Monetary Authority of Singapore

STRENGTHENING AML/CFT NAME SCREENING PRACTICES

INFORMATION PAPER

APRIL 2022

CONTENTS

Introduction

Name screening is a fundamental control in the anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks of financial institutions (FIs).

FIs screen the names of potential and existing customers, and their relevant parties[1], to identify associations with sanctions, politically exposed persons (PEP), and other adverse news. This identification enables FIs to assess potential money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks posed by these parties, and take steps to manage and mitigate these risks.

FIs typically perform name screening during customer onboarding, periodic Know-Your-Customer (KYC) reviews, ongoing batch screening, and transactions processing.

[1] For the purpose of this paper, "relevant parties" include customers' connected parties, persons appointed to act on their behalf, and their beneficial owners.

MAS' thematic inspections on name screening

MAS conducted thematic inspections on selected FIs' name screening processes, based on the requirements of MAS Notice 626/1014/824[2] on Prevention of Money Laundering and Countering the Financing of Terrorism for Banks, Merchant Banks, and Finance Companies respectively, as well as the corresponding Guidelines[3] to the Notices (collectively "the Notices and Guidelines").

Year of inspections: 2021

Coverage: Selected mid-size and small FIs

Objective: To assess the robustness of FIs' name screening frameworks and controls, relative to their risk profiles and business operations in Singapore

[2] Links to Notices:
626:https://www.mas.gov.sg/regulation/notices/notice-626
1014:https://www.mas.gov.sg/regulation/notices/notice-1014
824:https://www.mas.gov.sg/regulation/notices/notice-824

[3] Links to Guidelines to Notices:
626:https://www.mas.gov.sg/regulation/guidelines/guidelines-to-notice-626-on-prevention-of-money-laundering-and-cft-for-banks
1014:https://www.mas.gov.sg/regulation/guidelines/guidelines-to-mas-notice-1014-on-prevention-of-money-laundering-and-cft
824:https://www.mas.gov.sg/regulation/guidelines/guidelines-to-mas-notice-824-on-prevention-of-money-laundering-and-cft

In this paper

This paper sets out the observations and good practices noted by the thematic inspections, as well as MAS' supervisory expectations.

"Areas done well" and  "Areas for improvement" are observations from our benchmarking of the FIs' name screening practices.

FIs should benchmark themselves against the practices and supervisory expectations set out in this paper in a risk-based and proportionate manner. In doing so, FIs should give due regard to the risk profile of their business activities and customers.

Where FIs observe any gaps in their frameworks and controls, specific remediation/enhancement measures should be identified and implemented in a timely manner.

Typical name screening processes

1. Identify parties to be screened
2. Screen names against databases
3. Generate name screening results
4. Assess name screening hits if any
5. Follow up/ escalate if applicable

Scope of inspection

A. Senior management oversight

- Oversight of name screening frameworks and processes

B. Frameworks, policies and procedures (P&P)

- Identification of parties for screening
- Use of screening systems
- Criteria for alert assessment

C. Screening parameters and databases

- Setting of system parameters
- Inclusion of appropriate information sources
- Management of system screening lists

D. Alert resolution

- Assessment of screening alerts
- Documentation of alert assessment
- Checks and balances over alert resolution process

Overall observations

FIs generally had adequate management oversight and formalised P&P on the use of systems and resolution of alerts, to facilitate consistent implementation. However, the robustness of name screening practices was uneven across FIs.

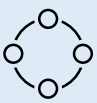
Senior management of some FIs did not exercise adequate oversight, leading to deficiencies in P&P and poor checks and balances over alert resolution. These resulted in lapses in the execution of name screening controls and, in some cases, potential regulatory breaches.

MAS also observed that several FIs placed undue reliance on system vendors to set the parameters in their name screening systems, without adequately understanding how the settings impact the accuracy and effectiveness of the screening results.

- There is a risk that the FIs' screening systems may not have been appropriately calibrated to cater to the risk profile of their business activities.
- FIs should adequately assess and test that the screening parameters are effective for generating name matches.
- FIs should draw their system vendors' attention to this paper, for them to gain a better understanding of MAS' expectations of FIs, and work with FIs to achieve them.

MAS' expectations of the Board and senior management

MAS looks to an FI's Board and Senior Management (BSM) to exercise oversight of the governance and implementation of effective name screening processes, as part of the FI's overall AML/CFT frameworks and controls. BSM should set an appropriate tone-from-the-top on the importance of these controls, and ensure that:



- adequate frameworks and P&P on name screening controls are established.

