



False Positives in AML Screening

AML flag analysis and measures to reduce false positives

How many alerts turned out to be false positives using both individual client and company screenings

Reviewed AML flags · False positive share

Closed as false positives

All checks 95% false positive



Individuals 97% false positive



Companies 89% false positive



False positive Other reviewed flags

AML screening · Flag rate

Checks with a potential match

Companies 24%



Individuals 9%



Company checks flagged

2.6x more often

The research is based on real AML screening checks from iDenfy's platform

Every figure in this report comes from anonymized AML screening checks that iDenfy's partners ran through our platform as part of their real compliance workflows. The dataset covers **71,260 checks** on individuals and companies, screened against AML databases such as sanctions lists, PEP databases, watchlists and adverse media, depending on each partner's configuration.

1 Individuals · 67,804 checks

AML screening of natural persons, for example, customers screened during KYC onboarding or ongoing monitoring.

2 Companies · 3,456 checks

AML screening of legal entities, for example, business clients screened during Know Your Business (KYB) onboarding.

71,260

AML screening checks
On individuals and companies

10%

Overall flag rate
Checks that returned at least one potential match

95%

Of reviewed flags were false positives
Based on 1,300+ flags reviewed and resolved

2.6x

Higher flag rate for companies
24% for companies vs. 9% for individuals

1,280

False positives closed
After a manual review by compliance teams

186

Countries & territories
Linked to the screened records

How to assess the AML hits?

A flag is a potential match that the system raises during an AML check. Not every flagged check gets a final decision straight away. Some flags are forwarded to a compliance analyst for extra review, depending on the severity and risk of the AML flag. To show how many flags turn out to be false positives, we only counted the flags that had already been reviewed manually and closed as either a true or a false positive. **The false positive share is the number of false positives divided by all reviewed flags.** Flags still waiting for review are left out. The flag rate is the share of all checks that returned a potential match. Percentages are rounded to whole numbers.

What counts as a false positive?

A false positive is an alert that flags a customer as a potential match to a risk signal in an AML database, even though they're a genuine client who isn't linked to the identified risk. Name matching is the method AML screening is based on, so false positives are a normal outcome, not an error. The goal is to control how many appear and how fast your team clears them.

The essence

False positives in AML screening are alerts that flag individuals or businesses as potential matches to a risk record when they are not actually linked to that risk. Reducing false positives helps compliance teams spend less time investigating irrelevant alerts and more time identifying genuine high-risk cases without weakening screening controls.

How many AML flags are false positives?

Most of them.

Compliance teams reviewed and resolved 1,300+ potential matches found during AML screening. Across individual and company screening combined, **95% of them turned out to be false positives**.

Individuals · 67,804 checks

Flag rate 9%



False positive share of reviewed flags 97%



1,047

False positives closed

About 97 of every 100 reviewed flags on people were false positives

Companies · 3,456 checks

Flag rate 24%



False positive share of reviewed flags 89%



233

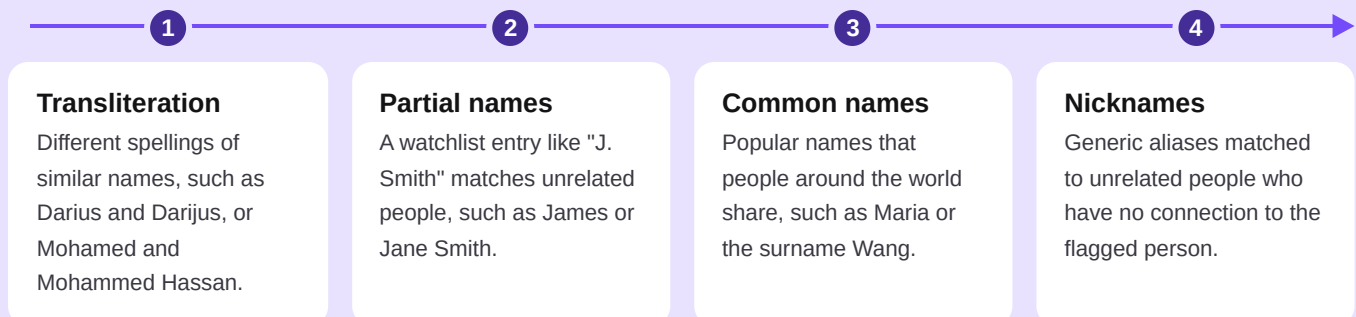
False positives closed

About 89 of every 100 reviewed flags on companies were false positives

Research summary

Type	Total AML checks	Flag rate	False positives	False positive share of reviewed flags
Companies	3,456	24%	233	89%
Individuals	67,804	9%	1,047	97%

Why false positives happen



Get inspired by our success story

iDenfy × FTMO®

Automating KYB onboarding with built-in AML screening

FTMO onboards business clients through iDenfy's KYB platform. **Built-in PEP and sanctions screening quickly detects red flags that may require manual review or a stricter onboarding flow**, while extra documents are requested automatically.

