Republic of the Philippines

ANTI-MONEY LAUNDERING COUNCIL

GUIDANCE ON SANCTIONS SCREENING

2022-2023 Thematic Review of the Effectiveness of Customer and Transaction Screening Systems of Covered Persons in Targeted Financial Sanctions Implementation

1. Introduction

1.1 Background

The Anti-Money Laundering Council (AMLC) applies a risk-based approach in performing its overarching role as the primary anti-money laundering/counter-terrorism financing (AML/CTF) supervisor and enforcer to ensure compliance of all covered persons, including designated non-financial businesses and professions (DNFBPs), with the Anti-Money Laundering Act of 2001, as amended; the Terrorism Financing Prevention and Suppression Act of 2012; their respective Implementing Rules and Regulations; and other issuances of the AMLC. This approach includes the conduct of risk-based supervision of targeted financial sanctions (TFS) on all covered persons.

The Philippines has been included in the Financial Action Task Force List of Jurisdictions under Increased Monitoring or the “grey list”, indicating that the country must improve its AML/CTF regime. Removal from such list requires accomplishing the country’s action plan within the prescribed timeline.

The said action plan includes enhancing the effectiveness of the TFS framework for terrorism financing (TF) and proliferation financing (PF) of weapons of mass destruction. Thus, the Philippines must, among others, demonstrate that covered persons understand their TFS obligations and that supervisors undertake risk-based supervision of TFS measures of financial institutions and DNFBPs.

1.2 Scope of Review

The AMLC selected covered persons to be tested in order to determine the effectiveness of their customer and transaction sanction screening systems in the implementation of TFS. The assessment was made against the testing of specific sanctions lists obligated under the Anti-Terrorism Act of 2020 and under UNSC resolutions (highlighted in section 1.4). The lists include individuals and entities that are sanctioned by the relevant regulatory bodies and accompanied by non-sanctioned records to assist in the measurement of efficiency of the customer and transaction screening systems.

The aim is to understand the effectiveness and efficiency of the primary client and transaction screening systems, with particular attention placed on four key considerations:

1. Does the system generate an alert when an ‘unmanipulated’ sanctioned name is screened?
2. Are the ‘fuzzy logic’ matching rules, configuration and threshold settings effective, such that a ‘manipulated’ sanctioned name generates an alert?
3. Are the levels of ‘false positives’ or ‘noise’ within operable/manageable levels?
4. Is the system performance in line with the regulator’s expectations?

1.3 What is Sanctions Screening?

Sanctions screening is a control employed within Covered Persons (CPs) to detect, prevent, and manage sanctions risk[1].

Most CPs conduct sanctions screening via two core systems: customer screening and transaction screening. Customer screening relates to the systems utilized to identify sanctioned individuals and entities at onboarding or throughout the client and/or supplier and/or relevant parties' relationship. Transaction screening relates to identifying the potential involvement of sanctioned individuals and entities within a transaction.

The process of name screening is typically enacted by organizations at onboarding, transaction, ongoing monitoring, or trigger-based events. Sanctions screening is undertaken through the usage of technology and sanctions data either through manual or automated systems and processes at singular name level or in batch format.

1.4 Current requirements under Philippine Law

The 2021 Sanctions Guidelines – Targeted Financial Sanctions related to Terrorism, Terrorism Financing and Proliferation Financing outlines the current requirements and obligations as set out by the AMLC.

Under current legislation, all CPs must screen all relevant parties against the Anti-Terrorism Council (ATC) List and United Nations (UN) Security Council Resolutions. The UN Security Council (UNSC) maintains a range of country-based financial sanctions that target specific individuals and entities connected with the political leadership of targeted countries. Each UN sanctions regime has a relevant Security Council Committee that maintains general guidance on the implementation of financial sanctions and current lists of targeted persons and entities.

At a minimum, the sanctions database should include the following and their successor resolutions:

(1) UNSC Consolidated List that includes UNSC Resolutions 1267/1989 (Al Qaeda), 1988 (Taliban), and 2253 (ISIL Daesh) for Targeted Financial Sanctions on terrorism and terrorist financing;

(2) UNSC Consolidated List that includes UNSC Resolution Numbers 1718 of 2006 (DPRK) and 2231 of 2015 (Iran) for TFS on Proliferation Financing.