- relevant staff have a good understanding of the strengths and limitations of the FI's name screening systems (and their corresponding parameters), and have processes to assess if the systems are performing as intended.

- effective checks and balances, such as maker-checker controls and quality assurance (QA) processes, are implemented for alert resolution.

A. Senior management oversight

Supervisory expectations

Senior management exercises active oversight of FIs' name screening frameworks, policies, and processes, including compliance with the Notices and Guidelines.

Areas done well

Structured processes for management reporting

Senior management or the management committees responsible for overseeing ML/TF/PF risks had access to relevant information, to monitor and deliberate follow-up actions.

FIs established processes to track the ageing of unresolved name screening alerts, including details such as days outstanding, functions responsible, and weekly trends. The ageing reports are reported to management committees for discussion.

Areas for improvement

Inadequate attention by senior management

A small number of FIs' senior management did not pay adequate attention to name screening matters, resulting in deficiencies such as:

- Inadequate name screening P&P, leading to inconsistencies and lapses in the assessment and documentation of name screening results.
- Insufficient understanding and lack of regular reviews of name screening system parameters, resulting in risks that systems might not be generating alerts accurately or effectively as intended.
- Inadequate checks and balances (e.g. "four-eye checks" or QA controls) over the alert resolution process, which could lead to true hits being erroneously dismissed.
- No records of substantive discussions on AML/CFT matters during management meetings to demonstrate accountability of issues and basis of decisions.

MAS expects senior management to pay close attention to the implementation of sound AML/CFT frameworks and controls. FIs' senior management should also maintain adequate oversight of AML/CFT processes, including name screening processes, to ensure that they are operating effectively.

B. Frameworks, policies and procedures

Supervisory expectations

FIs establish adequate frameworks, P&P on name screening for customer onboarding, periodic KYC reviews, ongoing batch screening, and transaction processing, covering areas such as:

- ✓ Processes to identify and track customers and their relevant parties for screening
- ✓ Frameworks and P&P to understand and review system parameters
- ✓ Guidance on use of screening systems, including how names of customers and relevant parties should be input for effective screening
- ✓ Criteria to assess and dismiss name screening alerts

Areas done well

Clear policies and procedures

P&P included detailed guidance and illustrations on key areas such as:

- Input of names in screening systems to effectively generate results (refer to Case Study 1A).
- Criteria to assess, escalate and dismiss alerts under various scenarios (this is related to Section D on alert resolution).
- Documentation of assessment of alerts (refer to Case Study 1B).

Wider scope of identified parties for screening

Some FIs implemented regular screening of parties beyond baseline regulatory requirements, such as:

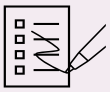
- Directors of intermediary shareholders
- Small or minority shareholders (e.g. shareholdings below 5%)
- Customers' major buyers and suppliers

B. Frameworks, policies and procedures

Areas for improvement

Inadequate tools for batch screening

A small number of FIs did not implement adequate systems or tools to perform ongoing batch screening (conducted between periodic KYC reviews) of customers and relevant parties against ML/TF/PF sanctions and non-sanctions databases.

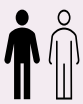


One FI conducted batch screening manually. Due to the large volume of information involved, the screening was not performed on a timely basis and was prone to human error.

Another FI's batch screening tool was unable to accommodate the names of all the relevant parties of customers (e.g. connected parties), and hence omitted them from the ongoing screening against some information sources (e.g. adverse news).

FIs should conduct regular batch screening of customers and relevant parties to identify new ML/TF/PF information in a timely manner (several FIs inspected performed batch screening on a daily basis). FIs conducting manual screening should ensure that safeguards are in place to mitigate human errors. Otherwise, FIs should consider a system solution to achieve more robust, automated, and efficient screening processes.

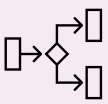
No screening of customers' former names



Some FIs did not screen, or did not formalise the requirement to screen, the former names of customers found in KYC documents. This could impede the identification of customers with adverse information under their previous names.

FIs should establish clear requirements to screen former names of customers where available.

No tracking of parties due for screening



Some FIs did not systematically identify and track the parties that were subjected to name screening requirements, resulting in some omissions and delays (e.g. an FI, without a screening checklist, omitted the screening of a customer's directors during onboarding and only rectified the lapse three months later).

