



19 January 2022

To: All Licensees

Supervisory Issues and Information Circular

Re: 2021 Review of TCSPs Compliance with AMLRs: Customer Verification and Identity

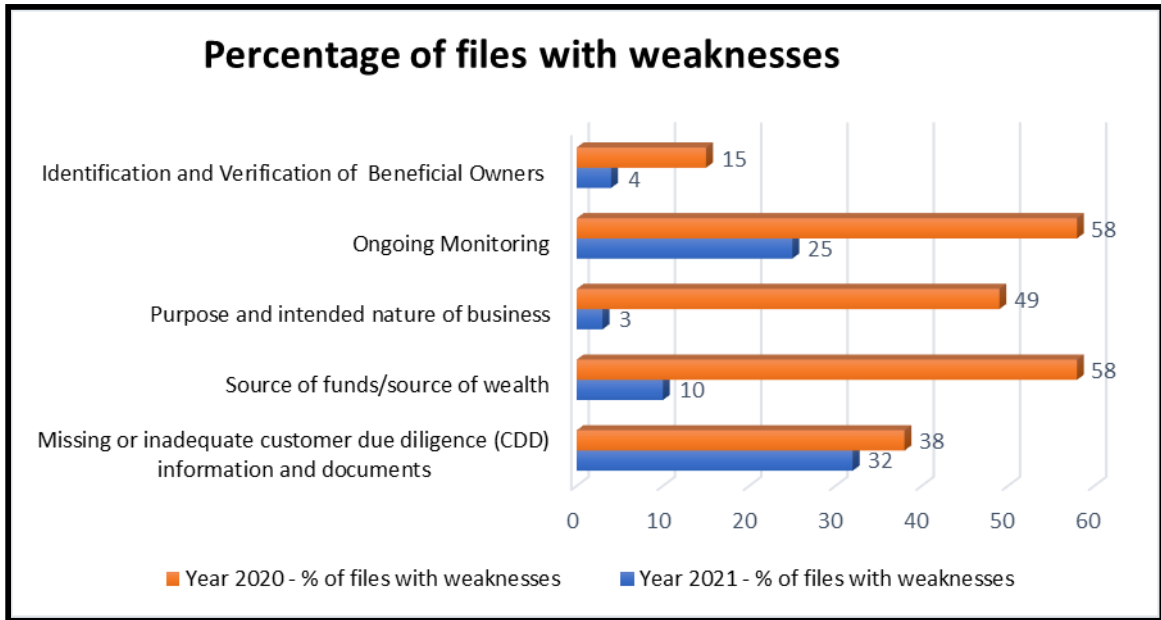
Introduction

1. Trust and Corporate Services Providers ("TCSPs") use, establish and/or act for legal persons and arrangements on a regular basis and are therefore important gatekeepers in the fight against financial crime. They are ideally placed to collect due diligence information, observe the behaviour and activities of beneficial owners and enquire and evaluate the rationale of prospective and ongoing business activities, helping to reduce the potential misuse of legal entities. However, they may also be vulnerable to abuse by criminals seeking to conceal the source of their illicit funds or the destination of the funds.
2. In 2020, the Cayman Islands Monetary Authority ("CIMA" or "the Authority") conducted a Focused Thematic inspection of a selected group of TCSPs ("2020 Thematic Review") to assess their compliance with regulation 12 of the Anti-Money Laundering Regulations (2020 Revision) ("AMLRs"), which relates to customer due diligence, identification of beneficial owners, purpose and intended nature of the business relationship, and source of funds.
3. Some of the major gaps identified during the 2020 Thematic Review included:
 - a) Failure to maintain accurate and up to date information, including information on beneficial owners and controllers; and
 - b) Inadequate implementation of ongoing monitoring procedures to foster greater visibility of business relationships and identify trends of misuse of legal persons and arrangements.
4. In 2021, the Authority continued its programme of anti-money laundering ("AML")/ countering the financing of terrorism ("CFT")/ countering proliferation financing ("CPF") and sanctions onsite inspections to assess compliance by TCSPs with statutory requirements. This included an assessment of the sector's compliance with regulation 12 of the AMLRs.
5. This Circular (the "2021 Review") sets out a comparison of the 2020 Thematic Review findings with 2021 onsite inspection findings, using data from 359 client files. These were reviewed pursuant to 16 different inspections (see Annex 1).