(3) Domestic designations (or those that are designated by the Anti-Terrorism Council [ATC] pursuant to UNSC Resolution 1373, Section 25 of the Anti-Terrorism Act of 2020, Rule 15.b of the Implementing Rules and Regulations of The Terrorism Financing Prevention and Suppression Act of 2012 [TFPSA]) and those proscribed by the Court of Appeals under Section 26 of The Anti-Terrorism Act of 2020.

The UNSC Consolidated List and the updates thereto may be downloaded from the UNSC website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list). Moreover, locally designated individuals and organizations may be downloaded from the ATC website (https://atc.gov.ph).

[1] Wolfsberg Group 2019, Wolfsberg Sanctions Screening Guidance, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

1.5 Benchmark Data

As a reference point for system performance metrics, the tables below highlight the Customer & Transaction Screening Benchmark Data for the month of January 2023. The data indicated should act as reference for CPs regarding the effectiveness levels seen globally which the Philippines-based organizations should also be targeting.

Global Benchmark as of January 2023			
Client Onboarding		Transaction Screening	
Control	Manipulated	Control	Manipulated
96.27%	88.90%	95.70%	90.89%

2. Common Trends and Observations

The Thematic Review undertaken over the last twelve (12) months has identified several common trends and findings. Some of these are:

- Overall underperformance against most sanctions screening testing metrics versus global benchmark data.
- Significant weaknesses seen in the ability of CPs to identify manipulated names in their screening system and processes.
- Official mandated sanctions lists are not included in screening system configuration.
- Reliance on manual processes with limited automation across the sanctions screening process.
- Lack of understanding into how sanctions screening systems operate and potential risks they bring.
- Where there was no prior testing of sanctions screening systems, there was limited understanding of system configuration resulting in poor performance.
- Over reliance on manual systems and processes along with an over reliance on technology and data vendors.
- Average returns per hit (efficiency indicators) also remains relatively high in comparison to global standards. This shows system inefficiencies, generating significant numbers of false positives.
- Vendors have been tasked with managing financial institutions risk without financial institution understanding or awareness of system settings and impact thereof.
- In some instances where systems have been tuned, alerting levels are tuned to current resource capacity as opposed to being turned to risk appetite.
- Limited number of CPs have testing and auditing programs in place.
- New systems are not being tested before implementation.
- Screening systems are not generating alerts to potential matches to sanction names where systems have not been tuned in any way for more than a year.
- Senior Management are not being adequately briefed on sanctions risk and programs.
- In some instances, there was a misunderstanding between the differences of transaction screening and transaction monitoring by CPs and the usages of identifying risks through a combination of customer screening, transaction screening and transaction monitoring technologies.

Most screening tools use similar technology and work in the same way. The key to optimum effectiveness and efficiency is how it is being used. Normally when a screening system is not performing as expected, it is because of one, or a combination of these things:

- Poor configuration.
- It is being used with ‘out of the box’ or factory settings.
- The rules and settings have not been updated to suit the changing risk appetite of the institution.
- It is an old version of the vendor solution that has not been updated.
- Poor list management – too many sanction sources are being screened.
- The list provider is not fully up to date.
- Problems with the institutions’ list feed in keeping up with list providers updates.

Throughout the Thematic Review, we have identified that it is how a system is used by the Covered Person and not the actual system itself that provided outstanding results against their peers. The expectation is that the following document is reviewed by each CP and followed assessment, validation, and implementation of the elements highlighted.

3. Supervisory Expectations

Financial institutions can minimize their risk of non-compliance through the following:

- Ensuring that senior management is committed to promoting sanctions compliance.
- Undertaking ongoing sanctions-based risk assessments to assess the likelihood of dealing with an individual or entity on a sanctions list.
- Ensuring that all employees have been adequately trained to recognize any potential sanctions issues.
- Ensuring adequate policies and procedures are in place and approved by senior management.
- Appointing a responsible person with the appropriate skills and experience to deal with sanctions related issues and take ownership of the sanctions regime.
- Using technology as a tool to identify financial crime risk through real-time and ongoing screening methods.
- Ensuring that there are proper internal escalation processes in the event of an actual match.
- Conducting independent, ongoing, and regular screening tests to assess the effectiveness and efficiency of the systems.
- Conducting, testing, utilizing peer comparative data and tuning to improve configuration of sanctions screening systems to drive greater effectiveness and efficiency.
- Ensuring that appropriate supervision is in place in key client facing/money transmitting departments.

