CENTRAL BANK of BELIZE

GUIDANCE NOTES

IMPLEMENTING TARGETED FINANCIAL SANCTIONS FOR CENTRAL BANK-REGULATED INSTITUTIONS

COMPLIANCE DEPARTMENT
GABOUREL LANE
BELIZE CITY
BELIZE

DECEMBER 2023

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AML/CFT/CPF	-	Anti-Money Laundering/Combating the Financing of Terrorism and Combating Proliferation Financing
CDD	-	Customer Due Diligence
Central Bank	-	Central Bank of Belize
Consolidated List	-	The Belize Consolidated Sanctions List
EU	-	European Union
FIU	-	Financial Intelligence Unit
MLTPA	-	Money Laundering and Terrorism (Prevention) Act
STR	-	Suspicious Transaction Report
The UN List	-	The United Nations Security Council Consolidated List
UK	-	United Kingdom
UN	-	United Nations

SECTION I - INTERNATIONAL SANCTIONS

1. The obligations of financial institutions with respect to international sanctions are set forth primarily in sections 12 and 68 of the Money Laundering & Terrorism (Prevention) Act (MLTPA). Notices of the Director of the Financial Intelligence Unit (FIU) under section12 of the MLTPA or Orders of the High Court under section 68 of the MLTPA have the effect of ordering the freezing the funds or assets of Listed Persons and prohibiting providing them with financial or other related services.

2. Financial institutions should make their sanctions compliance programme an integral part of their anti-money laundering/combating the financing of terrorism/combating proliferation financing (AML/CFT/CPF) compliance programme, subject to several key differences described in this Guidance Notes.

3. The guidance provided in this Guidance Notes is not exhaustive. Although this guidance focuses on financial sanctions and asset freezes, financial institutions must also be aware of the nature and requirements of other types of sanctions measures. It is the responsibility of each entity to put in place policies, procedures and controls that ensure compliance with the sanctions regime.

4. Financial sanctions are enforcement measures the international community uses to achieve, maintain, or restore international peace and security in a specified regime. Financial sanctions are imposed on an entity, regime, or natural person within a regime by the United Nations (UN), European Union (EU), or United Kingdom (UK) as a tool to comply with certain foreign policy or national security objectives. The effect of sanctions is to:

- **i.** Limit the provision of certain financial services; and
- **ii.** Restrict access to financial markets, funds, goods, services and economic resources.

5. Financial sanctions are largely imposed to:

- **i.** Coerce a regime or natural persons into changing their behaviour, or aspects of it, by increasing the cost on them to such an extent that they decide to cease the offending behaviour;
- **ii.** Constrain a target by denying it access to key resources needed to continue its offending behaviour, including the financing of terrorism or nuclear proliferation;
- **iii.** Signal disapproval, resulting in stigmatizing and potentially isolating the target, or as a way of sending broader political messages domestically or internationally; and
- **iv.** Protect the value of assets that have been misappropriated from a country until such assets can be repatriated.

6. Measures that are frequently applied through international sanctions include:

- **i.** Financial sanctions, including asset freezes, bans on investment or access to capital markets, limitations on banking activities or relationships and restrictions on the provision of other financial services or advice;
- **ii.** Trade controls on the importation, exportation, or financing of specified goods, services, equipment, and activities; and

7. Directions to cease all business with a specific person, group, sector, or country. The primary sources of international sanctions affecting Belize's financial institutions are the UN and EU.

1.1 The Belize Sanctions Regime

8. Most of Belize's international sanctions are brought into force through the MLTPA.

9. The scope of restrictions varies, and financial institutions must review the relevant provisions of the MLTPA together with each Notice issued by the FIU in accordance with section 12 of the MLTPA and each Order issued by the High Court in accordance with section 68, together with any accompanying lists, annexes, schedules, updates, or amendments, to ensure compliance with the specific requirements including:

- **i.** Asset freezing;
- **ii.** Prohibitions against provision of financial and other related services; and
- **iii.** Reporting.

10. An asset freeze generally prohibits dealings with frozen funds or economic resources belonging to or owned, held, or controlled by a sanctions target. An asset freeze may also prohibit making funds, economic resources and, in some cases, financial services available, directly, or indirectly, to or for the benefit of a sanctions target. Asset freezing can, therefore, affect any transaction or business relationship in which a customer, counterparty, beneficial owner, trustee, or other party is a sanctions target or is acting on behalf of or for the benefit of a sanctions target.

