Financial Intelligence Centre

PUBLIC COMPLIANCE COMMUNICATION

PUBLIC COMPLIANCE COMMUNICATION 44A

IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS IN SOUTH AFRICA

PCC SUMMARY

The Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act) places certain obligations on accountable institutions and other persons to implement measures in relation to the asset freeze requirements of the United Nations Security Council (UNSC) resolutions and South African domestic implementation of targeted financial sanctions (TFS) against individuals and entities so designated.

This public compliance communication (PCC) provides guidance to accountable institutions regarding their obligations to implement UNSC resolutions and domestic designations asset freezing requirements of TFS, which are aimed at combating the financing of terrorism (CFT) and of combating the financing of proliferation (CFP) of weapons of mass destruction (WMD). TFS obligations in terms of the FIC Act include scrutinising client information against TFS list to identify designated persons and entities directly or indirectly linked to clients, freezing property of designated persons and entities, filing terrorist property, and suspicious and unusual transaction reports with the Financial Intelligence Centre (Centre), as well as obligations regarding de-listing and unfreezing of individuals and entities no longer designated by UNSC resolutions.

In addition, the PCC provides examples of terrorist and proliferation financing risks and recommendations for the application of a risk-based approach (RBA) to combating both terrorist and proliferation financing.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the users' legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

COPYRIGHT NOTICE

OBJECTIVE

The PCC provides guidance to accountable institutions on the implementation of TFS aimed at CTF and CPF. The PCC sets out examples of terrorist and proliferation financing risks accountable institutions may face and provides recommendations regarding the implementation of a risk-based approach (RBA) to CFT and CFP.

1. INTRODUCTION

1. South Africa implements the targeted financial sanctions (TFS) that originate from the United Nations Security Council (UNSC) resolutions under Chapter VII of the Charter of the United Nations. By virtue of South Africa's United Nations membership, it applies all UNSC resolutions adopted under this Charter, which relate to among other aspects, the prevention and suppression of terrorism and terrorist financing, as well as the prevention, suppression and disruption of the proliferation of weapons of mass destruction (WMD) and its financing. The measures range from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans and financial or commodity restrictions.

2. Financial Action Task Force (FATF) Recommendations 6 and 7 require the implementation of UNSC resolutions on TFS for all FATF member countries.

3. South Africa's TFS obligations require accountable institutions to scrutinise information concerning clients against TFS lists, apply freezing of assets of designated persons or entities, and file terrorist property regulatory reports with the Centre. Furthermore, no persons may provide or make available funding to designated persons or entities.

4. In addition to TFS obligations, accountable institutions must adopt a risk-based approach to ensure their controls are proportionate to the TF and PF risks, and that sufficient resources are focused on heightened risks of TF and PF. The risk-based approach is intended to reinforce and complement the rules-based controls that accountable institutions have in place for TFS.

5. This PCC must be read together with Guidance Note 6A that provides guidance on the terrorist property reporting obligation, the South African National Terrorism Financing Risk Assessment[1], and the TFS list manual as available on the Centre's website. Accountable Institutions that are subject to the South African Reserve Bank (SARB)

[1] As at date of publication of PCC 44A the South African National Terrorism Financing Risk Assessment as published on 31 March 2022 factors was incorporated. https://www.fic.gov.za/wp-content/uploads/2023/11/2022.03-NRA-2022-Terrorist-Financing-National-Risk-Asssessment.pdf. Accountable institution must rely on the latest versions of national risk assessments.

oversight, must in addition consider the SARB issued Guidance Note 12/2022 that provides guidelines related to risk management practices concerning proliferation financing risk, SARB Guidance note 4/2023 on the use of Terrorist Financing or other unlawful activity and SARB Directive 1 of 2022.

6. This PCC applies to all accountable institutions and other persons.

7. Further information regarding the implementation of asset freeze requirements of relevant UNSC resolutions can be found in FATF guidance available on its website (https://www.fatf-gafi.org/). Information on the UNSC consolidated list is available on the UNSC website (https://www.un.org/securitycouncil/sanctions/information).

8. This PCC consists of four parts:

Part A – Targeted financial sanctions aimed at combating TF and PF
Part B – Risk-based approach to combating terrorist financing risks
Part C – Risk-based approach to combating proliferation financing risks
Part D – De-risking

PART A – TARGETED FINANCIAL SANCTIONS AIMED AT COMBATING TERRORIST FINANCING AND PROLIFERATION FINANCING

9. South Africa's application of UNSC resolutions and FATF Recommendations 6 and 7are reflected in sections 26A, 26B, 26C and 28A of the FIC Act and sections 4, 15, and 23 of the POCDATARA Act, (Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act 33 of 2004) which collectively set out TFS obligations for accountable institutions and all other persons in South Africa.

10. Section 26B read together with section 49A of the FIC Act, prohibits the financing of persons or entities who are subject to TFS in terms of section 26A of the FIC Act. The prohibitions relating to TFS regimes are absolute and must be applied by all persons in respect of designated person or entities. No person may directly, indirectly, in whole or in part enter into or facilitate a transaction for persons or entities listed on the UNSC resolutions.

11. This prohibition in section 26B of the FIC Act is applicable, but not limited to, all instances where the designated person or entity is:

11.1. The client

11.2. The person acting on behalf of the client

11.3. The client acting on behalf of another person

11.4. A beneficial owner of the client; or

11.5. A party to a client's transaction, including a party who benefits in any way from a client's transaction.

12. The TFS prohibition extends beyond the specific person or entity designated by the UNSC and could include instances where the clients are acting on behalf of another person who is designated, or where a designated person is acting on behalf of the client, or where the client is linked to a designated person or entity.

13. A designated person or entity refers to a specifically named person or entity pursuant to a UNSC resolution, e.g. a person or entity whose name is reflected on a TFS list.

14. Section 4 of the POCDATARA Act read together with section 15 of the POCDATARA Act criminalises the financing and facilitating of terrorist and related activity, which offence applies to everyone subject to South African law, not only accountable institutions.

15. Section 23 of the POCDATARA Act provides a freezing mechanism when there is reason to believe property is that of a designated person or entity, or where there is a reasonable belief terrorist activity is involved.

16. TFS obligations in terms of the FIC Act include the requirements to scrutinise, freeze and file a regulatory report to the Centre.

Scrutinising client information

17. In terms of section 26A of the FIC Act, the Director of the Centre must give notice of persons or entities who have been designated as sanctioned persons or entities in a resolution of the UNSC. The notice, as published by the Director of the Centre, communicates updates to the TFS list and is published on the Centr website.