3.1 Senior Management Oversight & Commitment

3.1.1 Culture of compliance, tone from the top

Senior management includes the Board of Directors, C-Level executives, and departmental leaders.

Senior management should have a good understanding of sanctions screening processes, procedures, frameworks, and technology with the capability to act should sanctions risk arise. Senior Management should actively assess, review, and approve the organizations sanctions compliance program including policies, procedures, resourcing, data and technology practices. Senior management should own the sanctions regime, as they will be accountable in the event of non-compliance.

A clear whistle blower policy and culture of compliance that does not penalise active reporting of potential sanctions violations or misconduct and ensures senior management acts when misconduct or violations are identified.

3.1.2 Adequate resourcing

Senior management need not only provide oversight and maintain governance protocols, they should also ensure adequate resources are provided to the compliance function. Resources including suitable and proper staffing, technology, data, and training to ensure sanctions screening can be undertaken in an appropriate matter aligned to the organizations risk-based approach.

3.1.3 Management reporting

Reporting on all relevant elements of the sanctions screening program should be provided to senior management on a frequent basis in a risk-based manner. Frequency should be no less than quarterly to the Board of Directors. Reporting should include but not limited to the alignment to this policy document and focused on being able to identify, assess, and act on sanctions risk. Compliance leaders should have a direct reporting capability to Board Directors to escalate critical sanctions risk information generated from the sanctions screening process.

3.2 Risk Assessment

In February 2019, the Wolfsberg Group published guidance on sanctions screening.

They said that screening *"requires a programmatic approach through which each financial institution must assess its own risks in order to define the manner, extent and circumstances in which screening is employed."*[2]

That process is built around four core principles summarized as follows:

- *Articulate the specific sanctions risk the financial institution is trying to prevent or detect within its products, services, and operations.*
- *Identify and evaluate the inherent potential exposure to sanctions risk presented by the financial institution's products, services and customer relationships.*
- *A well-documented understanding of the risks and how they are managed through the set-up and calibration of the screening tool.*
- *Assess where, within the financial institution, the information is available in a format conducive to screening.*

Being able to effectively identify potential threats and vulnerabilities within the sanctions compliance context will enable organizations to enhance their programs. A regular, periodic risk assessment of the sanctions screening program and associated policies, procedures and frameworks will produce stronger compliance programs. Organizations should construct, if they do not have one in place, a risk assessment methodology based on its ability to identify risk, assess, and manage those risks.

3.2.1 Emergent risk typologies

Due to the evolution of crime and continued usage of evasive techniques undertaken by sanctioned individuals and entities, there is a need to constantly monitor new emergent risks as well as test against the new typologies on an ongoing basis. Organizations should be constantly monitoring guidelines and alerts published by competent supervisory authorities and international standards bodies as well as through continual training and skill advancements. They should be able to enhance system effectiveness through the updating of policy and system configurations to meet new and emergent risks posed by sanctioned individuals and entities.

3.3 Ownership, Skills & Training

3.3.1 Responsible persons

Responsible persons need to be accountable within the organization for the overall effectiveness of the sanctions screening program. Responsible persons should be adequately skilled with requisite experience and be provided with ongoing training. Responsible persons should be knowledgeable

[2] Wolfsberg Group 2019, Wolfsberg Sanctions Screening Guidance, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

across all elements of the sanctions screening process and be accountable to the areas in which they oversee.

3.3.2 Risk-based training program

Training of responsible persons and associated personnel needs to be undertaken in a risk-based manner that is ongoing, frequent and helps develop appropriate expertise across all components of the sanctions screening program. Training should be across all functions linked to the sanctions program and should include accessible resources for all stakeholders to continue to drive understanding of sanctions risks, driving greater execution.

