the results.

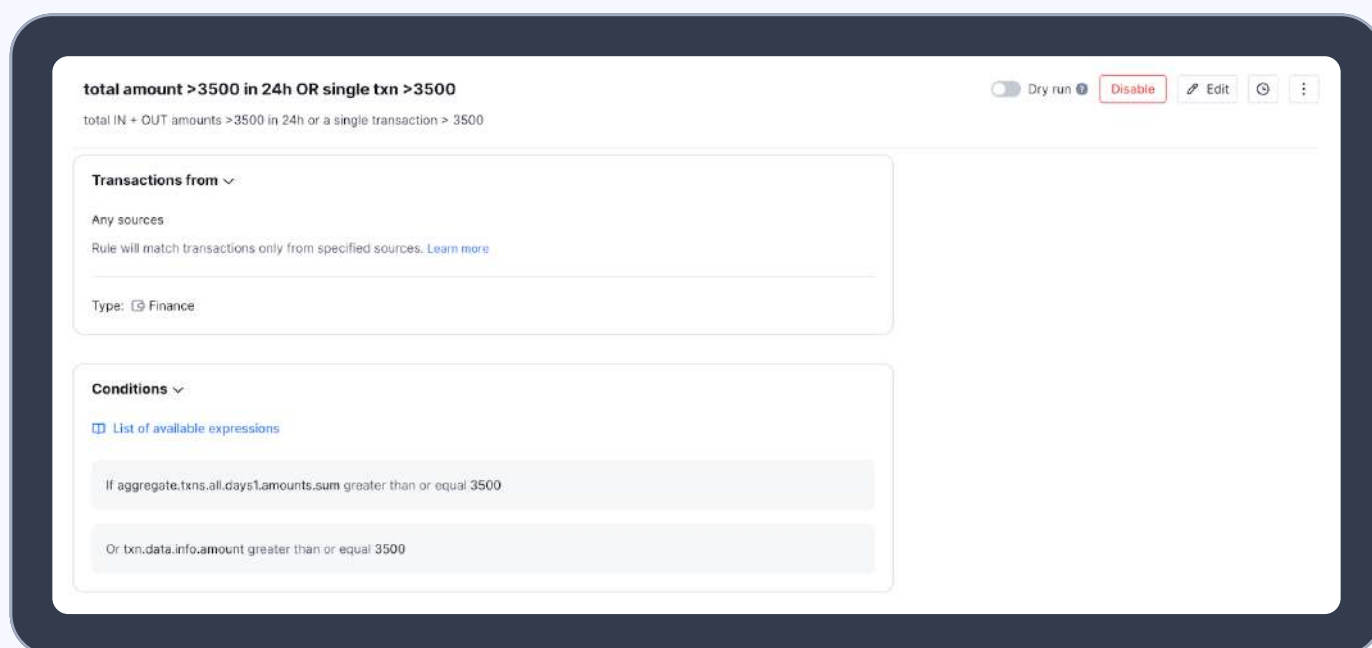
Title	Condition	Action
AML Check (including adverse media, sanctions, and PEP screening)	System rule. Initiate screening of the counterparty profile through sanction, PEP, and other databases.	Rules and triggers are enriched with data. For instance, risk labeling occurs after customer data is collected.
Counterparty with true positive AML hit	Reject the transaction if the compliance officer marks the AML hit as a true positive.	Reject transaction
Counterparty with potential AML hit	Put the transaction on hold and notify the assigned expert after the first rule is matched.	Put transaction on hold



## Leveraging AML transaction monitoring rules

This example will tackle one of the most commonly used transaction threshold rules.

We have set the value to \$3,500 to meet and exceed the current AML reporting threshold in the US.



In this case, the AML rule will be triggered if the customer deposits or withdraws \$3,500 or more in 24 hours or if a single transaction exceeds this amount.

If we look at the first case study mentioned earlier, involving Danske Bank and the CJA, it's easy to see how this AML transaction monitoring rule should have been used. However, the main reason the bank was fined was not because of their transaction monitoring processes alone, but because they did not report the inadequacies of the overall system after an internal audit. The correct procedure would have involved notifying the branch of these transaction monitoring failings and the risks they posed.

Next, we will look at how to monitor and stop a common money laundering technique known as smurfing.



## Smurfing

This technique involves structuring large amounts of money into smaller and multiple transactions. The people moving these smaller amounts – known as smurfs – will often spread the transactions over various accounts to keep them under the regulatory reporting thresholds and avoid detection.

Below is an example of how you can proactively stop smurfing. This AML rule compares ingoing and outgoing transactions and checks if a withdrawal amount is 10% less than the original deposit amount. This is a tell-tale sign of money laundering because the participant is usually paid a percentage for their efforts.