18. Section 28A(3) of the FIC Act requires that an accountable institution must scrutinise its information concerning clients with whom the accountable institution has a business relationship, against the TFS list, to determine if any persons are designated persons or entities or linked to designated persons or entities.

19. The Centre recommends that accountable institutions scrutinise information concerning clients with whom the accountable institution seeks to conclude a single transaction with against the TFS lists as published on the Centre's website.

20. There can be no scenario where the accountable institution does not scrutinise information concerning a client when establishing a business relationship. Accountable institutions must scrutinise information concerning clients against the TFS list regardless of any unique factors (such as a client being a South African national, a transaction is not cross-border etc.) or the level of the perceived risk is considered to be low. Screening must be applied for both domestic and international transactions.

21. The results from scrutinising information concerning a client, must be used as a factor that informs the risk rating. A positive match on a TFS list, for example, informs an immediate high-risk-rating for the client risk assessment. Where the positive match is either an existing client, beneficial owner, person acting on behalf of a client, person on whose behalf the client is acting, or party to a client transaction, that would result in a freezing and reporting obligation. The accountable institution must not onboard a prospective client where that person, the person's beneficial owner, the person acting on behalf of a prospective client, the person on whose behalf the prospective client is acting, or party to a prospective client's transaction, is a designated person or entity.

22. The accountable institution must apply adequate scrutinising at the appropriate frequency and intensity. Where there is an increased risk of breach of TFS, accountable institutions are cautioned to increase the frequency and amount of information sought to be scrutinised. The higher the TFS risk particular client types, products, services, or geographic areas pose to the institution, the greater the level of scrutiny required of clients' information.

23. Should the accountable institution fail to identify that a person is listed as or linked to a designated person or entity, the accountable institution will be found to be in contravention of the TFS obligations.

24. The accountable institution must obtain and scrutinise sufficient information to make a determination, with a certain level of confidence, that it does not inadvertently provide products or services to the benefit of a designated person or entity. The information concerning a client, includes but is not limited to information concerning the prospective client, existing client, person acting on behalf of the client, person on whose behalf the client is acting, beneficial owner or party to a transaction.

25. The information that should be used for scrutinising includes the person's name, identification number, place of birth, address, date of birth, nationality, entity's name and other information. Other information may include, but is not limited to, the country of residence in the case of a natural person.

26. Accountable institutions must have a process implemented and documented as part of their risk management and compliance programme (RMCP) for scenarios where a person or entity is a match on a TFS list, versus when a person or an entity is a false match.

27. Information relating to persons or entities linked directly or indirectly to clients, where available, and to the extent to which this is known by the accountable institution, should be scrutinised by the accountable institution to determine if such an indirect person or entity is designated.

28. Accountable institutions must scrutinise their information concerning a client:

28.1. At client onboarding

28.2. When conducting transactions and

28.3. When the TFS list is updated. All existing information concerning clients must be scrutinised against the TFS lists as and when the TFS list is updated.

29. The Centre strongly advises accountable institutions to scrutinise information concerning a client against the TFS list published on the Centre's website without delay. Accountable institutions are advised to regularly monitor the Centre's website for updates to the TFS list.

30. When a UNSC resolution is adopted designating persons or entities, that resolution has immediate effect in South Africa, which includes for purposes of the application of sections 26B, 26C and 28A of the FIC Act.[2] Accountable institutions may therefore as good practice also scrutinise information concerning clients against the UNSC consolidated sanctions list, in addition to the TFS list as published on the Centre's website.

[2] The General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act, 2022 (Act 22 of 2022) (GLA Act) amended **section 26A(1)** of the FIC Act

31. It is not the expectation of the Centre that the accountable institution performs extensive monitoring with sophisticated or complex systems to scrutinise information concerning a client. The process adopted for purposes of scrutinising client information against the TFS list can be done manually or through an automated system.

32. Where an accountable institution uses a third-party service provider(s) to assist in scrutinising information concerning a client, the accountable institution remains accountable to comply with its obligation to scrutinise without delay. In the scenario where the third-party service provider incorporates the TFS list notifications as published on the Centre's website in its internal screening tool lists, the accountable institution should consider any risk of delays where internal screening tool lists of the third party are not updated without delay. Refer also to PCC 12A which sets out guidance on outsourcing.

33. Where an accountable institution uses a third-party service provider(s) to assist with scrutinising, the accountable institution must document the process in its RMCP and be able to demonstrate that the third-party service provider(s) screening lists include the latest TFS list as published on the Centre's website.

34. Failure to scrutinise information concerning a client in accordance with section 28A read together with section 26A of the FIC Act amounts to non-compliance, as accountable institutions remain responsible and cannot delegate their obligation to a third party.

35. The TFS list published on the Centre's website is an up-to-date searchable list, that is downloadable and printable for audit records of all searches done. The Centre recommends that as part of the accountable institution's RMCP controls, it keeps record of the results of scrutinising information concerning a client against the TFS list. Further, where the accountable institution uses a third-party service provider(s) for scrutinising purposes, that accountable institution would nonetheless still have to keep records of scrutinising. The records kept should indicate the date on which scrutinising was done.

Example – manual scrutinising

Accountable institution A scrutinises its client information against the TFS list on the Centre's website, which returns "no results". The accountable institution proceeds to save the results as a PDF in the client records.

Example – automated scrutinising

Accountable institution B uses a third-party service provider's automated sanctions screening system, which incorporates the TFS list on the Centre's website into its data to scrutinise information concerning clients automatically. Alerts are generated where possible matches are detected, the system has an audit trail of true matches and false matches, and the accountable institution can evidence scrutinising information concerning clients against the TFS list.

36. Institutions that are not accountable institutions are advised to implement a process to scrutinise their client information to ensure that they do not provide products or services to designated persons or entities.

Applicable United Nations Security Council resolutions

37. The following TFS regime UNSC resolutions and successor resolutions currently form part of the TFS regime in terms of the FIC Act as of 10 December 2019.
    - Somalia Sanctions Regime
    - ISIL (Da'esh) and Al-Qaida Sanctions Regime
    - Iraq Sanctions Regime
    - Democratic Republic of the Congo (DRC) Sanctions Regime
    - Sudan Sanctions Regime
    - 1636 Sanctions Regime
    - Democratic People's Republic of Korea (DPRK) Sanctions Regime
    - Libya Sanctions Regime
    - 1988 Sanctions Regime
    - Guinea-Bissau Sanctions Regime
    - Central African Republic (CAR) Sanctions Regime
    - Yemen Sanctions Regime
    - South Sudan Sanctions Regime

- Haiti Sanctions Regime
- 1540 Sanctions Regime

*These UNSC resolutions listed relate specifically to financial sanctions that have an associated asset freeze obligation.