11. Indirect payments are those made to someone acting on behalf of a sanctions target. A payment that is for the benefit of a sanctions target is a payment that is made to a third party to satisfy an obligation of a sanctions target.

12. When a legal or natural person is named as a sanctions target, their name is recorded on The Belize Consolidated Sanctions List (Consolidated List). In that case, an asset freeze and restrictions on the provision of financial or other related services will also apply to entities that are wholly or jointly owned or controlled, directly or indirectly, by a sanctions target. Although entities owned or controlled by a sanctions target may not be included on the consolidated list, such entities are nonetheless subject to financial sanctions.

13. To assess whether a legal person or entity is owned by another person or entity, financial institutions should determine whether the sanctions target owns more than 50% of the proprietary rights of an entity or has a majority interest in it. If this criterion is met, then financial sanctions apply both to the sanctions target and to the majority-owned entity.

14. 'Owned' is interpreted to include direct and indirect ownership. If it is determined that a sanctions target is the ultimate beneficial owner of an entity, for example, where the sanctions target owns a corporate body that, in turn, owns another corporate body, then all entities that are part of the ownership chain are subject to financial sanctions.

15. To assess whether a legal person or entity is controlled by another person or entity, financial institutions should consider whether, with regard to the legal person or entity, a sanctions target:

i. Has the right or exercises power to appoint or remove a majority of the members of the administrative, management or supervisory body of such a legal person or entity;

ii. Has appointed, solely as a result of the exercise of the sanctions target's voting rights, a majority of the members of the administrative, management or supervisory bodies of a legal person or entity who have held office during the present and previous financial year;

iii. Controls alone, pursuant to an agreement with other shareholders in or members of a legal person or entity, a majority of shareholders' or members' voting rights in that legal person or entity;

iv. Has the right to exercise a dominant influence over a legal person or entity, pursuant to an agreement entered with that legal person or entity or to a provision in its memorandum or articles of association, where the law governing that legal person or entity permits it being subject to such an agreement or provision; or

v. Has the right to exercise a dominant influence referred to in the point above without being the holder of that right, including by means of a front company.

16. As required by sections 68 (5R), and (5S) of the MLTPA, sanctions in effect in Belize require financial institutions to inform the FIU of any instance in which:

i. The financial institution knows, suspects, or has reasonable cause to suspect that a customer or any person with whom the financial institutions have or has had dealings is a sanctions target; or

ii. The financial institution or sanctions target has breached a sanction.

17. Any report described in paragraph above must be made to the FIU, and a copy should be provided to the Central Bank.

1.2 Compliance with the Belize Sanctions Regime

18. Each financial institution must have adequate policies, procedures, and controls to comply with the Belize sanctions regime.

19. A financial institution's policies, procedures and controls should be documented and approved by its board of directors or senior management.

20. Each financial institution's policies, procedures and controls must enable it to conduct screening including ongoing screening of its customers and transactions to determine whether it is conducting or may conduct business involving any sanctioned person, entity, or activity.

21. The financial institution's sanctions checking processes should be proportionate to the nature and size of its business and should be likely to identify all target matches with sanctions targets.

22. A financial institution's process of determining which sanctions compliance measures is proportionate and likely to identify all target matches differs in a key manner from the risk-based approach for AML/CFT/CPF compliance.

23. Whereas a financial institution may choose to have a higher risk tolerance with regard to AML/CFT/CPF compliance and, therefore, may choose to transact with higher-risk customers, a

financial institution may not choose to transact in violation of the Belize sanctions regime. There is, therefore, no room for risk tolerance in sanctions compliance. Any financial institution that provides any funds or financial services to sanctions target or fails to freeze the assets of a sanctions target, is in breach of the sanctions regime and liable to be prosecuted.

24. Although sanctions compliance is a rules-based approach, a financial institution's assessment of its risk of exposure to sanctioned persons, entities and activities is expected to assist in preventing the financial institution from breaching the sanctions regime. Each financial institution should conduct such a risk assessment, conducting it in line with what is prescribed for the AML/CFT/CPF assessment and keeping it up-to-date with reference to the following non-exhaustive list of risk factors:

- **i.** Customers, products and activities;
- **ii.** Distribution channels;
- **iii.** Complexity and volume of transactions;
- **iv.** Processing and systems;
- **v.** Operating environment;
- **vi.** Screening processes of intermediaries;
- **vii.** Geographic risk; and
- **viii.** Any other relevant sanctions regulations.