### Withdrawal in 5min after Deposit & sum OUT < sum IN 5min by 10%

Rapid Outgoing transactions in 5 min after the deposit made AND outgoing SUM > 90% of the initial deposit

#### Conditions ▾

[List of available expressions](#)

```
If txn.data.info.direction equals out and diffPctGte(aggregate.txns.out.minutes5.amounts.sum, aggregate.txns.in.minutes5.amounts.sum, -10)
```

#### Affect applicant ▾

Change level PoSoF

Add tags Suspicious pattern

This rule can trigger one or both of the following automated actions:

1. Customer is asked to provide proof of Source of Funds (SOF)
2. Customer is assigned a tag that will show if further transactions are made

Sumsub makes it easy to detect money laundering with an expansive variety of customizable rules. In the rule below, you can see how the conditions can be altered if customers attempt to initiate multiple outgoing transactions within a certain time period after registration:

The screenshot displays the configuration for an AML rule titled "AML: New user 5d out >5k". The rule description is "Total OUT amount >5k in a default currency within 5 days after registration & only 1 IN transaction".

The configuration is set to "Conditions" and includes the following logic:

- Condition 1:** "If" `applicant.createdAt.ageInDays` is "less than or equal" to the value "5". A tooltip indicates: "Expression indicates the applicant's age in days".
- Condition 2:** "And" `aggregate.txns.out.allTime.a...` is "greater than" the value "5000". A tooltip indicates: "Here we refer to the Sum of all outgoing transactions and comparing it with threshold".
- Condition 3:** "And" `aggregate.txns.in.allTime.am...` "equals" the value "1". A tooltip indicates: "Checking that applicant had only 1 incoming transaction".

Additional options include "List of available expressions", "Delete group", "+ And", "Add score", and "+ Or group".

If the above rule is triggered, a risk score of **40** will be added to the customer, and based on the threshold settings (on the right side of the screen), the transaction status will change to **Put on Hold**

The screenshot displays the configuration page for an AML rule titled "AML: New user 7d out >5k". The rule description is "Total OUT amount >5k in a default currency within 5 days after registration & only 1 IN transaction".

**Rule Details:**

Type	Name	ID	Last updated	Created by
Finance	aml-new-user-7d-out-5k-ynHf	64d0fdf17b47e45eff859169	Aug 7, 2023 6:21 PM	Service