38. Accountable institutions are reminded that UNSC resolutions have immediate effect in South Africa. The General Laws (Anti-money Laundering and Combating of Terrorism Financing) Amendment Act 2022 (Act 22 of 2022) (GLA Act), amended section 26A of the FIC Act in this regard.

Non-targeted financial sanctions lists

39. Accountable institutions can scrutinise information concerning their clients against other domestic, regional and unilateral sanctions lists published by other regulators or supervisory bodies (e.g. the United States Treasury Office of Foreign Assets Control, Specially Designated Nationals and Blocked Persons list, the United Kingdom His Majesty's Treasury Office for Financial Sanctions Implementation, European Union Sanctions lists etc.) in accordance with its risk-based approach and/or obligations that stem from its correspondent relationships or due to the geographic area in which it operates etc.

40.1. Where there are true matches against these other domestic, regional and unilateral sanctions lists, the accountable institution must determine the course of action in accordance with its obligations and risk-based approach.

40.2. Section 26A, 26B, 26C and 28A of the FIC Act does not apply where the person or entity is not designated either on the TFS list as published on the Centre's website, UNSC consolidated sanctions list or in terms of a section 23 of POCDATARA court order.

40.3. Accountable institutions are strongly encouraged to submit a section 29 suspicious and unusual transaction report, where there is a true match against other domestic, regional and unilateral sanctions lists.

40.4. Accountable institutions are advised to seek further guidance from the relevant regulator or supervisory body who published the other domestic, regional and unilateral sanctions list where true matches are found in the sanctions lists.

Targeted freeze of property of designated persons or entities

41. Obligations relating to the freezing of TF and/or PF related property include:

41.1. An automatic obligation to freeze in terms of section 26B of the FIC Act

41.2. An automatic obligation to freeze in terms of section 4 of the POCDATARA Act, and

41.3. An *ex-parte* application for a freezing order in terms of section 23 of the POCDATARA Act.

Freeze in terms of section 26B of the FIC Act

42. The effect of the application of section 26B of the FIC Act, is that when an accountable institution identifies a designated person or entity, as its client or linked to its client, the accountable institution must immediately cease any activity in relation to that designated person or entity. This can include not releasing any property to the designated person or entity, and persons acting on behalf of the designated person or entity. This is viewed, and commonly referred to, as a “freeze”.

43. This action of freezing property is the process in which the prohibition can be practically adhered to and is considered an obligation in and of itself. Therefore, an accountable institution does not have to obtain any consent from either the Centre or through a court order to freeze the designated person’s or entity’s property in terms of section 26B of the FIC Act.

44. An accountable institution must have a process in place to ensure the freezing of a designated person’s or entity’s property immediately without delay where the accountable institution is in possession or control of such property. The freeze must also be applied where it is found that a person is acting on behalf of or at the direction of a designated person or entity, and a freeze should be applied to the related property.

45. Property also includes assets, any form of monetary value or funds, negotiable instruments (e.g. letters of credit, bills of lading, credit facility) that is owned, held, or controlled directly or indirectly for the benefit of a designated person or entity.

46. The freeze must be applied regardless of whether or not the property is going to be used in a terrorist attack, an attempted terrorist attack, the financing of terrorist activity, and/or for the purposes of financing of the proliferation of WMD or related activities. The mere fact that the accountable institution has in its possession or control property of a designated person or entity, including a person who committed or attempted to commit a terrorist or proliferation activity, is sufficient reason to apply the immediate freeze.

47. An accountable institution must freeze the designated person's or entity's property immediately, without delay. Such an accountable institution must not wait to first report to the Centre that it has in its possession or control property of a designated person or entity or wait to receive any communication from the Centre to freeze such property.

48. Failure to adhere to the prohibition in terms of section 26B of the FIC Act constitutes an offence in terms of section 49A of the FIC Act.

49. The Centre does not prescribe the communication that an accountable institution provides to a client, person or entity upon determining that such client is a designated person or entity impacted by TFS and an asset freeze. The accountable institution can exercise its discretion when determining this communication.

50. The accountable institution must have a documented process in its RMCP to ensure the freezing of a designated person or entity's property immediately, without delay.

51. An accountable institution may not proceed to provide or release any financial services or property to a designated person or entity unless prior written permission for such a release has been obtained from the Minister of Finance, or the Director of the Centre acting upon a delegation from the Minister of Finance, in terms of section 26C of the FIC Act, or unless the person is de-listed. Only financial services or property, as allowed for in the permit, can be made available to the designated person or entity. The

application form for permitted financial services in terms of section 26C of the FIC Act can be found on the Centre's website.

52. The accountable institution must not lift the freeze unless the designated person is de-listed by the UNSC, and this is communicated on the UNSC consolidated list and the Centre's TFS list or a permit is obtained in terms of section 26C of the FIC Act. Where a person is de-listed from the UNSC Consolidated list and the TFS list, the accountable institution may unfreeze the person's property automatically and does not have to seek further written permission (as envisioned in section 26C of the FIC Act).

Example – Bank in possession of designated person's property

Bank C scrutinises information concerning their client against the TFS lists and finds that Mr T is a designated person on the TFS list in terms of section 26A of the FIC Act. Bank C holds funds of Mr T in cheque and investment accounts. Bank C immediately ceases to release or facilitate any transactions on behalf of Mr T when it becomes aware Mr T is a designated person. Bank C must, in terms of its TFS obligations, apply an automatic freeze on funds it has under its possession or control or linked to Mr T. Bank C must report Mr T as a true match and client, as well as the freezing of Mr T's and any links to Mr T's property to the Centre.

53. The Centre does not prescribe the circumstances under which an accountable institution should seek to terminate a business relationship. Where an accountable institution terminates a relationship with a client which results in a designated person gaining access to property that termination would result in the breach of the accountable institution's targeted financial sanctions obligations.

Domestic designation and freezes in terms of the POCDATARA Act

54. Similar to section 26B of the FIC Act, section 4 of POCDATARA Act has the effect that when an accountable institution identifies a designated person or entity, or terrorist related activity, the accountable institution must immediately cease any activity in relation to that designated person or entity or terrorist related activity. This can include

not releasing any property to the designated person or entity, and persons acting on behalf of the designated person or entity.