98%

Overall KYB success rate

40 hrs

Saved per week with KYB/AML workflow automation

180+

Company registries connected

120+

Countries covered by registry access

[Read the case study →](#)

Company checks raise 2.6x more flags than individual checks

Why company names get flagged

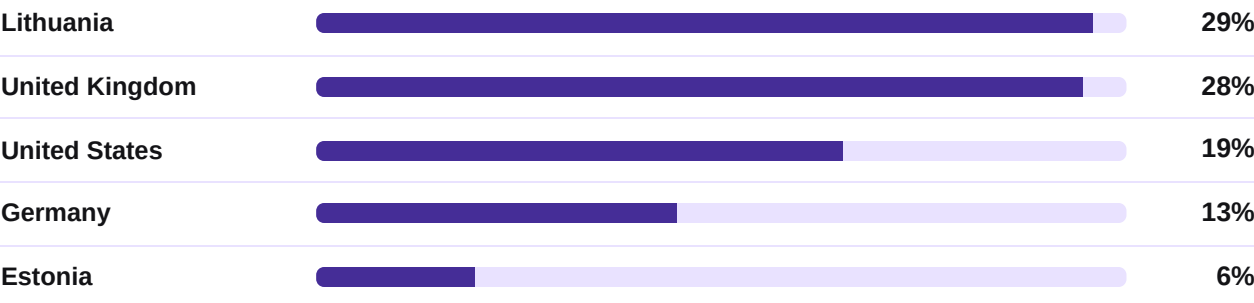
The same principle of nearly identical names applies to corporate entities. Common terms like "Trading", "International" or "Group" appear in many company names, so a single listed entity can return potential matches for unrelated businesses with similar names.

What it means for compliance teams

Compliance teams are required to review more alerts when screening businesses than when screening individuals, **increasing the manual workload, especially during KYB onboarding.**

Company flag rate by country

Countries with 100+ company checks · flag rate



Among countries with 100+ company checks, **company flag rates range from 6% to 29%**, compared with an overall individual flag rate of 9%.

Note: based on iDenfy's in-house data and its partners' usage of AML screening.

24%

Company flag rate

Almost 1 in 4 company checks raised a potential match

2.6x

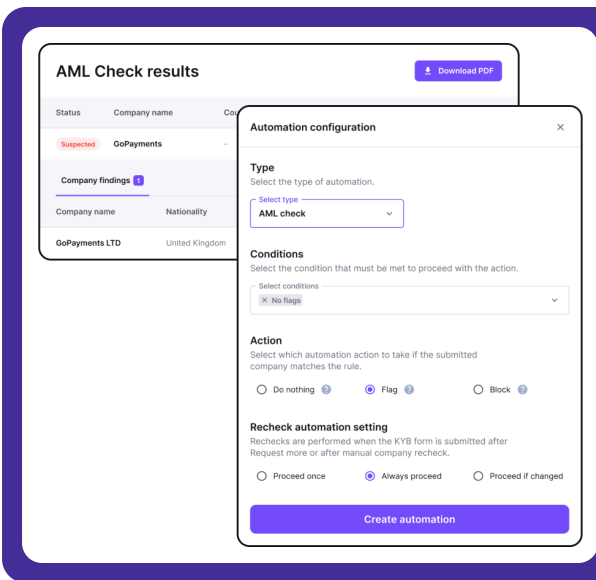
Higher than individuals

Company flag rate vs. the 9% individual flag rate

89%

Of reviewed company flags

Were closed as false positives



Let rules handle the clean cases

With iDenfy, you can build workflows using custom rules, based on risk factors such as the user's jurisdiction, to **automate approvals for cases without AML hits** while forwarding flagged cases for manual review.

Cleared matches stop triggering alerts unless new information appears, and you can download PDF reports with access to the original data sources.

Five ways to handle false positives without missing true matches

The more data you have and the more you customize your AML screening settings, the less likely you are to bump into incomplete or outdated data that also affects the false positive rate.

01 Set matching criteria based on risk

Requiring three or more matching criteria can cause genuine risks to go undetected, since some PEP records only contain a name and a country. Assign different weights instead: a full name and date of birth match is stronger evidence than a name-only match.

02 Prioritize alerts by match strength

Alerts with multiple matching identifiers go to further investigation first. Name-only matches and common names can receive a quicker initial review. The goal is to detect genuine risks, not to rule out every false positive as fast as possible.

03 Screen with verified data

Incomplete, inaccurate or outdated data makes it harder to tell genuine matches from unrelated people or businesses. Combine KYC and AML in one system, so screening runs on data extracted from a verified ID document.

04 Remove bias and document decisions

Analysts need evidence, not assumptions. Record the identifiers checked and the reason for closing each alert, so your AML log stays audit-ready and shows that your processes were followed consistently.

05 Whitelist cleared matches

Once a match is resolved as a false positive, whitelist it, so ongoing monitoring doesn't raise the same alert again and analysts don't review the same profile twice.

Other tips on effectively managing false positives

- Check the match details and which database fired
- Compare secondary identifiers, such as date of birth, nationality or ID number
- Read the full source, for example, the article behind an adverse media hit
- Decide if it's a true or false positive, and escalate if unsure
- Document which identifier cleared the hit and who reviewed it
- Whitelist the cleared match

Measure your own rate

Track alerts confirmed as false positives against a clearly defined total, such as all reviewed alerts. Also monitor alert volumes, review times and confirmed matches to assess efficiency **without compromising detection accuracy**.

Screen across the lifecycle

AML screening starts at onboarding, before a business relationship begins, and **continues through ongoing screening** to detect new sanctions listings, changes in a customer's risk profile and other emerging concerns.



Spend your review time on real AML risks

iDenfy's AML Screening solution is designed to reduce unnecessary AML alerts. Adjust fuzzy matching thresholds, filter PEPs by level, combine ID verification with AML screening on verified data, and build custom rules that approve cases without AML hits while flagged cases go to manual review.

One flat fee per monitored subject, with daily rescreening included.

45,000+

Official AML sources screened

Real-time

Results with alerts for new AML hits

200+

Countries covered



[Explore AML Screening →](#)