**Configuration** | Performance

**Rule actions**

- Only score
- Add score: 40

**Add tags to transaction**

- Structuring

**Priority when trigger rule**

0

**Stop on match**

Scanning **will not be stopped** if the rule is matched

**Total score range**

Score Range	Score
Total score range	40
Rule score	40
Conditions score	0

**Thresholds**

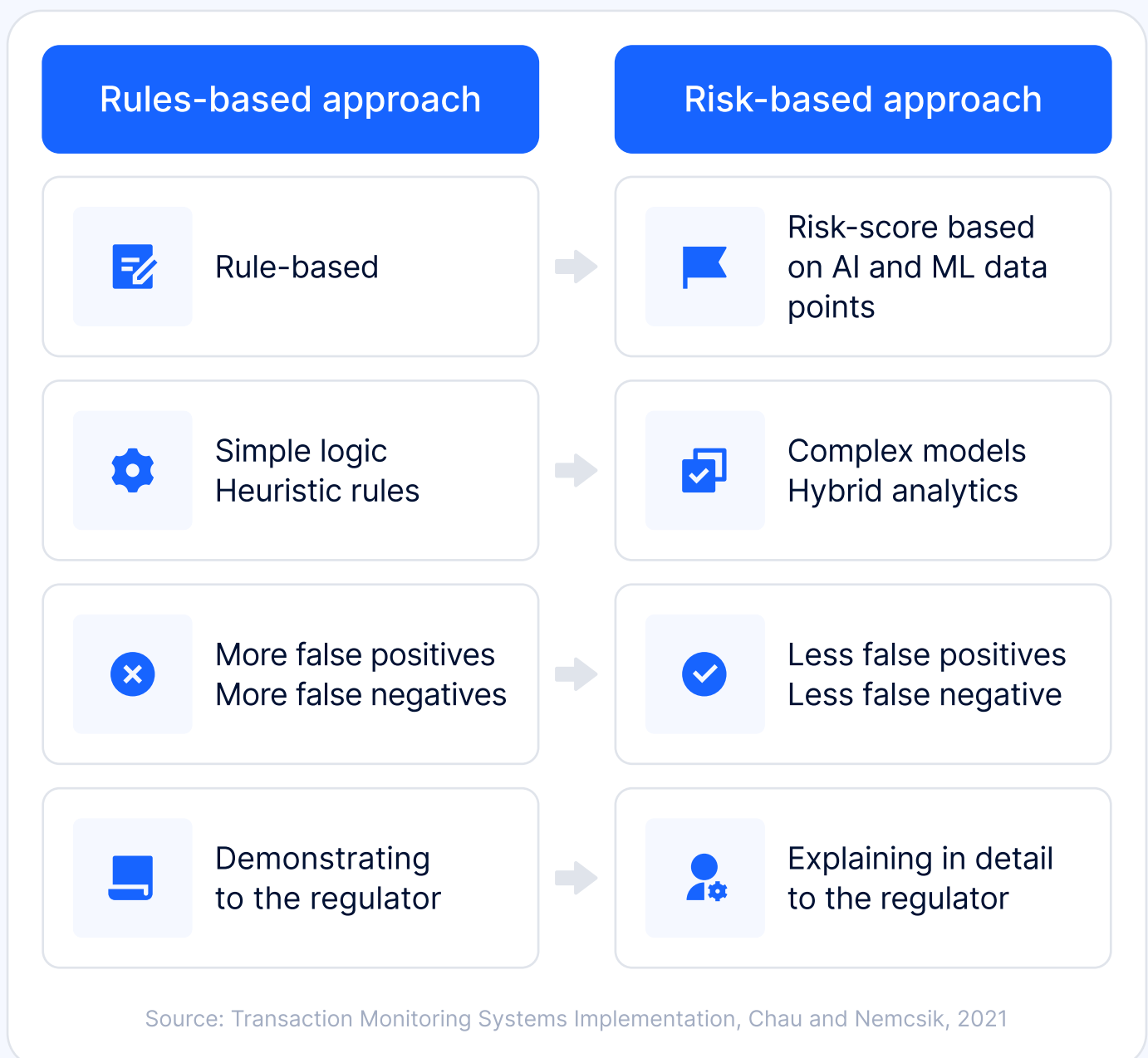
The status of the transaction will depend on the rule action and where the total score falls within the set threshold in Settings.

Score Range	Action
0 — 39	Approve
40 — 59	Put on hold
60+	Reject

## The evolution of transaction monitoring

Transaction monitoring is continuing to evolve from a rules-based to a risk-based approach. The risk-based approach pays increasing attention to regulatory outcomes and interconnected activities throughout an organization. This makes systems more adaptable and provides more accountability for outcomes.

This table summarizes the key benefits of risk-based approaches:



## Leveraging FATF transaction monitoring rules

### FATF rules

Rules to ensure compliance with FATF recommendations.

Title	Condition (the event that follows if the rule is matched)	Action
FATF black list countries	Reject transaction	Reject the transaction if the applicant's address or the payment method's issuing country is on the client's FATF black-flagged countries list.
FATF gray list countries	Put transaction on hold	Put the transaction on hold if the applicant's address or the payment method's issuing country is on the client's FATF gray-flagged countries list.

FATF transaction monitoring rules can be triggered if customers or the parties involved are located in a high-risk country. Plus, it can be a red flag if there is no apparent commercial reason for parties being connected via the transactions. Multiple transactions between the same parties in a short period of time can also be a cause for concern.

In the example shown below, we can see the **FATF black list country rule**, which will add a score of **100** and result in a **rejected transaction** if triggered.

### KYC customer from FATF black list country

Reject applicant if any of his data belongs to the FATF black list countries list

Type	Name	ID	Last updated	Created by
KYC	fatf-red-flag-cou-copy-CFKZ	64d0c4a0f6373405bac55002	Aug 7, 2023 2:17 PM	Service

[Configuration](#) [Performance](#)

#### Rule actions

Reject Add score: 100

---

Add tags to transaction

-

---

Priority when trigger rule

0

---

Stop on match

Scanning **will be stopped** if the rule is matched

The conditions show the expressions of the rule and the associated risk level. The full list of high-risk countries is available [here](#).

### KYC customer from FATF black list country

Reject applicant if any of his data belongs to the FATF black list countries list

**Conditions** ▾

[List of available expressions](#)

If Applicant country is in clientLists.fatf\_red\_flag\_countries

Or data.applicant.paymentMethod.issuingCountry is in clientLists.fatf\_red\_flag\_countries

Or Country is in clientLists.fatf\_red\_flag\_countries

**Affect applicant** ▾

Add risk level **High**

The transaction will be rejected if a risk score of 100 is added and Enhanced Due Diligence (EDD) may be required.