55. Section 23 of the POCDATARA Act provides a mechanism for the National Director of Public Prosecutions to apply for an order prohibiting any conduct and freezing of property linked to a specified offence or designated person or entity, through an *ex-parte* application.

56. The Centre will publish orders made in terms of section 23 of the POCDATARA Act on the Centre's website, the Centre will also give notice of the freezing order to accountable institutions.

57. Accountable institutions should scrutinise the information concerning their clients against the section 23 of the POCDATARA Act court order information, in the same manner as it would scrutinise information concerning its clients against the TFS list.

58. Where an accountable institution confirms a match with a person designated in terms of a section 23 of POCDATARA Act court order, then the accountable institution must immediately apply a freeze to that client's property held by them, and file a terrorist property report (TPR) in terms of section 28A of the FIC Act.

59. There may be instances where a court order granted in terms of section 23 of the POCDATARA Act is set aside by a High Court, this will have the effect of de-listing of the persons listed in the court order. The accountable institution must not lift the freeze from the relevant de-listed person's property held by them, unless the designated person is de-listed through a section 23 of POCDATARA court order being set aside, or a permit is obtained in terms of section 26C of the FIC Act.

United Nations Security Council resolution de-listing process

60. Where a person or entity is de-listed from a TFS list, an accountable institution that has property related to the person or entity has an obligation to "unfreeze" the property. This can be done automatically. Where an accountable institution requires further guidance

regarding the proposed action, it may contact the Centre. Refer to the FIC website for further information on de-listing.

Reporting

61. All persons are referred to Guidance Note 6A regarding TPRs and Guidance Note 4B for guidance on suspicious and unusual transaction reports (STRs), as issued by the Centre.

62. The Centre strongly urges persons who are approved to deal in controlled goods or activities gain an understanding of the various TF and PF typologies and implement enhanced controls to monitor transactions to identify suspicious and unusual transactions that relate to TF or PF. Where such suspicious and unusual activity is identified, such persons must report this in an STR to the Centre in terms of section 29 of the FIC Act. All businesses have a duty to report STRs to the Centre.

Example of an activity that requires scrutiny

Bank C has a client who is a diplomat, or a citizen or legal person of a high PF risk geographic area, and the client is not designated on a TFS list. However, the client's transaction activity is suspicious and unusual. The accountable institution should consider the risk of PF in this scenario and the filing of a STR with the Centre.

63. Accountable institutions must report activity or transactions suspected of being linked to TFS as soon as possible without delay to the Centre in a report in terms of section 29 of the FIC Act. This include instances where a transaction was attempted but not completed.

64. Where there is a positive match with a designated person or entity, the accountable institution must freeze the property linked to the designated person or entity and file a TPR in terms of section 28A of the FIC Act with the Centre. The accountable institution must monitor the property of the designated person or entity. Where further transactions are attempted concerning the property, the accountable institution must file a report in terms of section 29 of the FIC Act.

65. Accountable institutions must report TPRs regardless of whether a transaction is not concluded. The mere attempt at making a transaction linked to a designated person or entity, warrants reporting of a TPR.

66. The importance of filing reports in terms of section 29 of the FIC Act, must be understood in the context of domestic referrals to the UNSC for possible UNSC designation. Where an accountable institution suspects that a person or entity may be involved in the financing of terrorism, proliferation of WMD or related activity, the accountable institution must report this to the Centre, providing as much information and use the most accurate report indicators.

Risk management and compliance programme

67. The accountable institution's RMCP must provide for the manner in which it will comply with its TFS obligations, including but not limited to:

67.1. The manner in which and processes by which it will scrutinise client information,
67.2. freeze designated persons and entities' property, and
67.3. The process for reporting to the Centre, include filing the TPR in terms of section 28A of the FIC Act, as well as filing a suspicious and unusual transaction/activity report, terrorist financing transaction report (TFTR) or terrorist financing activity report (TFAR) in terms of section 29 of the FIC Act, where there is a suspicion that a transaction or property may involve terrorist financing or proliferation financing.

PART B – RISK-BASED APPROACH TO COMBATING TERRORIST FINANCING

68. The accountable institution's RMCP must provide for the manner in which and processes by which it will identify, assess, monitor, mitigate and manage TF risks in terms of section 42 of the FIC Act. The accountable institution's risk-based approach to combating TF must be documented in its RMCP.

69. Accountable institutions must conduct business risk assessments, client level risk assessments, as well as new product and process risk assessments to identify and assess the risk of TF, and implement controls to monitor, mitigate and manage the risk of TF.

70. The Centre strongly encourages accountable institutions to consider the South African National Terrorism Financing Risk Assessment when developing its risk-based approach to CFT. Accountable institutions should consider sector risk assessments and the Centre's published case studies and indicators, when conducting TF risk assessments, which may aid in identifying areas of concern.

71. The accountable institution should gain an understanding of the relevant international, regional, and domestic terrorist organisations and/or extremist ideologies, this type of information should be factored into the accountable institution's risk assessment of the clients, business, as well as products and services offered.

72. When assessing the ML, TF, and PF risks, accountable institutions should consider the factors as set out in this PCC as well as Guidance Note 7. The TF risk factors as shown below are not an exhaustive list and accountable institutions may determine further risk factors. The accountable institution must be able to demonstrate that it considered risk factors unique to ML, TF and PF, although the risk assessments need not necessarily be separated.

Raising, moving, storing and using property for terrorist activity

73. To identify risks, the accountable institution should understand the manner in which terrorists raise, move, store and use property. TF usually takes place through three phases. All three phases constitute TF. The diagram below provides a broad outline of

some factors to consider, which include, but are not limited to, the terrorist financing phases.

Raising and sourcing of property	Moving of the property	Use of the property
Criminal activity – proceeds of crimes	Banks	Carrying out of attacks
Crowd-funding, donations from the public, charities, non-profit organisation, etc.	Money and value transfer service providers (both formal and informal)	Operational costs of terrorist organisations or persons, including business operating costs, housing, food, transport etc.
Abuse of business entities	Cash movement	Training costs
Abuse of non-profit organisations	Mobile money	Recruitment costs
Other avenues of raising funds	Crypto asset service providers	Arms and ammunition costs

*FATF report – Ethnically or racially motivated terrorism financing, June 2021. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html

Terrorist financing methods – raising finance for terrorism

74. With TF, the source of funds could be either legitimate or illegal. This is different to money laundering where the funds are always from the proceeds of crime. With money laundering, the knowledge and suspicion would predominantly be focused on the source of the funds which is illegal. To identify terrorist financing, accountable institutions must analyse both the source of funds, as well as the intended use of the funds.