FIs should implement structured processes to track parties for screening, to prevent/detect omissions and delays.

Case study 1 – Examples of good P&P

An FI's P&P provides guidance to staff on how various tasks should be performed. Having clear and detailed P&P is fundamental to promoting a consistent standard of practice and reducing errors in performance. These are particularly important in the execution of key controls, such as name screening. The two case studies below provide examples of effective P&P.

Case 1A – Guidance on input of names in screening system

FIs typically use systems to conduct name screening. The systems are either built in-house, or more commonly, provided by external vendors. Different name screening systems vary in how they read and match inputs for screening, i.e. how names are keyed into systems could affect their similarity to names on screening lists. For example, the input of "Company A Pte Ltd" vis-à-vis "Company A" could result in fewer matches or more false hits, depending on a system's parameters.

For optimal generation of alerts, FIs should adequately understand their screening systems and corresponding parameters, to determine the most effective way to input names for screening (also refer to Section C on screening parameters and databases). The guidance on the input of names should be clearly set out in an FI's P&P.

Example below illustrates how an FI's P&P clearly specifies the parts of names that should be excluded from screening. The example is not meant to be prescriptive, as it depends on the system being used. FIs should work with their respective vendors to determine the most appropriate input method to adopt.

Exclude these	Examples
Titles	Sir, Honourable, Professor
Legal entity status	Pte Ltd, Inc, Pvt, Ltd, GmbH, SA, NA, PT, Sdn Bhd, Co., LLC, LLP, PLC
Punctuations and symbols	parenthesis, apostrophe, period, comma, hyphens
Common words	&, and, or, the, generational designations e.g. Sr., Jr., II, III, familial relationships e.g. bin, s/o

Case study 1 – Examples of good P&P (cont.)

Case 1B – Requirement to document assessment of alerts

A robust assessment of name screening alerts is important to identify and manage any potential ML/TF/PF risks. It is also important to adequately document such assessment (e.g. information considered, work performed, preparer and approver) so that the basis and accountability for any decision made are clear. This also instils discipline amongst staff and mitigates the risk of staff dismissing an alert without performing adequate checks or follow-up actions.

To promote a consistent standard of documentation of alert assessment, FIs should set out the documentation requirements clearly in their P&P.

Below is an example of how the P&P clearly sets out the documentation requirements with illustrative examples.

Procedure requirement	Further guidance with specific illustration
For sanctions alerts, a minimum of two identifiers (i.e. attributes to identify an individual/entity, such as date of birth, country of incorporation) have to be documented when dismissing an alert. Identifiers must be specified to support the assessment for dismissing an alert.	To illustrate, if the two identifiers are date of birth and country of residence, it is NOT sufficient to state “Customer has different date of birth and country of residence.” The actual differentiating details need to be documented e.g. “Customer’s date of birth is 02/03/50 and he resides in Country A, while alert name’s date of birth is 03/04/70 and he resides in Country B.”

C. Screening parameters and databases

Supervisory expectations

FIs, in implementing name screening systems, adequately assess and test that the screening parameters applied are effective for generating name matches. FIs also regularly review these parameters to assess if they remain effective over time, and make adjustments where required.

FIs establish control processes over screening databases to regularly assess if:

- ✓ vendors' databases are adequate or should be supplemented with other relevant information sources.
- ✓ internal screening lists maintained are complete and accurate.

Areas done well

Structured controls over system parameters

FIs implemented structured controls over name screening system parameters to ensure that systems are fit for purpose, which include:

- Formalised frameworks and policies to govern name screening systems and parameter settings, including regular monitoring, back-testing, and tuning

- Periodic testing and reviews of:
  - Name screening thresholds and parameters
  - Accuracy and completeness of data flow from source systems containing customer information (e.g. customer names) to name screening systems
  - Reconciliation of the number of records processed by name screening system to the total number of records requiring screening, as a form of completeness check

- Engagement of third-party consultants to perform independent validation of screening systems' parameter settings to obtain assurance that they work as intended

C. Screening parameters and databases

Areas for improvement

Over-reliance on vendors

For setting system parameters

Some FIs did not adequately understand, evaluate, and regularly review the appropriateness of the parameters applied in their name screening systems for their business activities. Consequently, some of the parameters adopted were ineffective in identifying relevant name matches for assessment (refer to Case Study 2).