## Enhanced Due Diligence (EDD)

EDD is a set of measures applied in situations that indicate a higher risk of money laundering and terrorist financing. EDD measures include:

- Obtaining specific information about the customer (e.g., source of funds)
- Determining the customer's beneficial owner
- Establishing the purpose and intended nature of the transaction



# How to develop an AML program in six steps

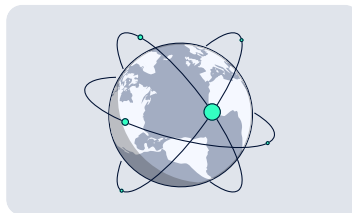
An effective AML compliance program will help prevent suspicious customers or transactions from entering the financial system. However, criminals constantly invent sophisticated money laundering and fraud methods to fly under the radar. Therefore, developing an AML program that can handle new and complex fraud attempts is essential. Otherwise, businesses expose themselves to financial and reputational losses.



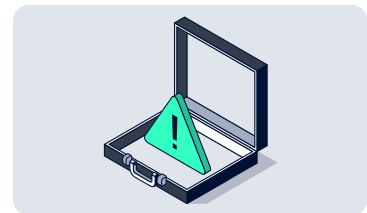
To create a compliance program, an organization has to summarize and define its potential risks and legal obligations, such as:



The money laundering risks it is exposed to and mitigation of these risks



Applicable local AML regulations and global rules



Potentially suspicious activities within the company



The following steps will help you develop your own AML compliance program:

### **Appoint an AML compliance officer**

AML legislation in most countries requires obligated entities to appoint an AML compliance officer/MLRO. This person handles everything related to the compliance program, such as internal audit management, compliance analysis, the development of appropriate guidelines, and employee training programs. In addition, the AML compliance officer is responsible for obligatory suspicious activity reporting.

### **Conduct employee training**

It is necessary to design an employee training program to meet the AML requirements of the company. The program should be scheduled per recent legislative changes or after serious incidents, such as employees involved in money laundering. If such incidents occur, the existing policy is ineffective and must be amended.

### **Perform risk assessments**

Relevant authorities require financial institutions to take steps to identify and assess their money laundering and terrorist financing risks, including factors relating to customers, countries, or geographic areas, as well as products, services, transactions, or delivery channels.

## Develop internal policies and procedures

Every financial institution must perform due diligence procedures that follow regulatory compliance demands and internal policies. Obligated firms must perform Customer Due Diligence (CDD) and ongoing monitoring for both natural and legal persons. The practices may vary depending on the nature of the money laundering risks and the firm's size.

Major regulators like the Swiss Financial Market Supervisory Authority (FINMA), Financial Conduct Authority (FCA), Cyprus Securities and Exchange Commission (CySEC), and the Monetary Authority of Singapore (MAS) have approved the AML solutions and systems at Sumsb.

## Detect suspicious activity and report it

It is necessary to expose red flags, such as:

- Atypical or abnormally large transactions
- Insufficient client information
- Any fake data submitted by a client

The complete list of suspicious triggers can be found [here](#).

Reporting is one of the main requirements for AML compliance. Based on FATF Recommendation 20, if a financial organization has reasons to suggest that certain funds were accumulated illegally or are linked to fraud and terrorism, it must promptly report them to a Financial Intelligence Unit (FIU).

## Organize independent audits

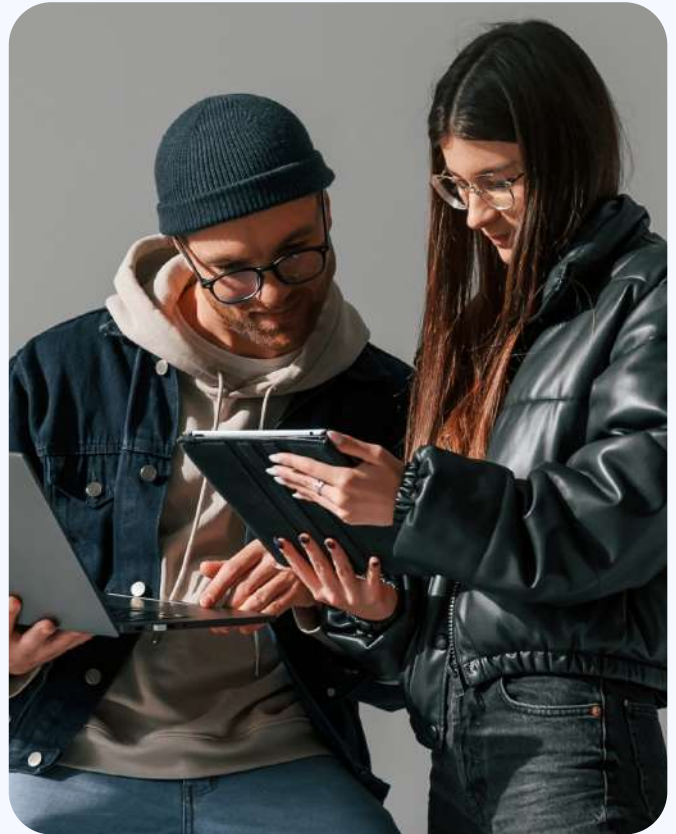
An excellent way to find flaws in a company's risk assessment and compliance program is to have it reviewed by an independent auditor. This review would include checking KYC due diligence procedures, compliance training, monitoring, and reporting systems. Financial regulators use such audits to check whether companies successfully prevent money laundering crimes.