75. An important part of combating TF is understanding the TF methods. In this way accountable institutions can proactively develop controls aimed at identifying transactions or activities that pose a heightened TF risk. The following financing methods are generally used to fund terrorism. Refer also to the FATF guidance on emerging terrorist financing methods:

75.1. Terrorists receive funds directly from private donors such as wealthy individuals or entities making direct donations. (e.g. caution should be exercised, for example, where funds are transferred from private, wealthy clients to high-risk geographic areas etc.).

75.2. Abuse of non-profit organisations (NPOs) for TF by a) diverting donations to illegitimate actors, b) criminally abusing legitimate NPOs c) establishing fake NPOs or d) affiliating terrorist organisations under names similar to legitimate NPO names, in high-risk geographic areas.

75.3. Organised crime and the proceeds of criminal activity used to fund terrorist activity. FATF has highlighted credit card fraud, smuggling of precious metals and stones as

well as drug trafficking as some of the predicate crimes where the proceeds of crime are channelled toward terrorist activity. The predicate crimes may vary and, therefore, constant analysis of emerging trends in this regard is recommended. Terrorists also loot and steal goods.

75.4. There may be instances where members of a terrorist organisation are charged membership fees, and certain communities may also be subject to a levy.

75.5. Fundraising events such as concerts or market days have been used by certain terrorists.

75.6. Diaspora or foreign émigré nationals who are from geographic areas with heightened TF risks face extortion by terrorists in their homes or countries of origin. Accountable institutions must conduct enhanced monitoring on cross-border transfers to high-risk geographic areas by such foreign nationals.

75.7. Kidnapping for ransom is another method used to raise funds by terrorists. Large amounts of cash are often transferred across borders to pay ransoms to kidnappers. Accountable institutions should consider as a red flag large cash withdrawals and negative media reports that highlight possible ransom payments.

75.8. Terrorists may also create legitimate businesses to generate proceeds which are then used in terrorist activity. The use of front or shell companies by terrorists poses a heightened TF risk. This highlights the importance of accountable institutions identifying and taking reasonable steps to verify beneficial owners. When funds are sent across borders in a manner that is not aligned to the business, this should raise red flags.

75.9. Fundraising through social media, crowd-funding platforms, public donations etc. Funds are raised on public platforms where clients publish account information or crypto addresses to solicit funds from the public. The accounts that receive such funds should be monitored for suspicious and unusual activity. Some typologies in this regard have shown that the terrorists publish their account information on public platforms but do not indicate the purpose for collecting funds. In this way, they attract funds without disclosing or attracting attention to their intended use of the funds.

*The method in which funds are raised, together with the geographic area the funds are destined for, are key risk factors the accountable institution must consider when assessing the risk of TF.

Moving terrorist finances

76. There are various ways in which funds are moved by terrorists which may include:

76.1. **Traditional banking** – Banks enable the fast transfer of funds, domestically and across borders. The large volume of transactions through the banking system often makes it difficult to identify small or negligible amounts destined for TF. An accountable institution's transaction monitoring therefore plays a pivotal role in the fight against TF. Refer to the Centre's Directive 5 read together with PCC 45.

Example – client profile monitoring is an important control in identifying suspicious and unusual transactions

Factors which accountable institutions can consider when assessing suspicious and unusual transactions, include but are not limited to, instances where various micro loans are obtained, the purchase of flight tickets to high-risk regions, the use of funds in and small transfers to or from high-risk geographic areas. Other indicators may be the use of cellular services to and from high-risk regions, which do not match the client's profile, and instances where the client is a South African national with no links to the foreign high-risk region.

Cellular service providers and airlines as businesses have an obligation in terms of section 29 of the FIC Act and are urged to file reports when they become aware of suspicious and unusual transactions.

76.2. **Money value and transfer services (MVTS)** are susceptible to abuse for TF, especially in high-risk geographic areas as more reliance is placed on these services due to the non-availability of formal banking. Accountable institutions must conduct enhanced monitoring of transactions made to high-risk geographic areas. A distinction should be drawn between formally registered and informal MVTS (e.g., hawaladars or others). The risk of TF increases when dealing with informal MVTS providers like hawaladars as there is a lack of regulatory oversight over these alternative or informal funds transfer service providers. Accountable institutions are encouraged to determine whether a client's transaction patterns are indicative that the client provides informal MVTS and apply enhanced monitoring to these client accounts. Activity indicating a client may be operating an informal MVTS includes pooling of funds

followed by large cross-border transfers. This type of activity should be considered a red-flag indicator. Accountable institutions should apply enhanced monitoring of MVTS transactions through high-risk corridors, which include high-risk geographic areas.

76.3. **Crypto currency** – New technologies including crypto assets are increasingly being used for TF due to the pseudonymous (e.g. transactions can be traced, but not the identity of the parties involved etc.) nature of the crypto assets, the ease of conducting domestic and cross-border transfers, and the fact that crypto transactions are subject to less scrutiny.

76.4. **Cash** – Cash payments enable anonymous transfers, are easily transferable, and leave no audit trail. Money mules, and cash couriers are often used by terrorists to transit funds. Transportation of cash to high-risk areas, numerous cash payments followed by transfers to high-risk geographic areas, and withdrawal of cash in high-risk areas that does not match the client's profile, may be indicators of possible TF. Cash-based economies enable anonymity and the risk of operation of terrorists within high cash-based geographic areas is heightened.

76.5. **Third party payment providers (TPPPs)** – Accountable institutions should remain aware of the potential abuse of TPPPs as intermediaries for MVTS transfers. The accountable institution should monitor transactions for red flag indicators, including:

- User or merchant device not recognisable
- Expiration of a device user's immigration permits or visas
- Beneficial ownership information is lacking
- Merchant devices have possibly been used by multiple individuals or more than one operator has access to device
- Excessive remittances over a short period
- Excessive remittances from the same geographical location, as it is common practice to rotate operation of the different "TPPPs"
- The entity's physical address is non-existent

76.6. **Alternative payment methods** – Including contactless payment, pre-paid cards, and mobile money face a heightened risk of being misused for TF. Accountable institutions should consider examples of how these types of payment methods have been misused or could potentially be exploited for purposes of TF, to identify controls aimed at mitigating the risk of TF.

