CENTRAL BANK OF THE BAHAMAS

GUIDANCE NOTES FOR SANCTION SCREENING

---

20 November, 2025

TABLE OF CONTENTS

INTRODUCTION

1. The Central Bank of The Bahamas ("the Central Bank") requires all Supervised Financial Institutions ("SFIs") to implement an appropriate sanctions screening framework. These Guidance Notes serve as a general guide regarding the Central Bank's minimum expectations for SFIs in establishing and maintaining an effective and adequate sanctions screening process.

2. Nothing herein prevents or limits the Central Bank from taking any course of action it deems necessary, to protect and strengthen the financial system in The Bahamas.

APPLICABILITY

3. These Guidance Notes apply to SFIs incorporated in The Bahamas and are to be applied proportionate to the nature and complexity of the SFI and inherent sanctions risks in their business activities.

SCOPE

4. These Guidance Notes were prepared by the Central Bank to assist SFIs in ensuring that their sanctions screening framework aligns with the Central Bank's expectations. It outlines the key elements that must be incorporated in SFIs' sanctions screening frameworks.

5. These Guidance Notes also reinforce the Central Bank's commitment to combating financial crime and incorporates international best practices based on, *FATF International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6);* and *the Wolfsberg Guidance on Sanctions Screening.* It should be read in conjunction with the *Central Bank's Guidelines for Supervised Financial Institutions on the Prevention of Money Laundering, Countering the Financing of Terrorism & Proliferation Financing ("AML/CFT/CPF Guidelines")*

PURPOSE

6. These Guidance Notes have been issued to raise awareness of the risks and vulnerabilities in regards to terrorism, terrorism financing (TF), proliferation and proliferation financing (PF), as well as the potential damage to The Bahamas if a regulated entity knowingly or unknowingly plays an appreciable role in TF or PF. The purpose of sanctions screening is to detect, prevent and manage sanctions risk as required by international obligations. It serves to drive improvements in financial crime risk management through identifying, assessing, and monitoring the sanctions risks faced by SFIs. Sanctions Screening is an essential component in a SFI's effective compliance program. The results of conducting sanctions screening can be used for various purposes including, but not limited to, the following:

i. To raise SFIs awareness of their domestic and international sanctions obligations;

ii. To eliminate threats to international security and peace in order to prevent, suppress and disrupt terrorism and proliferation of weapons of mass destruction and their financing;

iii. To identify gaps or opportunities for improvement in sanctions compliance policies, controls, and procedures; and allocation of resources;

iv. To support senior management in making informed risk-based decisions based on sanctions risk SFIs are exposed to;

v. To reduce SFIs' residual sanctions risk exposure through the development of risk mitigation methods;

vi. To aid senior management in tactical decisions related to reporting and escalation of designated individuals and entities;

vii. To aid the Central Bank in assessing the effectiveness of the SFI's sanctions screening controls; and

viii. To ensure regulators are informed of any probable sanction's risks, control gaps and remediation efforts across the SFI.

DEFINITIONS

7. For the purpose of these Guidance Notes:

"ATA" means Anti-Terrorism Act, 2018 (as amended).

"Attorney General" means Attorney General of The Bahamas.

"CDD" means Customer Due Diligence.

"Customer" means any of the following –

i. A person for whom a transaction or account is arranged, opened or undertaken;

ii. A signatory to a transaction or account;

iii. A person to whom an account or rights or obligations under a transaction have been assigned or transferred;

iv. A person who is authorised to conduct a transaction or control an account;

v. A person referred to in (i) to(iv) above; or

vi. Such other person as may be prescribed by the Minister[1].

[1] Minister –means Minister of Finance.

"Customer Screening" means the screening of full legal name and any other name provided by the customer, such as: known aliases against applicable official sanctions lists.

"Consolidated List" means the list maintained by the United Nations Security Council (UNSC) containing designated persons subject to financial sanctions (https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list)[2].

"Designated Person or Entity" means as defined in Section 2 of the Anti-Terrorism (Amendment) Act, 2019.[3]

"False Positive" means potential matches to listed persons and entities, either due to the common nature of the name or due to ambiguous identifying data, which on examination prove not to be matches[4].