For ensuring adequacy of information sources

Most FIs did not enquire about the information sources used in vendors' screening databases. FIs also did not assess if vendors' information sources were adequate for their specific business activities, or should be supplemented with additional sources (e.g. by including additional names in FIs' internal lists[4]).

[4]Internal lists are maintained by FIs (separate from vendor screening databases), which typically include persons/entities of concern to the FIs that may not be reported in public sources.

Several FIs did not include certain information sources, relevant to ML/TF/PF-related matters, in their screening databases (e.g. persons and entities of concern in the United Nations Security Council (UNSC) reports). As vendors may not include these information sources in their databases, FIs may fail to identify potential risks from these sources (refer to Case Study 3).

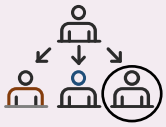
FIs should perform regular reviews of their screening parameters to assess whether they are effective in highlighting ML/TF/PF risks. Staff responsible for formulating policies on name screening should familiarise themselves with the screening parameters by undergoing regular training.

FIs should establish controls to regularly review the completeness of their screening databases.

C. Screening parameters and databases

Areas for improvement (cont.)

No fuzzy matching logic in screening tools



Some FIs' name screening tools, used for screening against internal lists, could only detect exact (i.e. 100%) name matches. Without screening tools with fuzzy matching logic (or appropriate system add-ins to implement partial-match capability), FIs would be impeded in identifying partial matches if there are minor name permutations, abbreviated names or typographical errors.

FIs should incorporate fuzzy logic matching capabilities to perform more effective name screening and minimise the risk of omission of true hits. In doing so, FIs should also assess that the fuzzy logic threshold is appropriately calibrated to generate relevant name matches.

No regular checks on internal lists

Some FIs did not conduct periodic checks to ensure that internal lists were properly maintained in their name screening systems, and contained adequate information sources to assess ML/TF/PF risks of customers (e.g. non-public seizure orders issued by law enforcement agencies in Singapore). Without periodic checks, FIs may be unable to ascertain if their internal lists are accurate and complete on an ongoing basis.

FIs should implement regular checks to ensure that their internal lists are up-to-date and remain accurate and complete.

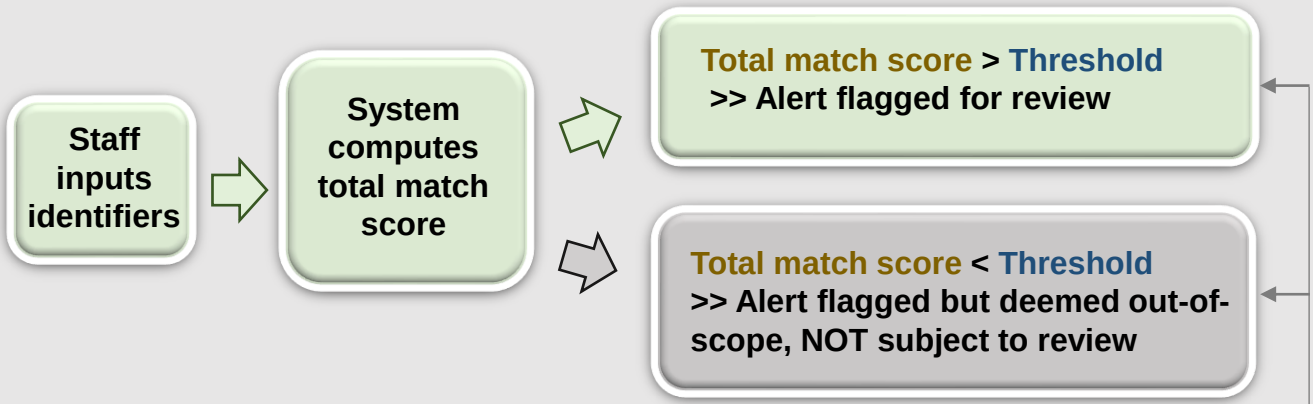
Case study 2 – Example of poor parameter setting

The calibration and settings of an FI's name screening system parameters are critical, as they affect how matches are identified (e.g. percentage of similar characteristics) and determine the alerts that are generated for review (e.g. criteria to trigger alerts).

It is important for FIs to actively understand how the parameter settings impact the generation of alerts, and calibrate them for their specific circumstances. The failure to do so could impede an FI's ability to identify customers with potential ML/TF/PF risks.