Storing or using terrorist finances

77. Terrorist finances raised could be used for different purposes which include but are not limited to:

77.1. Supporting terrorists living costs, food, rental, mortgage, petrol, and operations costs.

77.2. Carrying out terrorist activity, the purchase of goods used for terrorist activity (Business entities that provide controlled goods or services must gain an understanding of the terrorist activity risks. Examples of dual-use goods include, but are not limited to, 3D printers, drones, audio visual components, navigation devices, recreational shooting ranges, chemical products, etc.)

77.3. Recruitment of new members for terrorism

77.4. Marketing expenses, spread of propaganda e.g. certain publications have been used for terrorism propaganda.

TERRORIST FINANCING RISK ASSESSMENT

78. When assessing TF risk, an accountable institution must consider what areas of their business are vulnerable to TF abuse (e.g. products, services, controls or employees etc.) and the consequences if the terrorist activity would take place through the use of the accountable institution.

79. The consequences of terrorist financing activities are devastating to accountable institutions directly and to the broader society. Accountable institutions should therefore implement the necessary controls required, to identify, assess, monitor, manage and mitigate TF financing risks.

80. Where there is a match against the TFS list, meaning the person is a designated person, a zero risk tolerance approach must be applied (a risk-based approach is not applicable in this instance). The accountable institution must freeze the property linked to that

designated person and file a section 28A report with the Centre. In comparison to the scenario where there is a suspected link to a designated person, which cannot be confirmed, the accountable institutions must apply a risk-based approach including robust controls to mitigate the TF risks.

81. Risks associated with TF are constantly changing, and accountable institutions must adapt their risk-based approach to ensure they are adequate to mitigate new and emerging TF risks.

Client risk factors

82. The outcome of scrutinising client information against the TFS list must be considered when assessing TF risk on a client level. Where a client is found to be designated on a TFS list, this would result in an automatic high-risk rating, and the accountable institution would have to freeze the client property and file a report to the Centre.

83. Different clients pose varying levels of TF risk. To risk rate clients from a TF perspective, the accountable institution should gain an understanding of the different types of:

83.1. Terrorists, terrorist organisations and geographic areas in which the terrorists operate

83.2. Terrorist behaviour, and terrorist ideologies

83.3. Client types including natural and juristic persons, including beneficial owners that are vulnerable to terrorist behaviour or adhering to terrorist ideology. Various client factors can be taken into account including, but not limited to, nationality, age, etc.

84. Trends have shown that terrorist organisations use complex legal structures to evade detection, highlighting the importance of identifying the beneficial owners of clients.

85. There are certain instances of state-sponsored terrorism, dealing with foreign politically exposed persons should be considered as high-risk for this reason, especially where the foreign politically exposed person is from a geographic area which poses a heightened TF risk.

86. Foreign terrorist fighters (FTFs) include natural persons who possibly act alone, or in small groups, as opposed to the larger more advanced terrorist organisations that

conduct terrorist activity. FTFs are based in various geographic areas. Developing a client profile which might mirror that of an FTF could aid in identifying TF risk and mitigating that risk.

87. A possible indicator that a person is a lone actor, self-radicalised individual or foreign terrorist fighter, includes where the person travels to or intends to travel to high-risk TF geographic areas. Accountable institutions may identify this red flag from transactional activity to and from that high-risk TF geographic area. As part of the planning or preparing for participating in or supporting a terrorist activity, lone actors, self-radicalised individuals, or FTFs draw funding from various sources (e.g. obtaining numerous credit loans with different institutions, possibly defaulting on repayments, in a short period of time, followed by transfers to high-risk TF geographic areas etc.).

88. Nationals from geographic areas associated with or susceptible to terrorism pose a heightened risk for TF, especially where such a client(s) submits funds back to their country of nationality. Where an accountable institution identifies fraudulent use of identity, visa, permit documents etc., this might be a red flag indicator in combination with other sets of facts of possible TF.

89. Certain sectors are high risk from a TF perspective (e.g. trading in precious metals and stones etc). Accountable institutions may consider conducting enhanced due diligence and request further certifications relating to the relevant trade.

Geographic risk factors

90. A holistic assessment of TF risk must be conducted by the accountable institution, taking into account international risks, risks on a regional level and risks on a domestic level. Accountable institutions should consider regional TF hotspots and developments in countries bordering South Africa.

91. Refer to PCC 49 for further guidance on geographic area risks. Accountable institutions are required to assess the inherent TF risk of a geographic area. FATF guidance, open-source information on terrorism, international case studies, regional conflict zones, academic publications, adverse media reports, credible third-party publications and political instability should be considered in this regard.

92. There are geographic areas that pose a heightened risk of TF due to funds and resources being diverted through these areas to other geographic areas where terrorism occurs. These geographic areas pose a heightened risk for potential TF financing due to their proximity to countries where terrorism occurs, infrastructure and financial systems could be exploited by terrorists.

93. According to the *South African National Terrorism Financing Risk Assessment*, the country faces TF risk, due to:

93.1. The presence of FTFs and persons returning from high-risk geographic areas where terrorism occurs

93.2. The support for foreign terrorist organisations

93.3. The solicitation of support within South Africa and using the country as a transit hub and base for planning and logistics of terrorist attacks

93.4. Further growing regional terrorist attacks, and threats of retaliation should South Africa act with regard to regional terrorist activity, and

93.5. The country's porous borders.

94. Geographic areas with high levels of organised crimes, are susceptible to TF risk.

Products and services

95. Different business units within accountable institutions face different levels of TF financing risk. The accountable institution must assess the TF financing risk, each business unit faces. The following are examples of products and services that may pose a heightened risk of being used for TF:

95.1. Cash intensive products

95.2. Products that provide cross-border transfer of funds

95.3. Trade finance products

95.4. Product or services that enable easy transfer of funds.

PART C – RISK-BASED APPROACH TO COMBATING PROLIFERATION FINANCING

96. The accountable institution's RMCP must provide for the manner in which and processes by which it will identify, assess, monitor, mitigate and manage PF risks in terms of section 42 of the FIC Act. The accountable institution's risk-based approach to combating PF must be documented in its RMCP.

Risk-based approach

97. In addition to the TFS obligations to scrutinise, freeze and report, the Centre recommends that an accountable institution should adopt a risk-based approach to ensure sufficient resources are focused on heightened risks of PF. This could enhance the accountable institution's ability to apply the broader activity-based financial sanctions.

