



17 June 2022

To: All Regulated Entities

Supervisory Issues and Information Circular

Re: 2021 Review of TCSPs Compliance with AMLRs: Sanctions Screening Policies and Procedures

1. Trust and Corporate Services Providers ("TCSPs") use, establish and/or act for legal persons and arrangements on a regular basis and are ideally placed to help prevent their potential misuse. This includes ensuring that their clients – whether fund vehicles, virtual asset service providers, correspondent banks or other legal persons and arrangements - are not subject to, or seeking to circumvent, targeted financial sanctions ("TFS"). TFS are restrictive measures put in place to limit the provision of certain financial services and/or restrict access to financial markets, funds and other assets to persons or entities designated under the TFS regime.
2. TFS have always been an integral part of global efforts to prevent financial crime but following the military invasion of Ukraine by Russia earlier this year, new persons linked to the Russian government were designated by the United Kingdom, European Union, United States of America, Canada, and other countries, under their respective TFS regimes. The HM Treasury Office of Financial Sanctions Implementation ("OFSI") issued several notices that apply to obliged entities, including TCSPs and other financial institutions in the Cayman Islands.
3. When establishing a business and on an ongoing basis, TCSPs are required by the Anti-Money Laundering Regulations (2020 Revision) ("AMLRs") to assess whether the client, its directors, shareholders, beneficial owners, and other related parties are, or are involved with, persons or entities designated under the TFS applicable in Cayman Islands. Upon identification of such persons or entities, TCSPs and other financial institutions are required to freeze such accounts, funds or economic resources and report to the Governor, through the Financial Reporting Authority ("FRA"). Failure to comply with the above is a serious criminal offence. The FRA has the power to levy civil monetary penalties for breaches of financial sanctions¹. The FRA/Governor will also work with the Cayman Islands Bureau of Financial Investigation where criminal prosecution may be considered.
4. The Cayman Islands Monetary Authority ("CIMA") or (the "Authority") is not responsible for enforcing TFS measures. However, where the Authority identifies failings in TFS policies and procedures it can impose restrictions and/or take enforcement action. The compliance

¹ Schedule 4A of the Terrorism Act and Section 2D of the Proliferation Financing (Prohibition) Act

frameworks of TCSPs should therefore meet the TFS obligations set out in the AMLRs and the AML Guidance Notes².

5. This 2021 TCSP Sanctions Circular (the "Circular") outlines the findings of CIMA's assessment of compliance by TCSPs with TFS under Regulations 5 & 12 of the AMLRs during the year 2021, and the AML/CFT/CPF controls required to be undertaken to address the identified deficiencies.
6. TCSPs should take note of this Circular and ensure that their own sanctions policies, procedures, systems, and controls are of an appropriate standard. Not only will this enable TCSPs to deepen their understanding of how designated persons may use legal persons and arrangements to circumvent TFS, but it will also help reduce the risk of sanctions non-compliance, for which there are serious criminal penalties.

Scope of Review

7. The Authority considered the results of 27 inspections of TCSPs conducted during 2021 and assessed the levels of sanctions compliance at customer onboarding and during the course of business. A total of 567 client files were reviewed during the inspections. The scope and methodology is set out in Annex 1. Specifically, CIMA assessed the levels of compliance by TCSPs against the following provisions of the AMLRs:
 - a) Regulation 5(a)(v) of the AMLRs: A person carrying out relevant financial business shall maintain as appropriate, having regard to the money laundering and terrorist financing risks and the size of its business, **adequate systems to identify risk** in relation to persons, countries and activities which shall include **checks against all applicable sanctions lists**.
 - b) Regulation 5(a)(viii) of the AMLRs: A person carrying out relevant financial business shall maintain as appropriate, having regard to the money laundering and terrorist financing risks and the size of its business, **procedures for the assessment of one-off transactions and the ongoing monitoring of business relationships** for the purposes of preventing, countering, and reporting money laundering, terrorist financing and proliferation financing, and such procedures **allowing for the identification of assets subject to targeted financial sanctions** applicable in the Islands.
 - c) Regulation 5(a)(viii) of the AMLRs: A person carrying out relevant financial business shall maintain as appropriate, having regard to the money laundering and terrorist financing risks and the size of its business, **procedures to ensure compliance with targeted financial sanctions obligations** applicable in the Islands.
 - d) Regulation 12(1)(e)(i) of the AMLRs: A person carrying out relevant financial business shall **conduct ongoing due diligence on a business relationship including scrutinising transactions** undertaken throughout the course of the business relationship to ensure that transactions being conducted are consistent with the

² Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands

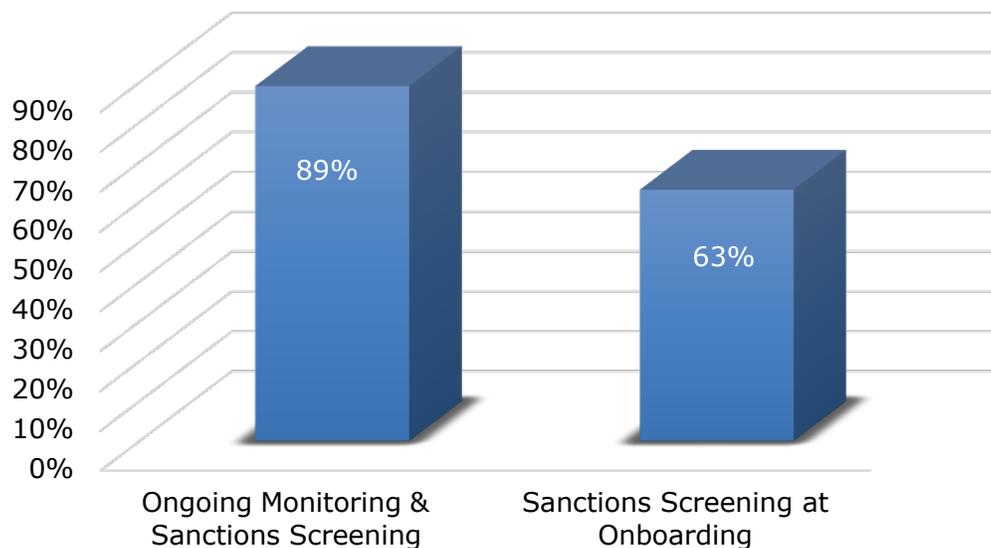
person's knowledge of the customer, the customer's business, and risk profile, including where necessary, the customer's source of funds

- e) Regulation 12(1)(e)(ii) of the AMLRs: A person carrying out relevant financial business shall **conduct ongoing due diligence on a business relationship** including ensuring that documents, data or information collected under the customer due diligence process is kept current and relevant to customer due diligence, by reviewing existing records at appropriate times, taking into account whether and when customer due diligence measures have been previously undertaken, **particularly for higher risk categories of customers**.

Executive Summary

8. The Authority acknowledges the progress that TCSPs have made in applying TFS screening measures, and notes that the majority of TCSPs have adequate policies and procedures in place for TFS:

Percentage of TCSPs with Adequate AML/CFT Policies & Procedures



9. However, the Authority also observed that policies and procedures were not always being effectively implemented in practice:
- a) **Overall effectiveness of implementation:** Only 26% of the TCSPs inspected were effectively implementing their TFS screening policies and procedures across all the client files reviewed. The remaining 74% had at least one client file with weaknesses around TFS screening of clients (and their related parties) at onboarding or on a periodical basis.

- b) **TFS screening not conducted for at least one client or associated party:** 15% of the files reviewed showed instances where at least one client or associated party was not screened for TFS during the conduct of customer due diligence at onboarding. Neither were they screened on a periodical basis, and whenever there was an update of the TFS list by HM Treasury.
 - c) **TFS screening not performed at client onboarding:** 14% of the files reviewed showed instances where TFS screening was not performed at the time of onboarding. The TFS screening process was done after the business relationship was already established.
 - d) **TFS screening not documented on client files:** 11% of the files reviewed showed instances where the TCSP was in fact screening its clients against relevant TFS lists but had at least one client where the records of the TFS screening were not documented and retained in the client file.
 - e) **TFS screening not conducted through ongoing monitoring or periodic review:** 5% of the files showed instances where the TCSP was not TFS screening during ongoing monitoring and/or through client file reviews on a periodic basis or whenever there was an update of the TFS list.
 - f) **Periodic reviews were not conducted in a timely manner, in accordance with the clients' business and risk profile:** 14% of the files reviewed showed instances where the TFS screening was subject to some level of review, but not in accordance with the clients' business and risk profile so that the client's documents, data, or information was kept current and relevant.
 - g) **TFS screening results not documented:** 1% of the client files lacked documentation to show how they treated positive and/or false positive hits flagged by their TFS screening IT systems.
10. The Authority has already taken prompt and robust steps to remedy TFS non-compliance by TCSPs, including issuing requirements and (in some cases) initiating enforcement action. TCSPs subject to requirements are required to remediate within prescribed timeframes and are monitored by the Authority.
11. Nevertheless, all regulated entities should note the TFS deficiencies identified by the Authority and ensure that they are in compliance with the AMLRs and AML Guidance Notes. Failure to comply with provisions of the AMLRs and AML Guidance Notes may result in the Authority taking action, including enforcement, where appropriate and proportionate.