25. To tailor its sanctions compliance measures to the nature and size of its business, a financial institution should take the following steps:

- **i.** Understand and identify the applicable sanctions;
- **ii.** Develop and document appropriate policies, procedures and controls in order to comply with the sanctions;
- **iii.** Apply the sanctions compliance policies, procedures and controls that have been developed and documented;
- **iv.** Maintain up-to-date sanctions information; and
- **v.** Regularly review, test, and improve the sanctions compliance policies, procedures and controls put in place.

26. Each financial institution should ensure that its sanctions-related policies, procedures, and controls effectively guide the institution in:

- **i.** Ensuring up-to-date knowledge of the applicable sanctions;
- **ii.** Tailoring sanctions compliance measures to the financial institution's business;
- **iii.** Screening the financial institution's customers, transactions, third-party service providers and geographic connections for potential matches with sanctions targets;
- **iv.** Reviewing potential matches to identify target matches;
- **v.** Freezing assets or taking any other required action in the event of a target match;
- **vi.** Reporting target matches and any breaches;

vii. Ensuring appropriate staff awareness and training; and

viii. Documenting and recording actions taken to comply with the sanctions regime and the rationale for each such action.

27. Reviewing the effectiveness of the financial institution's policies, procedures, and controls. Each financial institution must ensure that it knows its business and does not breach the sanctions regime. Financial Institutions should ensure that effective policies, procedures, and controls are implemented to prohibit and detect attempts by employees or customers to:

a. Omit, delete, or alter information in payment messages for the purpose of avoiding detection of that information by other payment service providers in the payment chain; or

b. Structure transactions for the purpose of concealing the involvement of a sanctions target.

1.3 Other Unilateral Sanctions Regimes

28. Where a financial institution has a presence or is otherwise active in a jurisdiction outside of Belize, it may be required to comply with the sanctions requirements of that other jurisdiction. Transacting with a customer or counterparty in another jurisdiction may also trigger the sanctions requirements of that jurisdiction, even if a financial institution has no presence there.

29. Financial institutions should obtain legal advice to understand which sanctions regimes apply to which aspects of their business and to ensure that they correctly comply with applicable sanctions while not incorrectly applying sanctions regimes of other jurisdictions to Belize business.

30. Where a financial institution operates in a number of jurisdictions, a consistent group policy should be established to assist local business units in ensuring that their local procedures meet minimum group standards while also complying with local requirements.

1.4 Training

31. Each financial institution should implement a sanctions-related employee training and awareness programme that is appropriate for the financial institution's business as well as the level of the employee.

32. The form, structure, and scope of a financial institution's training and awareness programme should be in line with these guidelines, bearing in mind the differences between complying with AML/CFT/CPF obligations and sanctions obligations.

33. The substance of the training and awareness programme should, at a minimum, include the financial institution's policies, procedures, and controls for:

i. Complying with new sanctions that come into force;

ii. Ceasing compliance with sanctions that have been retired from effect;

iii. Screening for applicable sanctions targets;

iv. Reporting target matches and any breaches;

v. Documenting actions taken to comply with the sanctions regime and the rationale for

each such action; and

vi. Communicating changes to the financial institution's sanctions obligations, including changes to its sanctions-related policies, procedures, and controls.

1.5 Documentation and Record-keeping

34. Financial institutions should ensure that appropriate record is made of the following:

i. The financial institution's sanctions-related policies, procedures and controls;

ii. Actions taken to comply with the sanctions regime;

iii. Information sought and obtained to confirm or eliminate a potential match;

iv. The persons who decide whether a potential match is a target match;

v. The rationale for the decision; and

vi. The information used for preparing and contained in any report to the FIU.

35. Financial institutions, at a minimum, should retain record of the following information about any potential match, whether it turned out to be a true match or a false positive:

i. The information or other grounds that triggered the match (e.g., a 'hit' provided by screening software);

ii. Any further checks or inquiries undertaken;

iii. The relevant sanctions regime;

iv. The person(s) involved, including any members of compliance or senior management who authorized treatment of the match as a false positive;

v. The nature of the relationship with the person or entity involved, including attempted or refused transactions;

vi. Subsequent action taken (e.g., freezing accounts); and

vii. Whether the financial institution consulted with or filed a report with the FIU.