98. Accountable institutions should conduct business risk assessments, client level risk assessments, as well as new product and process risk assessments to identify and assess the risk of PF, and implement controls to monitor, mitigate and manage the risk of PF.

Heightened proliferation financing risks

99. A key risk relating to PF, is the evasion of TFS through the use of legal persons. Designated persons or entities employ different methods in their attempts to avoid detection, or distance themselves from certain transactions, and often attempt to hide behind legal persons, trusts and partnerships. Shell or front companies are used to obscure either the identity of the beneficial owner, the goods and activities being provided, or the geographic area to which goods or activities are destined.

100. A second key PF risk relates to the particular industry in which a client operates and the associated nature of the client's goods and activities offerings. This risk can be further heightened given the nature of the accountable institution's product offering in support of their clients. A third key PF risk area is the provision of trade finance in facilitating international trade, especially in respect of dual used goods that can be used for the proliferation of WMD.

101. In addition to the risk factors as set out in the Centre's Guidance Note 7, when assessing the inherent risk of PF, the accountable institution should have regard to the risk factors described in this PCC, and any other additional risk factors deemed relevant. The list below is not an exhaustive and accountable institutions may consider other risk factors.

Client risk factors

102. Whether any person including the client, the person acting on behalf of the client, beneficial owner, or party to a transaction is a:

102.1. Designated person or entity (this would be a clear indicator that the business relationship or single transaction poses a high PF risk)

102.2. National of or based in a geographic area that is subject to PF TFS (e.g. consider UNSCR 2397(2017), which requires member states to repatriate income earning North Koreans that are listed in the resolution, with few exemptions); or

102.3. National of or based in a geographic area that is a concern due to possible diversion of funding or resources to a PF TFS country.

103. The client, beneficial owner, or person acting on behalf of the client is a foreign prominent influential person, high-risk domestic prominent influential person or government entity dealing in a high-risk sector such as arms and ammunitions or trading in other controlled goods and activities (dual-use goods or technology).

104. The client is represented by a third party in a manner that is not aligned to the client profile or that does not make business sense or seems unnecessary. Where there is an unusual or unexplained third party acting on behalf of the client this may be an indicator of a high-risk transaction.

105. The client's legal structure appears overly complex, which may be an attempt to hide beneficial owners that are subject to PF TFS.

106. The client is a legal person but functions as a shell or front company and does not have actual operations in an industry. That may indicate a heightened PF risk. Some indicators of shell or front companies include but are not limited to: unrelated

companies that have the same employees, and often transact with one another, unrelated companies that share the same addresses, phone numbers or similar registration information and transact with the same third parties, there is a notable lack of online presence, where a large entity has no website, and the entities name is very generic and could easily be mistaken for another well-known entity.

107. The use of joint ventures by legal persons to evade TFS (e.g. consider UNSCR 2375 (2017), which requires member states to prohibit joint ventures with North Korea, with few exemptions).

108. There are clients who offer certain products and services that face a heightened risk of being abused for PF. Examples of these may include but are not limited to import and export businesses (e.g. freight forwarders, airlines, road couriers, warehouses, vessels, shipping companies, maritime companies, clearing agents, import and export insurance companies, credit and insurance providers, among others), ports of entry, chemical manufacturing companies, precious metal dealers, as well as arms and ammunition manufacturers.

109. The nature of the client's business, including the industry in which the client operates, or the type of products and services the client provides are linked to controlled goods and activities (dual-use goods).

110. Where a client deals in controlled goods or activities and does not have approval from the relevant regulatory authority to do so, this may be an indicator that that client poses a heightened PF risk.

Controlled goods and activities

Accountable institutions are urged to consult and scrutinise the list of controlled goods and activities as published by the South African Council for the Non-Proliferation of Weapons of Mass Destruction (Non-Proliferation Council), which may serve as a guide to accountable institutions for purposes of determining and assessing the PF risks relating to the client's sector, and the goods and activities in which the client deals.

Controlled goods and activities include goods that have "*dual-purpose capabilities" relating to technology, expertise, service, material, equipment and facilities 'which' can contribute to the proliferation of weapons of mass destruction, but which can also be used for other purposes, including conventional military, commercial or educational use*[3]*"* (e.g. include technologies like drones).

The NPWMD offers guidance products available on the Non-Proliferation Council's website for further information.

There are various other lists that may apply, given the parties to a transaction and correspondent obligations. In addition, the UNSC publishes a list of prohibited items.

List of sources of controlled goods, activities and/or dual-use goods

http://non-proliferation.thedtic.gov.za/

https://www.un.org/securitycouncil/sanctions/1718/prohibited-items

https://www.gov.za/sites/default/files/gcis_document/201409/35272gon321.pdf

Geographic area risk factors

111. The geographic area in which either the client, the person acting on behalf of the client, beneficial owner, or persons who are party to the transaction are based is a geographic area that is:

111.1. Subject to PF TFS (e.g. the Democratic Republic of Korea (DPRK) or North Korea is specifically listed as being high-risk for PF concerns). The Centre's PCC 49 provides further guidance on geographic risks.

111.2. An area of concern due to the diversion of funds or resources to a geographic area subject to PF TFS (e.g. where the country is not listed but supports or aids sanctioned countries), also consider the proximity to the high-risk geographic area; or

111.3. An area of concern due to weak AML, CFT and CFP laws or export control laws and enforcement.

[3] The Non-Proliferation of Weapons of Mass Destruction Act 87 of 1993

112. Controlled goods and activities that are provided to geographic areas that do not seem to have the required skill or technology to deal with the controlled goods and activities, is a red flag indicator of possible evasion of TFS.

Product risk factors

113. There are certain product risk factors that could increase the vulnerability of accountable institutions and could result in heightened PF risks. These may include:

113.1. **Trade finance** which involves the financing of the import and export of goods and can include controlled goods or activities.

113.2. Trade finance transactions may be complex and involve the movement of funds to or from geographic areas that present a high PF risk.

113.3. There are various parties to a trade finance transaction who may be subject to PF TFS. The use of front or shell companies by bad actors in trade finance arrangements remains a heightened risk.

113.4. There are various trade finance transaction red flag indicators which include but are not limited to inconsistencies in information or documentation provided, false documentation, over-invoicing, under-invoicing, and circular types of transactions where the beneficiary turns out to be the originator of that same transaction.

113.5. Accountable institutions should gain an understanding of the trade patterns and the sector's high-risk geographic areas to better understand and mitigate the risks (e.g. North Korean front companies may deal in certain import and export of textiles, garments, fish, other seafood industries, etc.).