"FIU" means Financial Intelligence Unit established pursuant to Section 3 of the Financial Intelligence Unit Act, 2023.

"FTRA" means Financial Transactions Reporting Act, 2018.

"Fuzzy Matching" means a varied and algorithm-based technique to match one name (a string of words), where the contents of the information being screened is not identical, but its spelling, pattern or sound, is a close match to the contents contained on a list used for screening[5].

"Group of Financial Services Regulators" ("the GFSR") means the Regulatory Bodies which comprises of the Central Bank of The Bahamas, Securities Commission of The Bahamas, Insurance Commission of The Bahamas, Compliance Commission of The Bahamas, and Gaming Board for The Bahamas.

"Inherent risk" means the level of risk that exists within the operating environment before any controls or mitigation measures are implemented to reduce the likelihood or impact of the risk.

"Internal Controls" means a process, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

"IOEAMA" means International Obligations (Economic and Ancillary Measures) Act 1993 (as amended).

[2] See also the United States Office of Foreign Assets Control (US OFAC) List; European Union (EU) Sanctions List; the United Kingdom Office of Financial Sanctions Implementation (UK OFSI) List.
[3] See Section 2 of the Anti-Terrorism (Amendment) Act, 2019.
[4] FATF International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6). See also as defined in Regulation 2 of the Anti-Terrorism Regulations, 2019.
[5] Wolfsberg Guidance on Sanctions Screening.pdf.

"IOEMA Orders" means the International Obligations (Economic and Ancillary Measures) (Iraq) (Order), 2018; and International Obligations (Economic and Ancillary Measures) (Afghanistan) (Order), 2018; International Obligations (Economic and Ancillary Measures) (Democratic People's Republic of Korea) (Order), 2019 and International Obligations (Economic and Ancillary Measures) (Iran) Order, 2019;[6].

"KYC" means Know Your Customer.

"National Identified Risk Framework Coordinator" means the person nominated as the National Identified Risk Framework Coordinator[7].

"Proliferation" means the development, production, spread, distribution, stockpile, retention or transfer of weapons of mass destruction[8].

"Proliferation Financing (offence)" means the underlying financial services which make proliferation possible. It is the financing of proliferation activities[9].

"Residual Risk" means the level of risk that remains after controls or mitigation measures have been applied to address the inherent risk.

"Risk" means the possibility that an event of a given impact will occur, adversely affecting the achievement of objectives.

"Risk assessment" means the combined effort of identifying and analysing potential events that may negatively impact individuals, assets, and/or the environment.

"Sanctions screening" means a control used in the detection, prevention and disruption of financial crime and, in particular sanctions risk[10].

"Supervised Financial Institution" or **"SFI"** means all institutions licenced, registered, and regulated by the Central Bank. This includes, but is not limited to, licenced banks, banks and trust companies, and co-operative credit unions.

"STR" means Suspicious Transaction Report.

[6] International Obligations (Economic and Ancillary Measures) (Afghanistan) (Order), 2018 – (S.I. No. 56 of 2018) ('the Afghanistan Order"); International Obligations (Economic and Ancillary Measures) (Iraq) Order, 2018 – (S.I. No. 57 of 2018) ("the Iraq Order"); International Obligations (Economic and Ancillary Measures) (Iran) Order, 2019 – (S.I. No. 36 of 2019) ("the Iran Order"); International Obligations (Economic and Ancillary Measures) (Democratic People's Republic of Korea) Order, 2019 – (S.I. No. 23 of 2019) "the DPRK Order").

[7] As defined in Section 2 of the Anti-Terrorism Act, 2018. See also as defined in Section 5 of the Proceeds of Crime Act, 2018.

[8] As defined in Section 2 of the Anti-Terrorism (Amendment) Act, 2019. See also Guidance Note on Proliferation and Proliferation Financing, 2018.

[9] As defined in Section 9 of the Anti-Terrorism Act, 2018. See also Guidance Note on Proliferation and Proliferation Financing, 2018.

[10] Wolfsberg Guidance on Sanctions Screening.pdf

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"[11].

"Terrorist" means as defined in Section 2 of the Anti-Terrorism Act, 2018[12].