## Part 2: Anti-fraud transaction monitoring

### What is fraud?

Fraud is a deliberate act of deception intended to give the offender an unauthorized benefit or to deny the victim of a legal right, and the global rate rises every year. The majority of fraud occurs online, and the international costs of online crime are predicted to reach \$10.5 trillion by 2025.

To put this into perspective, Steve Morgan, Editor-in-Chief of Cybercrime Magazine, notes that the value of all cybercrime committed is on par with the world's largest economies, where it would be the third largest after the US and China.



### What is transaction fraud?

Transaction fraud occurs when stolen credit card data is used for illicit purposes. It can affect almost any seller, from enterprise companies to the smallest businesses. By investing in anti-fraud transaction monitoring technologies, businesses can successfully battle fraud, safeguard their clients and brand, maintain regulatory compliance, and realize long-term cost savings.

There are three broad categories of transaction fraud:



### Phishing/social engineering

Phishing is a type of social engineering attack where criminals use psychological manipulation to extract sensitive information from people and make fraudulent transactions.



### Card fraud

Card fraud usually involves the unauthorized use of payment information (card number, billing address, CVV, and expiration date) to purchase products online.



### Chargeback fraud

Sometimes ironically referred to as "friendly fraud", chargeback fraud is where an individual denies buying an item on a credit or debit card to get a refund from the card provider.

## Online payment fraud statistics

According to the AFP 2022 Payments Fraud and Control Report:

 **71%**

of survey respondents reported their organizations falling victim to payment fraud attacks in 2021

 **68%**

of organizations were targeted by business email compromise (BEC) in 2021

 **66%**

of all payment fraud was committed using checks, with 37% committed using ACH debits

 **58%**

of survey respondents stated that their Accounts Payable departments fell victim to payment fraud through email scams. AP departments continue to be the most susceptible to BEC

[Sumsb blog: What You Need to Know about Online Payment Fraud in 2023](#)

According to Statista, e-commerce losses to payment fraud were estimated at \$41 billion globally in 2022, up from the previous year. This figure is expected to grow to \$48 billion by 2023.

# Why is anti-fraud transaction monitoring important?

Here are some of the most important reasons why anti-fraud transaction monitoring can give you instant and long-term value:



## Fraud detection and prevention

Businesses can reduce damage by identifying fraud in real time. Advanced analytics, machine learning algorithms, and rule-based detection help react rapidly to suspicious patterns, abnormalities, and possible real-time fraud.



## Enhanced customer trust

In addition to protecting financial assets, anti-fraud transaction monitoring demonstrates a commitment to overall customer security. This builds consumer trust and loyalty and reduces reputational risk.



## Regulatory requirements

Transaction monitoring is required for regulated businesses because AML/CTF laws require it as a part of due diligence measures and suspicious activity reporting. If businesses fail to comply, they risk incurring regulatory penalties and fines. Anti-fraud transaction monitoring reviews transactions, detects fraud, and provides regulatory reporting documents to help organizations meet their obligations.



## Cost saving

Companies can avoid financial losses and costs related to investigations, legal proceedings, and consumer refunds by establishing comprehensive anti-fraud transaction monitoring. According to the Association of Certified Fraud Examiners (ACFE) 2020 Report to the Nations, firms without anti-fraud measures lost a median of 5% of revenue to fraud.

## Real-life challenges

Why is transaction fraud still so prevalent? The answer is simple and twofold:

### Ease of criminal access

Buying stolen credit card information is easy. McAfee researchers estimate that stolen credit card information can be bought for as little as \$5 in the US and between \$25 to \$30 in Europe.

### Lack of prosecution

Online fraud is rarely prosecuted. Cases can be complex and time-consuming to investigate—and when crimes cross international territories, there can be jurisdictional issues. Plus, extradition is costly, even if large frauds occur and perpetrators are identified.

#### Case study #3

### When fraudsters attack on P2P platforms

Zelle is an app that lets people send money to each other from their own bank accounts using peer-to-peer (P2P) transactions. The service processed \$490 billion in payments in 2021—many of which included a significant amount of fraud. Many fraudsters deceive their victims into allowing Zelle payments, and banks say they are not required to reimburse authorized transactions.