36. All related records should be retained in accordance with the record-keeping requirements in this Guideline.

1.6 Reviewing Effectiveness

37. Each financial institution should monitor its policies, procedures, and controls to ensure full, up-to-date, and timely compliance with rapidly changing sanctions obligations.

38. A financial institution should make the review of its sanctions-related policies, procedures, and controls part of its AML/CFT/CPF independent audit.

39. Senior management is responsible for the effectiveness of a financial institution's sanctions-related policies, procedures, and controls. The compliance officer may be the appropriate person to grant authority to:

i. Oversee the establishment, maintenance and effectiveness of the sanctions-related policies, procedures and controls;

ii. Monitor compliance with the relevant acts, regulations, and guidance; and

iii. Access all necessary records in a timely manner in order to respond to any information gathering authorized by an order.

1.7 Screening Customers and Transactions

40. Financial institutions should screen their business and transactions for any person, entity, activity or good that is a sanctions target. Screening should be conducted against appropriate lists, such as UN sanctions and Belize's consolidated list of all orders.

41. Screening should be conducted every three months and within hours of a new Order being issued. Screening should be conducted for new accounts and ongoing transactions.

42. Financial institutions should screen not only their customers but, wherever possible, any other related parties, including, but not limited to, the following:

i. Counterparties; trustees and similar persons;

ii. Beneficial owners, directors, signatories and similar persons of customers, counterparties and third-party service providers;

iii. Persons authorized by power of attorney; and

iv. The geographic connections of the abovementioned persons and entities.

43. At a minimum, each financial institution should screen every related party for which verification of identity is sought under the financial institution's risk-based policies, procedures, and controls.

1.8 Non-Standard CDD Measures

44. Where a financial institution chooses not to screen any customer or related party, it should be aware that it is increasing its likelihood of committing a sanctions offence.

45. Financial institutions should screen the payment information associated with transfers of funds to identify any potential sanctions targets. Financial institutions should screen information contained within the payment messages, cover messages or batch files of any messaging system, as well as any information associated with the transfer of funds that is conveyed by any other means.

1.9 Timing and Scope of Screening

46. Initial screening of customers and related parties should take place during the establishment of a business relationship or as soon as possible thereafter.

47. Where a financial institution conducts screening after the establishment of a business relationship, it should be aware that it risks transacting with sanctions target in breach of the sanctions.

48. The screening of payment information should take place on a real-time basis. A financial institution may accept an incoming payment prior to screening for a sanctions target, but it must not forward any payment, disburse any funds, or otherwise make funds or assets available to any party prior to

screening.

49. Financial institutions should consider conducting post-event screening only for incoming transactions, provided that the financial institution maintains control over the funds or assets and no funds or assets are made available to any other parties prior to the completion of screening.

1.10 Screening software

50. Financial institutions may choose to use commercially available screening software; other financial institutions may rely on manual screening.

51. Where a financial institution chooses to use screening software, the financial institution should ensure that the software will flag potential matches with sanctions targets in a clear and prominent manner.

52. Financial institutions should understand the capabilities and limits of any software and ensure that the software is appropriate given the nature and size of the business and the volume and types of data the business uses, including data held in any legacy systems.

53. Where automated software screening is used, financial institutions should monitor and test the ongoing effectiveness of the software and ensure that adequate contingency arrangements are in place in the event that the software fails.

54. Financial institutions should, wherever possible, use a screening system with 'fuzzy matching[1]' capabilities. These capabilities are often tolerant of multinational and linguistic differences in spelling, transliteration, formats for dates of birth and similar data. 'Fuzzy matching' systems may also screen for the reversal of names, the removal of numbers or the replacement of numbers with words, which are techniques that have been used in an attempt to evade sanctions.

55. A sophisticated 'fuzzy matching' system will have a variety of settings, allowing financial institutions to set greater or lesser levels of 'fuzziness' in the matching process. In determining an appropriate level of 'fuzziness', a financial institution should ensure that all potential matches are flagged.

1.11 Reliance and Outsourcing

56. In determining its screening policies, procedures and controls, a financial institution should not assume that the introduced business has been screened for sanctions compliance or that any screenings conducted were adequate or maintained up to date.