"Terrorism" means as defined in Section 14 of the Anti-Terrorism Act, 2018.

"Terrorist Financing (offence)" means as defined in Section 15 of the Anti-Terrorism Act, 2018.

"Transaction Screening" means the process of screening a movement of value within the SFI's records, including funds, goods or assets, between parties or accounts.

"True Match" means a screening result, where the characters contained with the information being screened match the details of a designated entity on a list that is in scope for screening.

"Without delay" means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee[13].

"United Nations Security Council" means the Security Council established under the charter of the United Nations[14].

LEGAL FRAMEWORK

8. The Bahamas is committed to combating financial crime pursuant to section 44(1) of the Anti-Terrorism Act, 2018 (as amended), and section 49(3) of the Anti-Terrorism Act, 2018 (as amended).

9. SFIs are required to adhere to the requirements outlined in the International Obligations (Economic and Ancillary Measures) (Amendment) Act, 2019 (Ch.16), specifically sections 3A and 3B[15].

10. To ensure compliance with The Bahamas' Sanctions Regime, SFIs are required to review the relevant provisions of the IOEAMA, together with each Notice issued by the Central Bank, in accordance with section 3A of the IOEAMA and each Order issued by the Attorney General, in accordance with section 3B of the IOEAMA, along with any updates, modifications or associated lists.

[11] FATF International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)
[12] See also as defined in Section 2 of the Proceeds of Crime Act, 2018.
[13] FATF International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)
[14] As defined in Regulation 2 of the Anti-Terrorism Regulations, 2019. See also as defined under "Security Council" in Anti-Terrorism Act, 2018. See also as defined in the International Obligations (Economic and Ancillary Measures) (Amendment) Act, 2019
[15] See the International Obligations (Economic and Ancillary Measures) (Amendment) Act, 2019

11. SFIs are encouraged to seek legal advice to ensure they meet their sanctions compliance obligations relevant to their business activities.

COMPLIANCE FRAMEWORK

12. SFIs should implement a robust sanctions screening compliance program with clear internal controls, policies and procedures to mitigate exposure to designated individuals or entities. The Board is responsible for regularly assessing, reviewing and approving the SFI's sanctions compliance program.

13. Sanctions screening is reliant on various factors including the type of inherent sanctions risk to which the SFI, its clients and products and/or services are exposed.

14. SFIs should adopt a risk-based approach when assessing their inherent sanctions risk to determine the scope, manner, and conditions in which screening measures take place.

15. When determining their inherent sanctions risks and defining its policies and procedures, SFIs should consider the following factors:

i. The type of products and services the SFI offers and whether or not those products and services correspond to a heightened sanctions risk;

ii. Its geographical, historical, and cultural proximity to sanctioned countries;

iii. Customers' location and the type of business activities they engage in; and

iv. The volume and frequency of transactions and its distribution channels.

16. SFIs should note that sanctions screening measures should be applied with other control elements including, but not limited to:

i. Asset or Funds freezing procedures;

ii. Asset market restrictions or investment prohibition procedures;

iii. Proper KYC and CDD procedures; and

iv. Adequate sanctions-related employee training program.

17. SFIs should ensure, at a minimum, that their sanctions screening compliance program includes the following compulsory aspects:

i. Risk Assessment;

ii. Appropriate policies and procedures;

iii. Internal Controls;

iv. Educated and experienced employees; and

v. Adequate testing.

Governance and Accountability

18. The Board and senior management are ultimately accountable for the effective oversight and implementation of the sanction's compliance program. The SFI must designate a qualified Compliance Officer or Money Laundering Reporting Officer, responsible for sanctions compliance, who has appropriate authority, resources, and independence to perform their duties.

19. The Compliance Officer or Money Laundering Reporting Officer is responsible for:

i. Ensuring adherence to all sanctions screening policies and procedures;

ii. Overseeing staff training and awareness;

iii. Reporting suspicious matches or activity to the Financial Intelligence Unit (FIU), the Attorney General (AG) and the Central Bank; and

iv. Liaising with regulators and law enforcement as required.