This case study illustrates how an FI uses a system to filter out false positives. However, due to inappropriately set parameters of its name screening system, exact name matches were inadvertently filtered out and not reviewed.

Overview of system generation of alerts for review[5]



Identifier	Identifier weightage (%)	Match score	Weighted match score (%)
Name	55	a	55a
Year of birth	25 or 0	b	25b
Country	20 or 0	c	20c
	Total match score =		**55a + 25b + 20c / Sum of weightages**

Screening database	Threshold
Sanctions	74%
PEP	80%
Adverse news	80%

Total match score vs Threshold

[5]The weightages, match scores, and thresholds stated are for illustrative purposes only. Refer to next page for explanation of key terms.

Case study 2 – Example of poor parameter setting (cont.)

Explanation of key terms

Total match score

- Weights are assigned to each identifier of the person/entity subjected to screening (e.g. name, country, year of birth (YOB)). If an identifier is not available in the alert, a 0% weight would be assigned to it, while keeping the weights for the remaining identifiers unchanged.
- The system calculates a match score for each identifier based on the degree of similarity of the information on the customer and in the alert (e.g. score of 1 for exact YOB match, score of 0.5 if YOB differs by 1 or 2 years, score of 0 if YOB differs by >2 years or if no information is available).
- The total match score (in %) is the sum of all weighted match scores divided by the sum of all the identifiers' weights.

Threshold for screening database

- Thresholds (in %) are set for each screening database to identify alerts for review. A lower threshold is set for the sanctions database relative to the PEP and adverse news databases.

Scenario

Name of Party A screened is an exact match of the name in the alert.
YOB of Party A is known to FI but not available in the alert.
Country of citizenship of Party A is known to FI. Only country of birth is in the alert. The countries do not match.

Total match score calculated by the system

	Identifier weightage (%)	Match score	Weighted match score (%)
Name - exact match	55	1	55
YOB - not available for alert name	0	0	0
Country - not match	20	0	0

Total match score = (55+0+0)/(55+0+20) = 0.733 or 73.3%

Resultant unintended consequence

Total match score (73.3%) is below thresholds for sanctions (74%), PEP (80%), and adverse news (80%) databases.

Under this scenario, **all alerts of exact name matches would be deemed out-of-scope and not reviewed by the FI**. This is contrary to the FI's intent to review all exact name matches.

FIs should understand and test the calibration of their systems' parameters to avoid inadvertently omitting alerts that FIs intend to highlight.

Case study 3 – Engaging vendors of screening systems

FIs commonly adopted vendor solutions to meet their name screening requirements. MAS noted that several FIs had over-relied on vendors to deploy their name screening systems. These FIs did not have a good understanding of how the systems worked, particularly in the following key areas:

1. System parameters
2. Sources of names with sanctions risks
3. Sources of adverse news
4. Management of sunset systems

This case study provides examples of how FIs should engage their vendors to avoid the common pitfalls in these four key areas. The case study also suggests possible ways to close residual control gaps in vendor solutions.

System parameters

Common pitfall

FI did not assess and regularly review if system parameters (e.g. fuzzy matching logic, assigned weights for identifiers) were effective in generating alerts as intended.

How to engage vendor

Clarify and assess:

- How system parameters, including thresholds used, affect the generation of alerts (these would differ across screening solutions, including different solutions by the same vendor)
- How to calibrate parameter settings for FIs' specific circumstances
- Whether additional controls are required to address any system limitations

Closing residual gaps

- Upgrade screening tools if vendor enhancements are available
- Supplement name screening processes (e.g. risk-based performance of additional internet searches)
- Consider additional or alternative name screening solutions

Sources of names with sanctions risks

Common pitfall

FI did not consider whether a vendor's screening database included names linked to sanctions risks from UNSC reports.

How to engage vendor

Enquire about the vendor's sources used for sanctions screening, including the UNSC reports, and assess if these sources should be supplemented.

Closing residual gaps

Supplement vendor's databases with FI's internal screening lists. For example, if vendor excludes names from UNSC reports, the FI implements processes to review UNSC reports to include relevant entities in internal screening databases.

Case study 3 – Engaging vendors of screening systems (cont.)

Sources of adverse news

Common pitfall

FI did not enquire about the news sources included in a vendor's screening database, and any criteria that the vendor may use to determine which types of adverse news would be incorporated.