In 2021 and the first half of 2022, four banks had 192,878 Zelle-related payment fraud complaints totaling \$213.8 million. Banks only repaid 3,500 clients in total, with just 47% of the unauthorized financial transfers refunded.



## Three important rules for anti-fraud transaction monitoring

Now, let's look at three examples of anti-fraud transaction monitoring rules you can implement to avoid the issues mentioned in the previous case studies.

The rule below will show you how different internet protocol (IP) addresses can be compared to determine if any are anomalies. The following addresses are compared in the **IP distant location** rule:

### Address 1

Device IP  
(from current user session)

### Address 2

Proof of Identity  
(POI) IP  
(extracted from the attached document)

### Address 3

Camera IP during  
a liveness check

#### IP distant locations

##### Stop on match

Scanning **will not be stopped** if the rule is matched

##### Transactions from ▾

Any sources

Rule will match transactions only from specified sources. [Learn more](#)

Type:  KYC

##### Conditions ▾

[List of available expressions](#)

if applicant.riskLabels.device contains distantIpLocations

Since fraud is often connected to suspicious IP address location patterns, the rule has the following actions and conditions:

The screenshot shows a rule configuration page for a rule named "> 4 IP countries for the same remitter in 1 week". The rule is currently in "Production" mode and is a "Dry run". It is set to "Put on hold" if the remitter used more than 4 IP addresses located in different countries >4 within 1 week.

**Rule details:**

- Type: Finance
- Name: TXDE2
- ID: 64d105482c364c2d26ee41d9
- Last updated: Aug 7, 2023 6:52 PM
- Created by: Service

**Configuration options:**

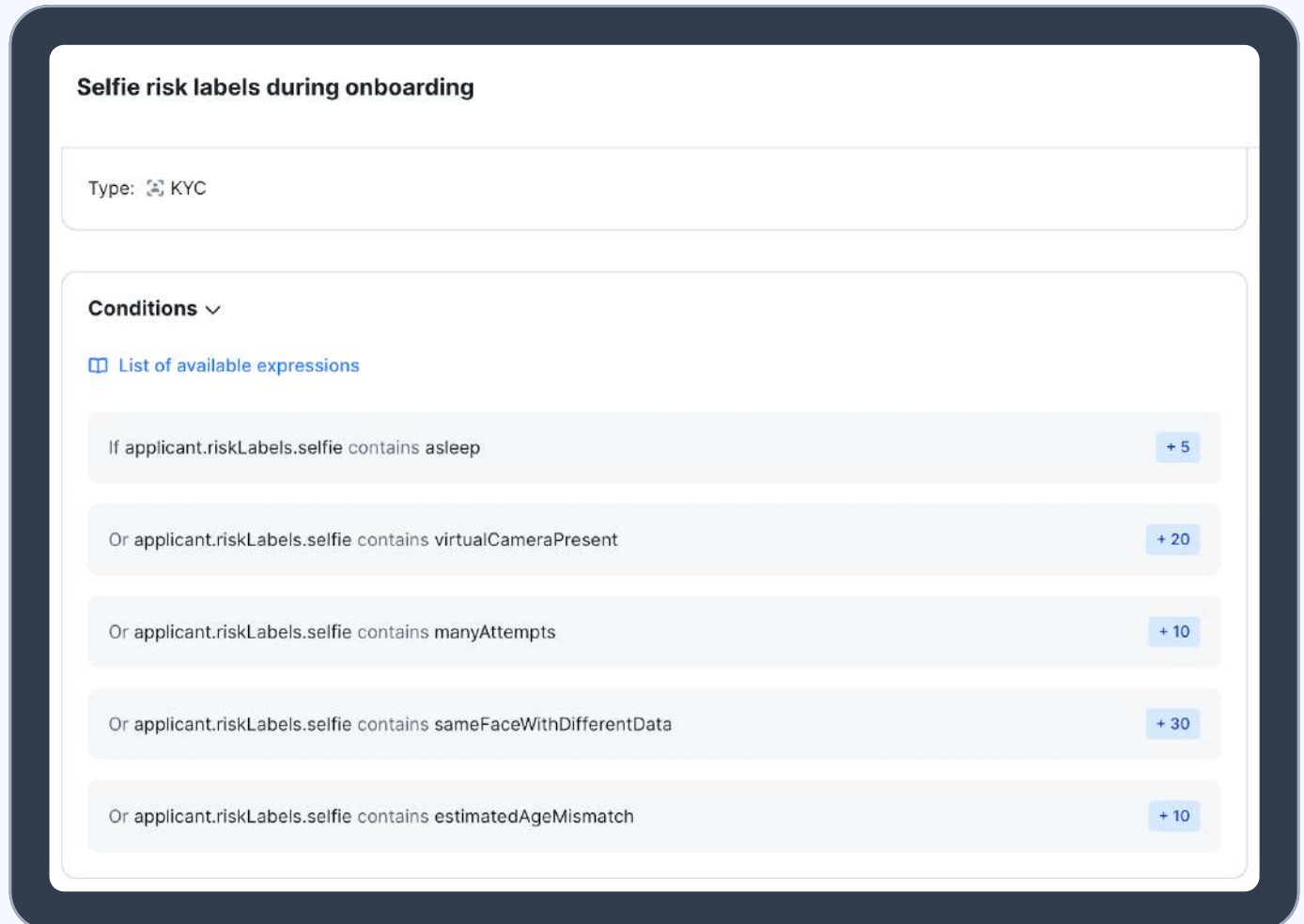
- Rule actions:** Put on hold (Add score: 0)
- Add tags to transaction:** -
- Priority when trigger rule:** 0
- Stop on match:** Scanning will not be stopped if the rule is matched.
- Transactions from:** Any sources. Rule will match transactions only from specified sources. Type: Finance.
- Conditions:** If aggregate.txns.sameRemitter.days7.ipCountries.distinctCnt greater than 4.
- Affect applicant:** Add tags: IP fraud.
- Raw condition:** >