Risk Assessment

20. SFIs should conduct a routine risk assessment to identify potential sanctions risk that the SFI may be exposed to. After identifying and assessing its inherent sanctions risk, the SFI must also evaluate its residual sanctions risk. Risk-based decisions should be used to address elements in the SFI's sanctions compliance program which include, but is not limited to:

i. which sanctions list(s) should be used;

ii. what data elements to screen;

iii. when screening should occur;

iv. when there are updates to sanctions lists;

v. the frequency of an ongoing screening, commensurate with the institutions risk exposure;

vi. the level of fuzziness used when tuning systems; and

vii. the required level of automation and sophistication for the screening system.

21. Based on their sanctions risk assessment, SFIs should determine, implement, and document sanctions screening controls that are appropriate to manage their specific risk exposure. Among other elements, the following should be assessed, justified, and documented:

i. the frequency and triggers for sanctions screening (e.g., real-time, daily, batch-based, periodic);

ii. the selection and use of appropriate sanctions lists;

iii. the categories of data to be screened (e.g., customer, transaction, counterparty;

iv. the level of system automation; and

v. the regularity and procedures for testing and validating the effectiveness of the screening system.

22. The Board and senior management must clearly define and document the sanctions screening decision making process and governance structure. This should be supported by metrics, periodic effectiveness reviews, and ongoing analysis and testing of the sanctions screening controls and system configuration.

Appropriate Policies and Procedures

23. The Board must define clear screening requirements and ensure that the SFI's sanctions compliance policies and procedures are applied. SFIs are expected to determine and document their sanctions screening policies and procedures based on inherent and residual sanctions risks, approved by the Board.

24. SFIs should review, test and enhance their sanctions compliance policies and procedures on an ongoing basis, especially when vulnerabilities have been identified or sanctions screening industry best practices have been updated.

Internal Controls

25. SFIs are required to implement internal controls to detect, escalate, report, and document prohibited activity, when applicable, regarding sanctions screening obligations and compliance.

26. SFIs should document screening software configuration to assess its effectiveness in detecting and managing the SFIs' sanctions risk. Software limitations and vulnerabilities should be transparent and should be decided on by the Board using a risk-based approach.

Education and Experience

27. SFIs should ensure that responsible persons are educated and experienced on sanctions obligations regarding The Bahamas' sanctions legal framework and screening software used. SFIs are responsible for enforcing ongoing sanctions compliance employee training programs to update responsible persons on any amendments or enhancements to sanctions compliance obligations and industry best practices.

Testing

28. SFIs should assess the effectiveness of their screening software, systems and other technology at minimum, annually, to validate that the screening system is performing as expected. Additionally, SFIs should validate screening systems after the implementation of any new enhancements or changes in outsourced vendors. Ongoing testing of screening systems should be validated by metrics, analysis and reporting.

SANCTIONS LIST

29. Management of the sanctions lists is essential for SFIs to meet legal obligations, particularly the requirement to screen against the mandatory United Nations Security Council (UNSC) Consolidated list. In addition to this, SFIs are encouraged to adopt a risk-based approach by considering other key sanctions lists as a matter of best practices. These may include, but are not limited to:

- United States Office of Foreign Assets Control (US OFAC) List;
- European Union (EU) Sanctions List; and
- United Kingdom Office of Financial Sanctions Implementation (UK OFSI) List.

30. SFIs should ensure they screen against all sanctions lists relevant to their business operations and risk exposure.

31. SFIs should regularly update their internal lists based on notifications from the Central Bank and other reliable sources to ensure screening against the most current data.

INDEPENDENT REVIEW AND PROGRAM EFFECTIVENESS MONITORING

32. To ensure the ongoing effectiveness and adequacy of sanctions compliance programs, the three lines of defence strategy should be employed.

33. SFIs are required to perform periodic independent reviews, which should be conducted by Internal Audit. If not performed by Internal Audit, periodic independent reviews may be conducted by a qualified outsourced vendor. SFIs may also conduct third-party assessments, or other independent evaluations.