3.4 Policies & Procedures

3.4.1 Documented methodology

All configurations of the sanctions screening program including processes, policies, procedures, frameworks and technology configurations need to be adequately documented. Documentation should be securely stored and reviewed on an ongoing basis with continued updates in line with improvement programs. Documentation should have ownership by Responsible Persons and be accessible, and understood, by Senior Management.

3.4.2 Processes & procedures

Clear and appropriate processes and procedures should be instituted and followed by all persons in the sanctions screening process as well as the wider organization. Clear processes need to be defined and ratified by senior management. Processes and procedures should be accurately documented and validated by Responsible Persons aligning to the risk-based approach of the organization.

3.4.3 Record keeping

In line with current obligations under Philippine Law, all risk relevant records need to be properly documented and securely stored in both physical and digital means depending on the nature of the document and aligned with the organization’s business practices.

3.5 Technology

3.5.1 Balancing effectiveness and efficiency

Financial institutions should first ensure that they have the correct AML/CFT technologies in place to detect financial crime indicators. This should include a robust sanction screening system which is set up to alert against names on globally important sanction lists and tuned to flag sanctioned names even when they have been altered using algorithms to assess the fuzzy logic matching capabilities of a screening system. Algorithmic manipulation will stress test a screening system and make it harder for a system to identify and alert against sanction records.

Sanction screening systems should be tested regularly to ensure that they are working as expected and that the number of false positives generated by the system are manageable and do not overwhelm available resources.

Sanction screening system testing will help a financial institution to understand a system's configuration whilst determining its weaknesses within pre-defined detection parameters. Testing and the ongoing monitoring of the screening system will facilitate improvement and enhancement of system performance through ongoing iterative tuning to optimize the efficiency and effectiveness of a sanctions screening system.

All AML/CFT technologies should be monitored on an ongoing basis to ensure that they remain correctly calibrated and that the number of false positives generated by the system remain at a manageable level.

A highly tuned AML/CFT system that is fit-for-purpose leads to relevant and valid alerts without the interference of excess system noise caused by numerous irrelevant false positives.

3.5.2 Manual & automated systems

Within the Thematic Review, many organizations were utilizing Manual screening systems including those of substantial scale and with potential risks and vulnerabilities to sanctions. The choice between implementation of Manual and Automated screening systems should be risk-based.

Where commercially available, or in-house systems developed, automated screening software is implemented, firms should understand its capabilities and limits, and make sure it is tailored to their business requirements, data requirements, and risk profile. Firms should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used, firms should be satisfied that they have adequate contingency arrangements should the software fail and should periodically check the software is working as they expect it to.

Automated screening systems provide batch screening system capabilities which enable more efficient screening due to delta screening capabilities, more effective use of data segmentation, ability to utilize secondary identifiers with greater effectiveness, and typically have far greater ability to customise configurations based upon risk.

Delta Screening is the process of screening customer accounts whenever a change occurs in either the customer accounts or the watchlists used in the screening process. This limits the unnecessary process of a full list of customers screened against the full list of sanction parties every day. After the full list of customers is screened against the full list of sanction parties once, then the full list of customers can be screened only against new sanction names thereafter. Then only new customers can be screened against the full list of sanction parties daily, without screening the full list of customers against the full list of sanction parties daily.

3.5.3 Exact matching & fuzzy logic

In some circumstances, in the name screening process, exact matching may be appropriate such as in the case of adverse media screening. However, in the instance of sanctions screening, the usage of fuzzy logic, or black box technologies powered by algorithms to detect manipulations of sanctioned individuals or entities names is required. This can be provided either by third party vendors or built in-house. In the Thematic Review, the AMLC identified a consistent underperformance of CPs' ability to match against manipulated names across the market and all forms of market segments. This underperformance is expected to be addressed by CPs in their own uplift programs.