How to engage vendor

Enquire about the vendor's coverage of adverse news:

- Sources – e.g. which major newspapers or relevant regional and local newspapers are included or excluded.
- Types – e.g. whether news on allegations or unconfirmed investigations/legal proceedings are included or excluded.

Assess if the vendor database's coverage of news sources and types are adequate to meet the needs of the FI's specific circumstances.

Closing residual gaps

Supplement vendor solutions with other adverse news screening processes (e.g. risk-based performance of additional internet searches).

Management of sunset systems

Common pitfall

FI was unaware that its name screening solution was a sunset system, and did not actively manage system limitations.

How to engage vendor

- Regularly check in with vendors to understand changes to system solutions, if any.
- Assess adequacy of vendor support and upgrades for sunset systems.

Closing residual gaps

Actively plan to migrate to newer solutions, particularly if vendor no longer provides adequate support to maintain and update sunset systems.

D. Alert resolution

Supervisory expectations

FIs perform robust and timely assessment of name screening alerts, and maintain adequate documentation of the assessment. FIs also implement effective independent checks and balances, such as maker-checker controls and regular independent QA reviews, for the assessment.

Areas done well

Detailed guidance on alert resolution

Some FIs established clear P&P for the resolution of alerts, which included detailed guidance and examples on criteria to assess, types of identifiers to consider, and documentation requirements (refer to Case Studies 1B and 4).

Areas for improvement

Inappropriate criteria used to determine relevance of news

- An FI would treat a piece of adverse news as out-of-scope, solely because it came from regional or local news sources (refer to Case Study 5A).
- An FI would determine if a piece of adverse news was relevant or out-of-scope based solely on its recency (refer to Case Study 5B)

In determining the relevance of adverse news, FIs should consider all key factors, such as the nature of adverse news and whether allegations are substantiated, instead of solely considering the sources or recency of the news.

Inadequate documentation of screening results and assessment

Some FIs did not establish clear documentation standards on name screening. This led to:

- missing records of screening results
- inadequate documentation of basis for alert dismissal

FIs should set clear requirements for staff to maintain adequate documentation of the assessment of alerts to demonstrate accountability and basis for alert resolution.

D. Alert resolution

Areas for improvement (cont.)

Insufficient basis for alert dismissal

Some FIs' P&P did not include adequate practical criteria for and guidance on the assessment and dismissal of alerts (e.g. types of identifiers to consider and their relative relevance as differentiating details). This led to alerts being dismissed without adequate basis. For example:

- Some FIs dismissed a group of alerts on a consolidated basis without addressing the specific unique information in each individual alert (refer to Case Study 5C).
- Some FIs dismissed alerts using generic explanations (e.g. "profile differs", "not same person") that were inadequate to justify the conclusion (refer to Case Study 5D).

FIs should provide detailed guidance on factors to consider when resolving name screening alerts, as well as requirements for staff to document justification for dismissing each alert.

Inadequate checks and balances

- A small number of FIs lacked maker-checker and/or QA controls to review if alerts were dismissed appropriately and in a timely manner. In some other FIs, the coverage of QA controls and frequency of reviews were insufficient to be meaningful.
- Such inadequacies in checks and balances could hinder the timely detection and remediation of any alerts that were wrongly dismissed (refer to Case Study 5D).

FIs should implement adequate checks and balances over alert resolution, such as regular QA checks by the second line of defence. This is to facilitate more timely detection and management of possible issues relating to the resolution of alerts.

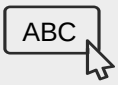
Case study 4 – Examples of guidance on alert dismissal

This case study provides some good examples of practical guidance for the assessment and dismissal of alerts, taken from the P&P of the FIs inspected. The examples are not exhaustive.

Guidance on assessing alerts for dismissal

Passport numbers

- Differences in passport numbers should not be used to dismiss alerts. Passports are renewed periodically and passport numbers are typically subject to change.



Variations in names

- Differences in names based on translation (e.g. Chen vs Tan) should not be used to dismiss alerts. Such variations pertain to the same root word.
- Differences in the spelling of names due to abbreviations (e.g. ABC Co. Ltd vs ABC Company Limited) should not be used to dismiss alerts.
- Differences in middle names alone should not be used to dismiss alerts.

C/O or a P.O. box addresses

- C/O or P.O. box addresses should not be used as identifiers to justify dismissal of alerts. Such addresses are neither permanent nor indicative of the parties' locations.