34. Such periodic reviews should include, but are not limited to, an evaluation of the following:

i. The accuracy and efficiency of sanctions screening tools, including false positive and false negative rates;

ii. Compliance with regulatory requirements for sanctions screening, reporting, and asset freezing;

iii. Adequacy of policies, procedures, and controls relating to sanctions compliance;

iv. Screening against the latest UNSC Consolidated list during the review period;

v. Effectiveness of staff training programs and awareness initiatives;

vi. Timeliness and completeness of reporting to regulators; and

vii. Appropriateness of escalation and false positive management procedures.

35. Results of independent reviews must be reported to senior management and the Board of Directors, with documented action plans to address any identified deficiencies or weaknesses.

SCREENING OBLIGATIONS

36. SFIs are required to screen their entity for any individual, products or business that is considered a target. The most common types of sanctions screening methods consist of customer screening and transaction screening.

Customer Screening

37. SFIs are required to implement effective customer screening measures that validate key demographic information, including, but not limited to, the customer's legal name, date of birth, and nationality or place of incorporation (including any associated business operations). Screening must be conducted as part of the SFI's KYC and CDD obligations and must occur at onboarding and on an ongoing basis, in accordance with the SFI's risk profile and applicable legal requirements.

38. Customer screening is a critical control for the detection and prevention of financial crime and must be proportionate to the nature, size, and complexity of the business relationship.

Screening of Connected Individuals and Entities

39. SFIs are required to screen all relevant individuals and entities connected to the customer relationship. At a minimum, this includes:

i. Beneficial owners, trustees, authorised signatories, directors and officers;

ii. Individuals granted authority through power of attorney or equivalent legal arrangements; and

iii. Jurisdiction linked to the customer or connected parties, including country of residence, incorporation, or any jurisdiction where the customer conducts substantial business or financial activity.

40. SFIs must assess any **geographical risk**, particularly where connections exist to jurisdictions subject to **UN Security Council sanctions**, **FATF high-risk or under increased monitoring lists**, or otherwise designated by competent authorities. Where

such risks are identified, SFIs must apply enhanced due diligence measures, as appropriate.

Transaction Screening

41. SFIs should screen transactions during the end-to-end transaction process to identify and block any possible transactions involving designated individuals or entities to avoid potential violations.

42. SFIs should consider the scope and frequency of transaction screening against its sanctions screening policies and procedures considering factors such as:

i. the cross-border nature of transactions;

ii. the type of currency;

iii. the route of the transaction;

iv. the bank name and bank and routing codes;

v. the trade finance documentation; and

vi. the International Securities Identification Number (ISINs) or other related product identifiers.

43. SFIs should ensure that list maintenance is performed when sanctions notices are sent by the Central Bank. SFIs should outline a clear process of adding to or removing from the designated individuals/entities internal list to ensure it adheres to sanctions compliance obligations, reducing the risk of potential violations.

SCREENING TOOLS

44. SFIs have the right to select any screening software option, whether manual screening (where the names are entered and reviewed individually) or automated screening using commercially available or internally developed software.

45. In deciding screening software, SFIs should determine whether manual screening or automated screening is best suited based on the complexity, nature, and size of the operations, including the characteristics of their client base and business activities. SFIs conducting manual screening should ensure that safeguards are in place to mitigate human errors. Larger or more complex SFIs should implement an appropriate automated software that flags probable findings of designated individuals or entities in a clear and effective manner.

Automated Screening Software

46. When using automated screening software, SFIs should ensure that systems used:

i. are able to apply the SFI's risk-based screening procedures and adhere to its specific policies;

ii. are able to screen against consolidated sanctions lists;

iii. are able to adequately and clearly signal probable matches through alert creation;

iv. incorporates 'fuzzy matching' proficiencies; and

v. uphold data integrity and presents applicable metrics and reporting.

47. SFIs should properly assess sanctions screening software effectiveness if software is outsourced externally, ensuring that sanctions compliance obligations are met in accordance with The Bahamas' sanctions regime. Sanctions screening must be conducted against the UNSC Consolidated List.

48. SFIs should ensure that sanctions screening systems uphold customer data protection in accordance with the Data Protection (Privacy of Personal Information) Act, 2003. When using fuzzy matching systems, SFIs should ensure that systems are tuned to an appropriate level of fuzziness that efficiently flags all probable matches but minimises frequent false positive alerts. Proper tuning of fuzzy matching tools is an essential element, as it helps to identify probable matches where information is missing in the SFI's database when screening against the UNSC Consolidated list, US/OFAC Sanctions List, or EU Sanctions List.