Example – Abuse of trade finance transactions for PF

Bank Y is financing a trade agreement where, following the review of the bill of lading, it is found that the shipping vessel is subject to PF TFS. Bank Y's client is not a designated person or entity, however, the agreement will financially benefit a designated entity. Therefore, Bank Y cannot proceed with the payment.

114. **Correspondent banking** which is the provision of banking services by one bank to another bank, and services include international transactions and cash management. An accountable institution should assess whether their correspondent bank operates in

or has any links to geographic areas with heightened PF risks, or links to persons including beneficial owners who are designated persons or entities. Accountable institutions should understand the controls the correspondent bank has in place to combat PF.

115. **Foreign exchange** which refers to the conversion of one country's currency into another country's currency. Where foreign exchange payments are made to or received from countries that pose a heightened PF risk, accountable institutions should consider the risk of possible evasion of TFS.

116. **New technologies** including crypto assets are increasingly being used for PF due to the pseudonymous nature of the crypto assets, the ease of domestic and cross-border transfer, and the fact that crypto transactions are subject to less scrutiny.

117. **Cash payments** as it enables anonymous transfer of funds, is easily transferable and leaves no audit trail. For these reasons cash payments to or from accounts of clients that pose a high risk from a PF perspective, is a red flag.

Other risk factors

118. False documentation or documentation that seems unusual could indicate an attempt to evade sanctions. Criminals often attempt to obscure the true nature of goods, destination of goods, beneficiary, the originator, intermediary or vessel etc. through false documentation.

119. Adverse information relating to PF on the end use and end user of the controlled goods and activities.

120. Deceptive shipping practices which include but are not limited to:

120.1. Altering vessel names and numbers to conceal identity,

120.2. Conducting ship to ship transfers at sea, of controlled goods

120.3. Disabling or manipulating the shipping vessel's identification systems, so that vessel movement is not tracked.

121. Supply chain risks include but are not limited to:

121.1. Instances where suppliers outsource work to high-risk geographic areas without informing parties to the supply contract.

121.2. Excessive pricing in the form of low prices by high-risk entities

121.3. Sale of information technology goods and services from high-risk geographic areas or entities, which goods or services can be used for military and law enforcement purposes.

Customer due diligence

122. Information on who has approval to deal in controlled goods and services is not made available publicly. This information is held confidentially by the relevant regulatory bodies. Accountable institutions are encouraged to enquire from their clients who deal in controlled goods or activities, whether the client has approval from the relevant regulatory body (e.g. Non-Proliferation Council) and request a copy of such approval from the client.

Example – Enhanced due diligence for controlled goods and activities

Upon processing a trade finance transaction, Bank A becomes aware that the transaction involves controlled goods and activities. As part of Bank A's risk-based approach, it requests a self-declaration from the client, to determine whether or not the client is authorised to transact in the controlled good or activities.

123. Where a client poses a higher PF risk, an accountable institution must conduct enhanced due diligence, and is encouraged to obtain the following additional information:

123.1. Immediate family members and known close associates

123.2. Past nature of business or occupation

123.3. Information on financial statements

123.4. Information available in media, and the internet

123.5. Information on the end use and end users of the controlled goods and activities; and information of the authorisation of the end user, and intermediaries to the transaction. *This list of additional information is not exhaustive.

124. It is critical for an accountable institution to conduct ongoing due diligence and enhanced account monitoring on high-risk business relationships. This includes assessments of transactional information and documentation to be able to identify suspicious and unusual transactions and activities, including possible PF or evasion of PF controls and PF TFS.

125. As part of ongoing due diligence, an accountable institution should analyse whether transactions processed for clients presenting a heightened PF risk are consistent with any permits or authorisation issued to that client, and other documentation that forms part of the transactions.

126. When assessing a high-risk transaction, an accountable institution should request additional client, transactional and end-user information as is necessary, so as to not breach TFS obligations. The additional information may include but is not limited to the beneficial ownership information of all the parties to the transaction and end users.

127. Where additional information is required to clarify whether or not a transaction poses a PF risk, and such information is not provided, the accountable institution should consider submitting a report in terms of section 29 of the FIC Act.

128. The accountable institution may also scrutinise the client information against the TFS lists more frequently.

PART D – DE-RISKING

129. In addition to the principles as set out in Guidance Note 7, it is not considered effective or adequate risk management if an accountable institution decides to de-risk a client for the mere fact that the business relationship or single transaction with the client poses a heightened PF or TF risk. When dealing with designated persons or entities directly or indirectly, however, the accountable institution must freeze and report in compliance with its TFS obligations.

130. It is the Centre's view that where an accountable institution de-risks solely based upon the fact that there is a heightened risk, then that accountable institution has not complied with its obligation to follow a risk-based approach.

131. Where an accountable institution takes the decision to not onboard a certain category of clients, the accountable institution must be able to demonstrate the application of a risk-based approach in terms of which risk factors have been considered.

132. Ineffective application of de-risking can cause inadvertent consequences including the loss of valuable information through regulatory reporting to the Centre.

133. Accountable institutions are reminded of their obligations not to tip off a client where suspicious and unusual activity is suspected. Where a person or entity is designated on a TFS list, the person or entity would in all probability be aware of the designation, in this regard, freezing the client's property would not amount to tipping the client off that they are listed on a TFS list.

134. An accountable institution must not process transactions where they are unable to determine accurately whether such transactions would breach TFS obligations. Where the accountable institution is uncertain whether a person or an entity is a designated person or entity, the accountable institution may seek independent legal advice.

Issued By:

The Acting Director Financial Intelligence Centre

29 February 2024

Resources

- Financial Action Task Force Recommendations
- Financial Action Task Force, International best practices – Targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6), June 2015
- Financial Action Task Force, Guidance on Counter Proliferation Financing the Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, February 2018
- Financial Action Task Force, report – *Ethnically or racially motivated terrorism financing*, June 2021
- HM Treasury, Office of Financial Sanctions Implementation – UK Financial sanctions. General guidance for financial sanctions under the Sanctions and Anti-money Laundering Act 2018, August 2022
- HM Treasury, Office of Financial Sanctions Implementation – Maritime Guidance, December 2020
- HM Treasury, Office of Financial Sanctions Implementation – Importers and Exporters – Financial Sanctions frequently asked questions, December 2020
- HM Treasury, Office of Financial Sanctions Implementation – Charity sector guidance, December 2020