Other considerations

- Differences of one or two years in the year of birth alone (in the absence of information on the day and month of birth) should not be used to dismiss alerts. The year of birth recorded may only be an estimate.
- Differences in occupations alone should not be used to dismiss alerts. The relevant parties could hold multiple roles concurrently or change occupations over time.

Case study 5 – Examples of inappropriate alert resolution

Case 5A – Treatment of adverse news as out-of-scope solely because it comes from regional or local news sources

Are adverse news alerts subject to further review?		Categories of adverse news		
		Sanctions-related	Lawsuit	Other adverse information (e.g. regulator's investigation)
Sources of news	International news agencies	Yes	Yes	Yes
	News agencies where Head Office is located	Yes	Yes	Yes
	News agencies in region where FI is located[6]	Yes	Yes	No
	Local news agencies where FI is located	Yes	Yes	No

[6]Region where FI is located is different from that of Head Office.

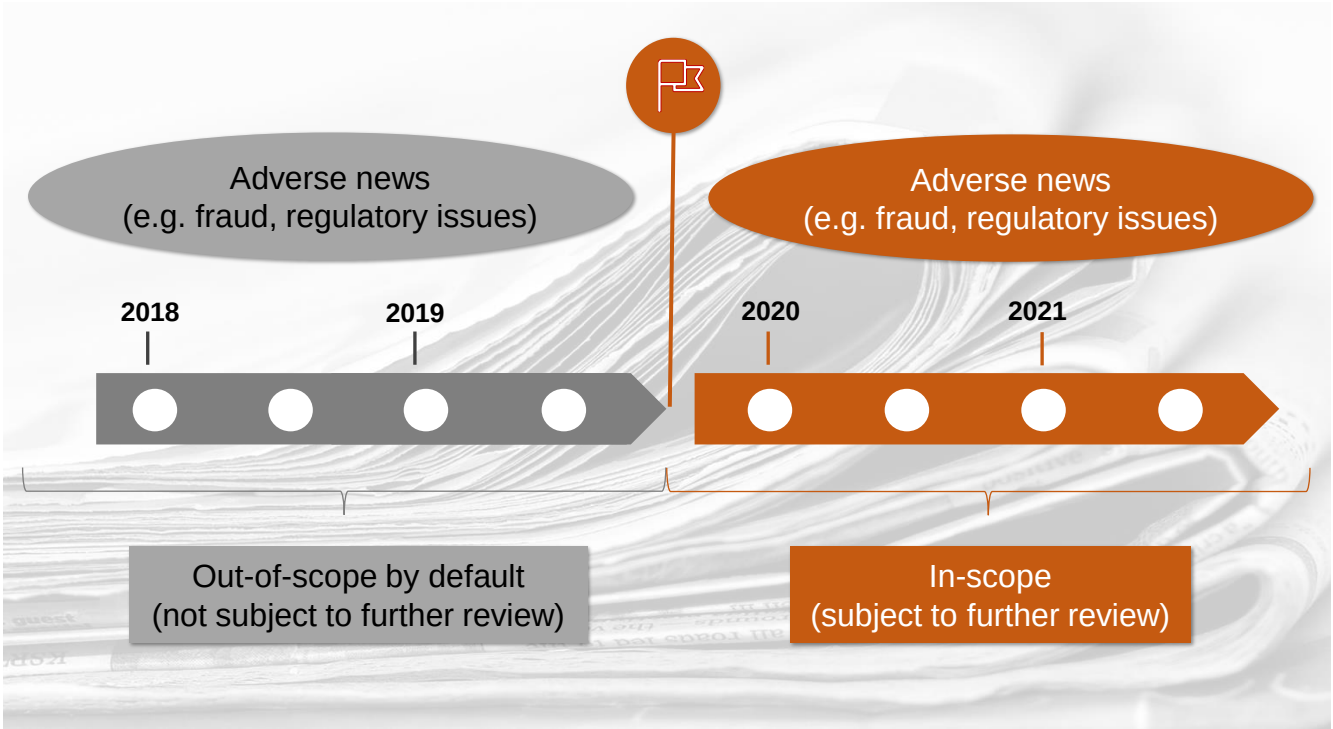
Why is this treatment inappropriate?

Information reported in regional or local newspapers would likely be relevant to an FI's regional and local customers.