49. When screening for designated individuals or entities, SFIs should distinguish and document true matches from false positives. Demographic details, including an individual's name paired with their date of birth, can help distinguish accurate matches from potential false positives.

50. SFIs are encouraged to utilise a whitelist to manage individuals that have already been confirmed as false positives and the rationale that was determined by senior management or other authorised persons that explains why an individual or entity was placed on the whitelist.

51. SFIs that utilise automated screening software should test such software before implementation. Additionally, testing should be carried out on an ongoing basis to assess the effectiveness of the systems' ability to manage the SFI's inherent sanctions risks and to address any vulnerabilities captured.

52. SFIs should ensure that testing of screening software is clearly and adequately documented. SFIs should ensure that a clear audit trail including metrics, analysis and reporting is produced on testing results before and after software implementation.

Third-Party and Vendor Management

53. SFIs that outsource sanctions screening or other compliance functions to third parties must maintain effective oversight over such arrangements.

54. Outsourcing agreements should clearly define the following:

i. Compliance obligations regarding sanctions screening;

ii. Responsibilities for metrics reporting and escalation; and

iii. Data protection and confidentiality requirements.

55. SFIs remain fully responsible for ensuring third-party compliance with The Bahamas' sanctions regime.

TRAINING AND AWARENESS

56. SFIs should ensure that proper training on sanctions compliance and international obligations are undertaken by responsible persons in line with The Bahamas' Sanctions legal framework.

57. SFIs should ensure that sanctions screening for employee training is provided under a structure and frequency that is appropriate and in line with its risk profile and risk assessment. SFIs should tailor training to specific employee roles and communicate clear sanctions compliance responsibilities to each employee. Employees of SFIs should be held responsible for sanction compliance through training assessments.

58. SFIs' sanction-related employee training programs are required at a minimum to include its policies and procedures for:

i. Compliance with new sanctions implemented by the UNSC or Attorney General;

ii. Screening for designated individuals or entities;

iii. Reporting any true matches to the FIU and Central Bank;

iv. Terminating compliance with sanctions that have been withdrawn by the UNSC or Governor General;

v. Documenting compliance procedures taken in accordance with The Bahamas' sanctions legal framework and basis for such procedures; and

vi. Documenting and communicating any amendments to SFI's sanctions screening policies and procedures.

59. Sanction-related employee training programs should be ongoing at least annually, ensuring that responsible persons are adequately informed and updated on changes in sanctions screening obligations and industry best practices. Sanctions screening employee training should be documented to ensure requirements are met and to detect any shortcomings or limitations.

AUDITABILITY, RECORD KEEPING, AND DOCUMENTATION

60. SFIs must maintain comprehensive and accurate records of all sanctions screening activities for a minimum of five (5) years to ensure transparency, accountability, and regulatory compliance. These records should be easily retrievable and must include, but are not limited to:

i. Documentation of all matches and investigations conducted, including the classification of true matches versus false positives;

ii. Configuration settings and tuning parameters of sanctions screening systems;

iii. Results of system testing, validation, and any subsequent adjustments;

iv. Documentation of reporting to the Financial Intelligence Unit (FIU), the Attorney General and the Central Bank, including dates, content, and confirmations; and

v. Records of internal communications, escalation procedures, and management approvals related to sanctions screening.

61. All records must be retained for a minimum period as prescribed by law or regulatory requirements and must be readily accessible for review by supervisory authorities during examinations or audits.

ESCALATION PROCEDURE

62. SFIs, when screening for sanctioned individuals or entities, should distinguish and document true matches from false positives. Demographic details, including an individual's name paired with their date of birth, can aid in distinguishing accurate matches from potential false positives.

63. Upon identification of a potential match to a targeted individual or entity, SFIs must promptly conduct an internal review to determine the validity of the match.