57. Financial institutions may choose to outsource to a third-party service provider some or all of its sanctions screening or other sanctions-related processes, bearing in mind that a financial institution cannot contract out of its statutory and regulatory obligations under the Belize sanctions regime. Financial institution should ensure that the responsibilities in any outsourcing relationship are clearly set forth in a service level agreement. Financial institutions should satisfy themselves that the service

[1] 'Fuzzy matching' describes any process that identifies non-exact matches. Where data in a financial institution's records or in official sanctions lists is misspelt, incomplete, or missing, a screening system with 'fuzzy matching' capabilities will, nonetheless, identify potential matches.

provider is providing an effective service.

58. Financial institutions must not rely upon or enter into any outsourcing arrangement with a third party where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions.

1.12 Reporting Matches and Breaches

59. Financial institutions should investigate potential matches with sanctions targets to determine whether there are any target matches.

60. A target match arises where a financial institution knows, suspects, or has reasonable grounds to suspect that it is conducting or may conduct business involving a sanctions target.

61. A financial institution may need to seek sufficient information from relevant parties to enable it to determine whether it has knowledge, suspicion, or reasonable grounds for suspicion of a target match. A financial institution should ensure that there is a clear rationale for any decision that a potential match is not a target match.

62. Financial institutions should maintain a record of the information sought and obtained, the person or persons involved in the review of the potential match, and the rationale for the decision made.

63. Financial institutions must ensure that they have clear internal and external reporting processes for reporting target matches to the FIU and the Central Bank of Belize (Central Bank).

64. Where a financial institution identifies a target match, it should verify whether the sanctions target is listed in a Notice or an order that has been given effect in Belize.

65. Where a financial institution identifies a target match for sanctions that are in effect in Belize, the financial institution must:

- **i.** Immediately comply with the terms of the order by immediately freezing any funds or economic resources, where required, or taking any other required action; and
- **ii.** Not enter into financial transactions or provide financial assistance or services in relation to the sanctions target, and not engage in any other activity sanctioned under the directive unless there is an exemption in legislation on which the financial institution can rely;
- **iii.** Immediately report the target match to the FIU in a manner specified by the FIU.

66. When informing the FIU of a target match or that a financial institution or a sanctions target has breached a sanction, the financial institution should copy the Central Bank and include the following:

- **i.** The information or other matter on which the knowledge, suspicion or reasonable grounds for suspicion or breach is based;
- **ii.** Any information held by the financial institution about the sanctions target by which the target can be identified; and

iii. The nature and amount, quantity or value of any funds or economic resources held by the financial institution in relation to the sanctions target.

67. Where a financial institution freezes assets, it should do so immediately upon discovering the target match and should ensure that relevant staff do not process any further transactions without an express direction from senior management. Freezing and/or ceasing the provision of services must take place immediately upon detection and then should be followed by the filing of the relevant form.

1.13 Suspicious Transaction Reports and Tipping-Off

68. Where a financial institution has knowledge, suspicion, or reasonable grounds for suspicion that funds or assets involve criminal property, it must comply with its obligations under the MLTPA.

69. The fact that a target is subject to sanctions is public information, and there is no prohibition on financial institutions informing customers or third parties of a target's sanctioned status. Informing customers or third parties of a target's sanctions status is not a tipping-off offence. Remember however that freezing and/or ceasing the provision of services must take place immediately upon detection and then should be followed by the filing of the relevant form.

70. By contrast, where a financial institution has filed a suspicious transaction report (STR) with the FIU, disclosing the fact that the STR was filed is a tipping-off offence.

1.14 Penalties for Non-compliance

71. Financial institutions must be aware that, in contrast to AML/CFT/CPF measures, which generally permit financial institutions to set their own timetables for verifying and updating customer due diligence (CDD) information, a financial institution risks breaching a sanctions obligation as soon as a person, entity or good is listed under a sanctions regime in effect. In addition, whereas a financial institution may choose to transact with a higher-risk natural person or entity, it may not transact with any natural person or entity subject to the sanctions regime in breach of such regime.

72. The sanctions regime applies to natural persons as well as legal persons and arrangements. Where any financial institution is guilty of an offence and that offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the financial institution, or any person who was purporting to act in any such capacity, both that person and the financial institution are guilty of that offence and liable to be proceeded against and punished accordingly in accordance with the MLTPA.