3.5.4 Sanctions screening systems tuning

Tuning screening system parameters needs to be undertaken in an evidence-based manner to ensure configurations are aligned to the organization's risk-based approach. Configurability of the sanctions screening technology in place needs to be addressed at procurement and implementation stage to enable the ongoing tuning to risk. The ability to continually optimize the technologies and usage of data needs to be undertaken on a periodic basis. Tuning should be undertaken in line with Testing Frameworks highlighted in section 3.7.4 and should be targeted at the tuning stage for effectiveness and efficiency - reducing false positives whilst not sacrificing effectiveness levels. Tuning should be iterative with audit capabilities and reporting should be established to be escalated internally to stakeholders.

3.5.5 Over reliance on vendors

Technology third-party vendor reliance continues to be prevalent in organizations as they look to rely on the implementation and technologies prescribed by vendors without proper evaluation and assessment. Screening technology providers are heavily relied upon in the configuration of systems settings and rules without proper oversight from responsible persons which can lead to incorrect or erroneous system configurations. Covered Persons must understand that off-the-shelf solutions from vendors may not meet and combat all their potential risks in which customization and tuning would need to be undertaken after testing is completed.

3.5.6 Group-wide system management

If there is a group-wide screening policy, localization measures and controls need to be provided to local offices to meet local regulatory obligations.

3.6 Sanctions Data

3.6.1 List selection

Appropriate Lists are to be selected in accordance with regulatory agreements in place with other territories, exchange control agreements which enable trade relations, and any separate legislative prescriptions. Internal lists that prohibit relationships with certain parties can and should be included in screening configuration. Lists are updated by governments and other sanction sources daily. Sanctions lists include individuals, entities, vessels, aircrafts, banks that have been sanctioned and Dual Use Goods.

Commercial lists are available for procurement and are developed in the format required for screening system use. Commercial list providers retrieve list records from official published sources and provide consolidated list services to institutions in need. List providers are private companies and not the official source of sanction data. Thus, they carry the risk of not updating records immediately, making errors in spelling of names, and incorrectly classifying records. CPs should show that the selected sanctioned lists from the chosen commercial list vendor are comprehensive and efficient enough to detect all sanctioned parties and are updated with source updates. This can be done by comparing content and customer support of commercial list vendors.

United Nations Resolutions, as highlighted in the section 1.4 and Anti-Terrorism Council lists, are mandated to be included in the screening process under Philippine Law.

3.6.2 Segmentation

Segmentation is the process of segmenting lists within data sets to screen at appropriate configurations depending on the risk. Sanctions, Politically Exposed Persons (PEP), and Adverse Media data should be segmented in the screening process to ensure that a risk-based approach is implemented. Segmentation allows for the ability to tune to differing thresholds for screening based upon risk and enables the ability to tune for greater efficiency utilizing exact matching versus fuzzy logic as highlighted in section 2.5.3.

3.6.3 Whitelisting

Whitelisting/Good guy lists usage is the implementation of rules and configurations to automatically eliminate potential hits from screening. Whitelisting enables organizations to drive greater efficiency in screening practices.

3.7 Testing & Audit

3.7.1 Independent & objective

Testing of sanctions screening systems and validation should be independent of the compliance function and executed either by third parties or internal audit. The assessment and testing need to be objective and carried out by skilled practitioners with detailed metrics and analytics. Reporting should be provided to the organization that aligns with over-all effectiveness and efficiency goals set out by senior management. Testing should utilize dummy/synthetic data, fit-for-purpose, and Clean Identification for further efficiency testing. Testing is a mandatory requirement for all CPs to ensure they understand their TFS requirements and implementation of a program to identify any potential sanctions risks.

3.7.2 Frequent testing and validation

Testing of sanctions screening systems and the assessment and validation of sanctions screening processes and frameworks should be undertaken on a frequent and ongoing manner. Frequency should be risk-based, depending on the scale and risk assessment undertaken by the organization, but more than once per year at a minimum. Testing should be iterative and should utilize a consistent methodology with reporting to senior management of results on a regular basis with the overall effectiveness of the sanctions screening compliance program to be reported as defined in clause 2.1.3. Peer comparative data should be utilized in testing to ensure system performance is meeting industry benchmarks.

3.7.3 Pre & Post implementation testing

Thorough, rigorous, and robust testing at pre and post implementation of new or updated systems needs to be undertaken before systems go live to ensure relevant controls are in place to identify potential sanctioned individuals and entities. Testing should be undertaken on all parts of the technology with a clear audit trail of testing.