**Score and Thresholds:**

- Total score range: 0
- Rule score: 0
- Conditions score: 0
- Thresholds:**
  - 0 — 39: Approve
  - 40 — 59: Put on hold
  - 60+: Reject

A "Test configuration" button is located at the bottom left of the configuration area.

Fraudsters can also be stopped by using more advanced liveness or selfie checks. Below, you can see the rule conditions that help prevent fraud at the KYC stage:



The screenshot shows a configuration interface for a rule titled "Selfie risk labels during onboarding". The rule is categorized as "KYC". Under the "Conditions" section, there is a list of available expressions that can be added to the rule. Each expression is shown in a light blue box with a corresponding risk score in a small blue button on the right.

Condition	Risk Score
If applicant.riskLabels.selfie contains asleep	+ 5
Or applicant.riskLabels.selfie contains virtualCameraPresent	+ 20
Or applicant.riskLabels.selfie contains manyAttempts	+ 10
Or applicant.riskLabels.selfie contains sameFaceWithDifferentData	+ 30
Or applicant.riskLabels.selfie contains estimatedAgeMismatch	+ 10

## Detecting account takeovers or sold accounts

This rule allows us to check if the remitter (or sender) has used 3 or more different devices in 7 days. We developed this rule to tackle account takeovers and illicit account selling, combining it with IP address detection to provide more clarity about suspicious behavior.

### 3 or more different devices in 7 days

Add 3 points to the transaction risk score if the transactions from the same remitter were initiated from 3 or more different devices within the previous 7 days.

#### Transactions from ▾

Any sources

Rule will match transactions only from specified sources. [Learn more](#)