Findings of the 2021 Review

TFS Screening at Onboarding - Policies and Procedures

12. Regulation 5(a)(v) and (viii b) of the AMLRs, and Part II, Sections 13, 14, 15 of the AML Guidance Notes outlines the requirements for TFS compliance policies, procedures, systems, and controls.

13. Under these regulations and guidelines, TCSPs are required to screen their customers and/or relevant parties or transactions to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country.
14. The 2021 review noted that 63% of TCSPs inspected had AML/CFT and Sanctions policies which adequately provided for procedures to implement TFS screening at client onboarding. The remaining TCSPs did not include provisions for:
 - a) Ensuring that clients are adequately screened against all TFS lists applicable to the Cayman Islands.
 - b) Keeping track of all TFS lists (and updates) applicable to the Cayman Islands.
 - c) Ensuring that relevant parties involved in the business relationship are adequately screened against all TFS lists applicable to the Cayman Islands, irrespective of the client risk rating.
 - d) Managing how false positive and potential matches are addressed, including the escalation process and the timeframe for clearing these matches.
 - e) Filing a Compliance Reporting Form (CRF) when making a report to the Financial Reporting Authority.

TFS Screening at onboarding – Implementation

15. Regulation 5(a)(v) of the AMLRs requires TCSPs and other financial service providers to maintain procedures on the need for their businesses to have adequate systems to identify risk in relation to persons, countries and activities which include checking against all applicable TFS lists.
16. Part II, Section 13(B)(4) of the AML Guidance Notes also states that TCSPs and other financial service providers shall screen applicants, customers, beneficial owners, transactions, service providers and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant TFS lists, TCSPs may discover that certain TFS are applicable to one or more of their customers, existing or new.
17. Of the client files reviewed during the inspections, 42% demonstrated weaknesses in TFS screening at onboarding, including:
 - a) No evidence of TFS screening being carried out for the corporate clients, directors, protector of a trust client, and other principal parties to determine (in a timely manner) whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person / country (15% of the files reviewed)

- b) TFS screening was being done for the corporate clients and principal parties, but the results were not adequately evidenced on the client files (11% of the files reviewed).
- c) TFS screening was being done, but only in response to the inspection team's enquiries rather than at the onboarding or ongoing monitoring stage (5% of the files reviewed).
- d) TFS screening was being done, but this was after client acceptance and was never subject to ongoing monitoring procedures and/or periodic reviews (14% of the files reviewed).
- e) No evidence of how hits provided by the screening software were being resolved (1% the files reviewed).

TFS Screening as part of Ongoing Monitoring - Policies and Procedures

- 18. Regulation 5(a)(viii) of the AMLRs stipulates that a person carrying out relevant financial business shall maintain as appropriate, procedures for the ongoing monitoring of business relationships or one-off transactions for the purposes of preventing, countering, and reporting money laundering, terrorist financing and proliferation financing and such procedures allowing for the identification of assets subject to TFS applicable in the Islands.
- 19. The Review noted that 89% of the TCSPs had adequate AML/CFT and Sanctions policies for TFS screening for the ongoing monitoring of business relationships or one-off transactions covered provisions of regulation 5(a)(viii) of the AMLRs. The remaining TCSPs did not include provisions for:
 - a) Conducting periodic reviews of its TFS screening lists to ensure compliance with the TFS requirements in force in the Cayman Islands.
 - b) Keeping track of all the applicable TFS, and where the TFS lists are updated, ensure that existing customers are not listed.
 - c) Implementing adequate risk-based procedures regarding periodic reviews or re-assessments.