3.7.4 Testing frameworks

Testing frameworks should be defined within the organization's policy and utilized by Responsible Persons. Testing frameworks should be based upon evidence and documented tuning practices. Testing should enable CPs to understand system performance, diagnose deficiencies and weaknesses within the technologies or data, and allow for configuration support and a clearly documented methodology.

3.7.5 Ongoing supervisory testing and reporting

The AMLC requires CPs to provide ongoing testing results of their sanctions screening systems and program as well as continue to undertake the TFS Thematic Review of the effectiveness and efficiency of sanctions screening systems, selecting, and testing CPs in 2023 and beyond.

Glossary

Anti-Terrorism Council List – This is a list specified by the Anti-Terrorism Council (ATC) and can be found on the website, https://atc.gov.ph/. The Anti-terrorism Policy adopted by the Anti-Terrorism Council is "to protect life, liberty and property from acts of terrorism; to condemn terrorism as inimical and dangerous to the national security of the country and to the welfare of the people; and to make terrorism a crime against the Filipino people, against humanity, and against the law of the nations."

Not all terrorist groups designated by the ATC are automatically included in the UNSC Consolidated List. Individuals/entities are included in the UNSC List because they are known to have a connection with international sanctioned groups (e.g., Taliban, Al-Qaida). For example, the Abu Sayyaf and the Maute Group pledged their allegiance with Al-Qaida or ISIL, and because of those acts they can be included in the UNSC Sanctions lists under the UNSCR 1267.

The Security Council also noted that there are homegrown terrorist groups who are not affiliated with international sanctioned groups. Hence, there is no consolidated list for these types of groups that have no international connection. The purpose of Security Council Resolution 1373 on each country is to:

(i) have its own domestic designations especially if there are no outside connections and

(ii) allow other countries to designate domestic/local terrorists to prohibit obtaining support from abroad, and vice-versa.

Customer Screening – The process of checking if customers of the institution are listed on a sanction watchlist. This takes place upon account opening and daily as watchlists are updated daily.

Effectiveness - the degree to which the matching of sanction names is successful in producing a desired alert.

Efficiency – This is the measurement of the number of alerts that generate for analysts to review. It is an indication of the levels of staff needed to clear alerts generated by screening systems in identifying sanction risks.

Efficiency Score - in sanction testing, is the ratio or the average number of returns per alert.

Fuzzy Logic - Fuzzy matching relates to the rules used in screening solutions which allow for non-exact matches to be identified. The parameters of the systems need to be wide enough to detect slight differences in sanction names but not too wide so that there are large amounts of false positive alerts.

Targeted Financial Sanctions - means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

Transaction Screening – relates to identifying the potential involvement of sanctioned individuals and entities within a transaction in a domestic or international payment.

Transaction Monitoring – refers to the monitoring of customer transactions, including assessing historical/current customer information and interactions to provide a complete picture of customer activity. This can include transfers, deposits, and withdrawals. Transaction Monitoring holds an important place in AML compliance. Through the analysis of financial transactions, AML Transaction Monitoring is used to detect potential money laundering and illicit criminal activity.

Whitelisting - Instead of alerting on all names on sanction lists, whitelisting allows only specific names on sanction lists to not generate any alerts. This is usually done by creating a rule in the configuration of the system to not let any customer name generate a match against a name that is whitelisted in the aim of reducing false positives to names that hold no or low sanction risks.

United Nations Security Council Resolutions – Resolutions are formal expressions of the UN Security Council. The Resolutions are issued as individual documents. At a minimum, the sanctions database and system configuration should include the following UN Resolutions and their successor resolutions:

- UNSC Consolidated List that includes UNSC Resolutions 1267/1989 (Al Qaeda), 1988 (Taliban) and 2253 (ISIL Daesh) for Targeted Financial Sanctions on terrorism and terrorist financing;
- UNSC Consolidated List that includes UNSC Resolution Numbers 1718 of 2006 (DPRK) and 2231 of 2015 (Iran) for TFS on Proliferation Financing.