By excluding adverse news from regional and local news sources, an FI may fail to detect information that may affect its assessment of potential ML/TF/PF risks associated with their customers.

Case study 5 – Examples of inappropriate alert resolution

Case 5B – Determining whether a piece of adverse news is relevant or out-of-scope based solely on its recency (e.g. news older than two years)[7]



[7]The years stated are for illustrative purposes only.

Why is this treatment inappropriate?

The nature and significance of a piece of past adverse news may continue to be relevant to an FI's assessment of the potential ML/TF/PF risks posed by a customer.

By only reviewing more recent adverse news, an FI may not have an accurate and complete view of the ML/TF/PF risks posed by a customer.

Case study 5 – Examples of inappropriate alert resolution

Case 5C – Dismissal of a group of alerts on a consolidated basis without addressing the specific unique information in each individual alert

Name screening result: 15 alerts with similar names	
Alerts	**Identifiers[8]**
Alert 1 - Charged with fraud	Resident of Country A, YOB 1960
Alert 2 - PEP	Born in Country B, YOB 1980
Alert 3 - Fined for false statement	Resident of Country C
….	….
Alert 14 - Bankruptcy proceeding	Citizen of Country D, YOB 1970
Alert 15 - PEP	Resident of Country A, YOB 1950

Consolidated justification by FI to dismiss all alerts:

"Able to dismiss all alerts as the countries of match results are different from our customer's. There was adverse news where person in alert was fined for false statement in [Country C] but our customer is from [Country A]."

[8]The identifiers stated are for illustrative purposes only.

Why is this treatment inappropriate?

The consolidated justification did not adequately address the specific unique information in each alert (e.g. "country" could refer to country of birth or citizenship, the individual may have dual citizenships, or there could be other identifiers which match).

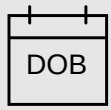
The justification documented also did not address all the alerts relating to Country A (i.e. Alert 1 and Alert 15).

The inadequate basis for dismissing alerts could be indicative of staff adopting a perfunctory approach towards assessing and closing alerts, and could impede the FI's ability to ascertain whether all alerts have been reviewed and appropriately closed.

Case study 5 – Examples of inappropriate alert resolution

Case 5D – MAS' observations of actual cases of alerts dismissed with generic explanations that were inadequate to justify the conclusion

1



Reason for dismissal: "Mismatch in date of birth (DOB) between the relevant party and the party in the alert."

Why inadequate: No DOB information included in the alert.

2

Reason for dismissal: "Alert is non-AML related."

Why inadequate: Nature of the adverse information classified as "corruption and bribery", which indicated potentially higher ML/TF risk.

3

Reasons for dismissal:

- Relationship manager and customer represented that the party in the alert is "not the same."
- "Profiles differ."
- "Profile does not match. Not related to alert."
- "Party is still a [relevant party] of customer and unlikely to be the same as alert name who was charged."
- "No ML/TF concerns."

Why inadequate: Lack of details to explain conclusion and no evidence of verification work done (e.g. to substantiate the representations of the relationship manager and customer).

Annex – Note to vendors of name screening solutions/ systems

This paper, highlighting MAS' supervisory expectations and key observations, is primarily targeted at FIs to improve their risk awareness and controls. However, some observations in the paper, particularly those on screening parameters and databases (Section C and the accompanying case studies), are similarly relevant to vendors of name screening solutions or systems.

Vendors play an important role in the ecosystem, as they develop and maintain solutions/systems to facilitate more efficient and effective screening checks by FIs. These solutions/systems are often equipped with proprietary capabilities, and some may be customisable for an FI's needs. Each screening solution/system has its own strengths and limitations.

MAS does not prescribe the use of any specific ML/TF/PF information sources and screening solutions/systems as the needs of FIs differ. FIs are expected to regularly assess the adequacy of the screening solutions/systems used, to ensure that they remain appropriate for the FIs' risk and business profiles.

A proper evaluation would require FIs to adequately understand the parameters used and their impact on the generation of alerts, as well as the strengths and limitations of the screening solutions/systems. This will allow FIs to identify any residual gaps and operational issues that could result from the use of a particular solution/system.

MAS recognises that the screening solutions/systems are based on proprietary information developed by the vendors. We encourage vendors to work closely with the FIs, to balance the FIs' need for information to effectively evaluate the screening systems/solutions, even as vendors protect the proprietary information of their solutions/systems.