64. Where the match is considered plausible then, at a minimum, the following should occur:

i. The Compliance Officer should escalate the matter to senior management;

ii. Full documentation of all findings and investigative steps should be maintained; and

iii. Only after internal validation should a positive match be reported to the FIU, the Attorney General and the Central Bank using the applicable Suspicious Transaction Report (STR) and Targeted Sanctions Reporting Form.

65. Timely escalation and clear documentation help to ensure appropriate and consistent reporting.

REPORTING OBLIGATIONS

66. In an effort to further improve industry practice, the Central Bank, in conjunction with the Group of Financial Services Regulators, in its collective efforts of harmonising practices that lead to better coordinated supervision and improvement of regulatory reporting, released joint Targeted Financial Sanctions Reporting Forms and accompanying Guidance Notes for licensees and registrants deemed 'financial institutions' pursuant to section 3(1) of the Financial Transactions Reporting Act ("FTRA") and regulated and/or supervised by any one or more GFSR member(s). The Forms comprise of the following: FORM A - Targeted Financial Sanctions Reporting Form, FORM B - Targeted Financial Sanctions Quarterly Reporting Form, FORM C - International Obligations (Economic and Ancillary Measures) 2018 Orders (IOEMA) Annual Declaration and FORM D - International Obligations (Economic and Ancillary Measures) 2019 Orders (IOEMA) Annual Declaration.[16]

67. SFIs are required to report only positive matches found after screening for designated individuals or entities to the Attorney General, FIU and the Central Bank without delay[17].

68. SFIs should ensure that reporting procedures and internal controls are clearly defined and carried out in a timely manner. Senior management should enforce an appropriate and clear culture of reporting regarding sanctions screening compliance.

69. Prior to reporting a designated individual or entity to the Attorney General, FIU and the Central Bank, SFIs that identify any designated individual or entity in their system must freeze any assets or funds held without delay. SFIs must also freeze any assets or funds held by entities that are owned or controlled[18] directly or indirectly by a designated individual without delay. SFIs should ensure that any transactions instructed or carried out by a designated individual or entity, following action to freeze assets or funds are prohibited.

70. Pursuant to the FTRA, when detecting or suspecting any designated individuals or entities, SFIs are required to report findings to the Attorney General, FIU and the Central Bank without delay. The process of reporting should, at a minimum, comprise of:

i. Written evidence, including Customer Due Diligence (CDD) information, transaction detail and the volume of assets owned, must be thoroughly documented prior to reporting any positive matches of designated individuals or entities; and

ii. Comprehensive evidence gathered and the applicable STR and Form A - Targeted Sanctions Reporting Form should be sent to the Attorney General, FIU and the Central Bank.

[16] GFSR GUIDANCE NOTES ON TARGETED FINANCIAL SANCTIONS REPORTING FORMS

[17] Pursuant to Anti-Terrorism Act, 2018 (as amended)

[18] Pursuant to the Financial Transactions Reporting Act, 2018

71. SFIs should provide full cooperation in any investigation conducted by the FIU, where necessary.

NON-COMPLIANCE PENALITIES

72. Financial Institutions identified as having failed to screen their systems in accordance with sanctions notices issued during the quarter, will be subject to penalties.

73. Financial Institutions that do not comply with the reporting requirements pursuant to section 44(1) of the Anti-Terrorism Act, 2018 (as amended), commits an offence and are liable on summary conviction to a fine not exceeding two hundred and fifty thousand dollars ($250,000), pursuant to section 49(3) of the Anti-Terrorism Act, 2018 (as amended).

74. SFIs risk potential violation as soon as a designated individual or entity has been added to the UNSC Consolidated List, US/OFAC Sanctions List, or EU Sanctions List. It is imperative that SFIs immediately screen their systems for any designated individuals or entities when instructed by the Central Bank to avoid penalties or reputational damage.

75. SFIs are strictly prohibited from offering any products or services to any designated individual or entity. SFIs proven guilty of an offence regarding sanctions obligations are liable to be proceeded against and punished accordingly in line with IOEAMA and ATA.

76. SFIs found guilty of failing to screen their systems in accordance with sanctions notices issued by the Central Bank and the Attorney General, will be subject to penalties. Any employee of an SFI identified as failing to adhere to sanctions obligations is liable to be penalised accordingly along with the SFI.