TFS Screening during Ongoing Monitoring - Implementation

- 20. Under the regulations 5(a)(v) and 12(1)(e)(i) & (ii) of the AMLRs, FSPs (including TCSPs) are required to have adequate systems to identify risk in relation to persons, countries and activities which shall include checks against all applicable TFS lists, and conduct ongoing due diligence, which include scrutinising transactions undertaken throughout the course of the business relationship, and ensuring that documents, data or information collected under the customer due diligence process is kept current and relevant to customer due diligence.
- 21. Of the client files reviewed during the inspections, 20% demonstrated weaknesses in TFS screening during ongoing monitoring, including:

- a) No evidence of ongoing monitoring or client file reviews being conducted on a periodic basis, or whenever there was an update of the TFS lists (5% of the client files reviewed).
- b) Although there was some evidence that reviews were being done, there was no evidence to show that these were conducted in a timely manner, in accordance with the clients' business and risk profile, so that the client's documents, data, or information was kept current and relevant (15% of the files reviewed).

Conclusion and Recommendations

- 22. The majority of TCSPs examined by CIMA had adequate policies and procedures for TFS screening and ongoing monitoring, but the Authority identified weaknesses in implementation. Clients (and their associates and service providers) should always be screened against the TFS lists applicable to the Cayman Islands, both at onboarding and on an ongoing basis to determine whether the TCSP is conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country.
- 23. Where there is a true match or suspicion, TCSPs are required to take the necessary steps to comply with the TFS obligations, including filing of compliance reporting forms to the FRA. TCSPs are also required to consider whether it is appropriate to file a suspicious activity report with the FRA, and document all the actions undertaken to comply with the TFS regime, and the rationale for each action.
- 24. TCSPs should further document and record all the actions that were taken to comply with TFS, and the rationale for each such action. In the event of updates to the relevant TFS lists, TCSPs may discover that certain TFS are applicable to one or more of their customers, existing or new.
- 25. It is also important that TCSPs provide adequate TFS related training to their staff and periodically assess their AML/CFT compliance programmes to ensure that they are commensurate with the nature, size, and complexity of the businesses.
- 26. TCSPs should take note of these findings and take appropriate measures to ensure that their own AML/CFT compliance frameworks meet the prescribed standards. CIMA will continue to promote and implement its supervisory mandate through offsite monitoring and onsite inspection processes.
- 27. Where deficiencies were found, the relevant TCSPs have been directed to remediate the identified deficiencies in a timely and thorough manner. The Authority will closely monitor requirements and TCSPs are reminded that any breach of the AMLRs, or non-compliance with the AML Guidance Notes or Statement of Guidance may result in an enforcement action, which can also include, or be in addition to, the imposition of an administrative fine.

Annex 1

Scope and methodology for the Inspections

1. The 2021 TCSP Sanctions Circular was compiled through data obtained from onsite AML/CFT/CPF and Sanctions inspections during the year 2021, where final inspection reports had been issued by November 2021. This amounted to 27 different regulated entities and 567 customer files.
2. As part of the onsite inspection process, the sample population of 567 customer files were reviewed across all the selected TCSPs. The files were randomly selected and were not based on the risk type of the customers.
3. The Authority assessed each file against various elements of the AMLRs, including compliance with regulation 5 and 12 of the AMLRs. It considered the adequacy of information obtained on TFS screening carried out at or after client onboarding; and ongoing monitoring procedures and processes undertaken in the TFS screening regime, including TFS screening done as part of transaction monitoring and periodic review.
4. Percentages for findings provided in this document are expressed as out of the total number of 27 entities inspected and 567 files reviewed.

The Authority also prepared individual reports for the TCSPs subjected to inspections in 2021.

References

FSPs are encouraged to review the links below which provide further guidance on the subject matter:

1. [Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands](#)
2. [FATF Targeted Financial Sanctions Related to Terrorism and Terrorist Financing \(Recommendation 6\)](#)
3. [UK Financial Sanctions: General Guidance - December 2020](#)
4. [AML/CFT Activity Report 2020](#)
5. [The Anchor](#)
6. [FATF - Misuse of Corporate Vehicles including Trust and Company Services Providers - October 2006](#)
7. [FRA Financial Sanctions Guidance - February 2020](#)