Type:  Finance

#### Conditions ▾

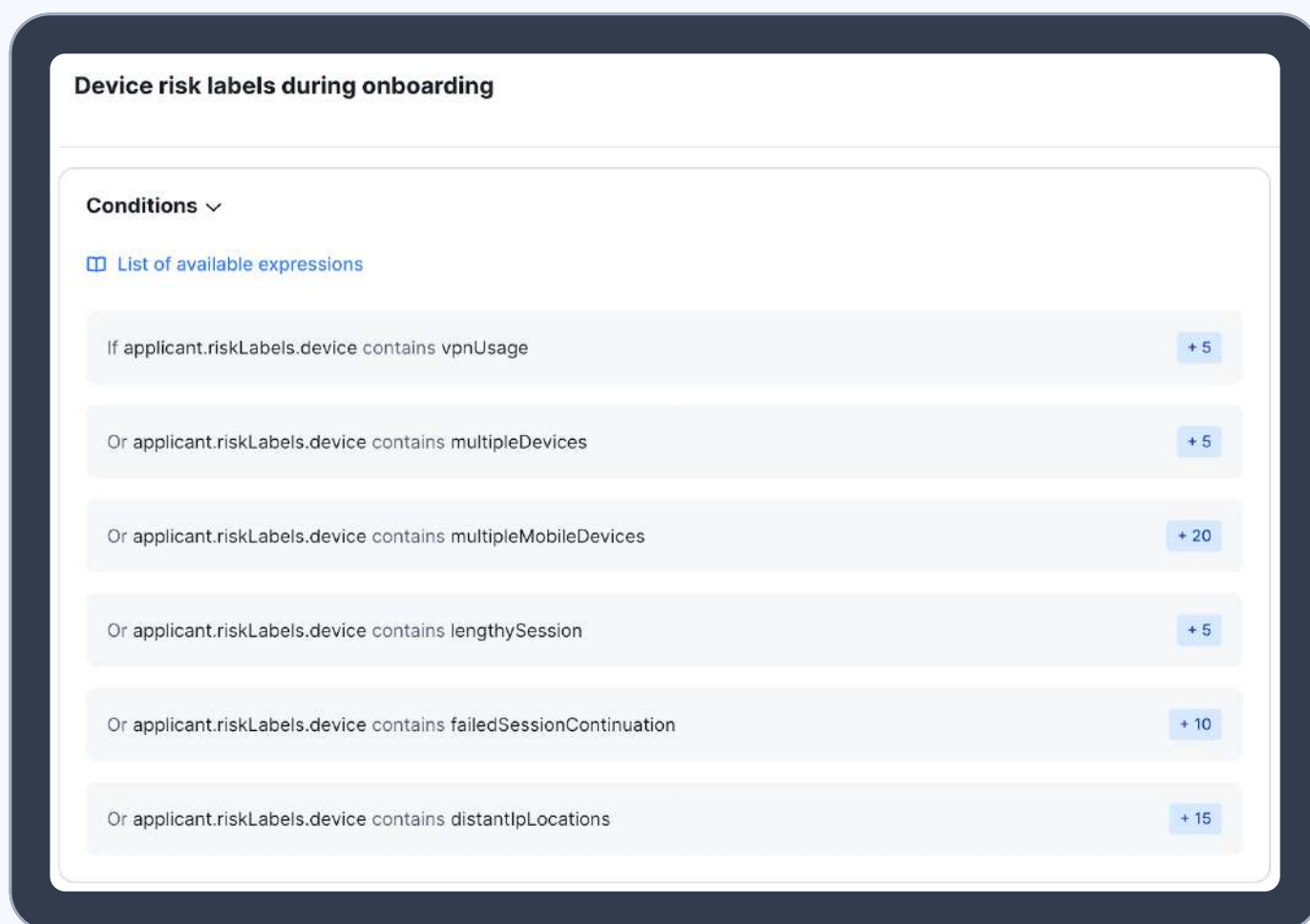
[List of available expressions](#)

If `aggregate.txns.sameRemitter.days7.deviceFingerprints.distinctCnt` greater than or equal 3

## Detecting risk labels during onboarding

Frequent device switching during onboarding is a common sign of fraudulent behavior. Therefore, we created the following rule to detect:

- Active VPN use during onboarding
- Multiple device usage (i.e., some steps are passed on one device, but documents are uploaded from another)



The screenshot shows a rule configuration interface titled "Device risk labels during onboarding". Under the "Conditions" section, there is a "List of available expressions" button. Below this, several conditions are listed, each with a corresponding score:

- If applicant.riskLabels.device contains vpnUsage (+ 5)
- Or applicant.riskLabels.device contains multipleDevices (+ 5)
- Or applicant.riskLabels.device contains multipleMobileDevices (+ 20)
- Or applicant.riskLabels.device contains lengthySession (+ 5)
- Or applicant.riskLabels.device contains failedSessionContinuation (+ 10)
- Or applicant.riskLabels.device contains distantIpLocations (+ 15)

Sumsu's transaction monitoring solution adjusts to advances in the fraud landscape, and the scenarios shown in this eBook are only a snapshot of what our platform has to offer you.

No matter the challenges, we help businesses stay ahead of fraud and money laundering with ease.

# Summary

Successful transaction monitoring requires creating properly automated alert systems, since even the most advanced transaction monitoring systems cannot prevent fraud or money laundering if alerts are not actioned.



Sumsub helps companies focus on workflows that administer fine-tuned transaction monitoring rules by offering your company the following:

## Full lifecycle coverage

- Reusable onboarding data for transaction monitoring
- KYC in 50 secs with more than 14k documents supported
- Doc-free verification (in certain countries)
- Cross-border team of compliance experts
- High conversion rates across the globe (UK: 95%, US: 91%, Spain: 97%)

## No-code customization

We offer a solution architect who will build advanced transaction monitoring rules for your business needs. Transaction monitoring rules are easily customized with no coding required, while preset rule bundles provide instant usability.

## Industry validation

2000+ clients trust Sumsub, and our devoted customer support team works hard to ensure your company can secure every step of the user journey with confidence.

# Ready to improve your compliance team's performance?

Stay ahead of the most advanced fraud and money laundering schemes with Sumsub's transaction monitoring solution.

We seamlessly integrate transaction monitoring with your workflow, so that user, business, and onboarding verification are consolidated within one system.

[Speak to our experts →](#)