6. During the 2021 Review, the Authority observed notably fewer deficiencies than when compared to the 2020 Thematic Review. These results are encouraging, showing a significant improvement in compliance by TCSPs with regulation 12 of the AMLRs.
7. However, areas of concern remain, including deficiencies around the quality of customer due diligence (“CDD”) documentation and ongoing monitoring. The 2021 Review highlights the AML/CFT measures TCSPs and other financial service providers need to undertake to effectively implement the requirements under regulation 12 of the AMLRs, including under Part IV (CDD), Part V (simplified CDD) and Part VI (enhanced CDD).
8. The Authority continues to remind all TCSPs of their regulatory obligations to adhere to AML/CFT/CPF legislation, regulatory rules and/or statements of guidance, and ensure that their own policies, procedures, systems, and controls are of an appropriate standard. In doing so, TCSPs will deepen their understanding of how criminal activities are/can be perpetrated using legal persons and arrangements and will be able to reduce the risks of their businesses being abused by criminals.

Executive Summary of the 2021 Review

9. TCSPs demonstrated a significant improvement in compliance with regulation 12 during the period under review. There was a clear decline in the number of files that had weaknesses between 2020 and 2021: Indeed, the number of files with weaknesses was 69% less in 2021 than in 2020 (from an average of 46% to 14%).
10. Whilst weaknesses in the implementation of provisions of regulation 12 of the AMLRs still exist within the TCSPs, effectiveness in the implementation of regulation 12 has clearly improved.
11. The 2021 Review identified the following weaknesses, specifically:
 - a) **Identification and verification of the identity of Ultimate Beneficial Owners (“UBOs”) & Authorised Persons:** 4% of the files reviewed across the sector showed weaknesses of TCSPs not adequately identifying and verifying the identity of beneficial owners and authorized persons, using relevant information or data obtained from reliable sources. In 2020, 15% of files reviewed indicated this weakness.
 - b) **Ongoing Monitoring:** 25% of the files reviewed indicated weaknesses of TCSPs’ monitoring systems to effectively scrutinise transactions undertaken throughout the course of the business relationship and ensure that transactions being conducted are consistent with the customer’s business and risk profile, and source of funds. In 2020, 58% of files reviewed indicated this weakness.
 - c) **Purpose and intended nature of business:** 3% of the files reviewed indicated weaknesses in relation to the recording of information on the nature or purpose of the business or insufficient documentary evidence to confirm that the TCSPs have insight on the purpose and intended nature of the business relationships. In 2020, 49% of files reviewed indicated this weakness.
 - d) **Source of funds/source of wealth:** 10% of the files reviewed indicated weaknesses in gathering and maintaining information on the customer’s source of funds/source of wealth or maintaining supporting documents to corroborate the origin of the funds or the circumstances under which the wealth was acquired. In 2020, 58% of files reviewed indicated this weakness.
 - e) **Missing or inadequate CDD information and documents:** 32% of the files reviewed indicated weaknesses related to missing or inadequate CDD. In 2020, 38% of files reviewed indicated this weakness.



12. The Authority acknowledges the positive engagement from TCSPs subject to inspection in 2021. CIMA continues to help raise standards in the TCSP sector through outreach and guidance, risk-based AML/CFT/CPF supervision and monitoring and use of enforcement where appropriate and proportionate.

2021 Review Findings

13. Regulation 12 of the AMLRs, and Part II, Section 4 of the AML/CFT Guidance Notes¹ set out the obligation of FSPs, including TCSPs, to conduct CDD procedures to identify and verify customers, identify beneficial owners, understand, and obtain information on the purpose and intended nature of the business relationship, and obtain information on source of funds.

Identification and Verification of Customers and Beneficial Owners

14. Regulation 12(1) of the AMLRs includes that a person carrying out relevant financial business shall:

- identify a customer, whether a customer in an established business relationship or a one-off transaction, and whether natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information;
- verify that a person purporting to act on behalf of a customer is properly authorised and identify and verify the identity of the person; and
- identify a beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from reliable sources, so as to be satisfied that the person knows the identity of the beneficial owner.

15. The 2021 review identified weaknesses in TCSPs not effectively implementing regulation 12(1) above. Four percent (4%) of the files reviewed indicated lack of adequate information and/or

¹ Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands

documents being maintained to demonstrate that the TCSP identified and verified the identity of ultimate beneficial owners and authorised persons such as directors, persons issued with powers of attorney, and other parties who have effective control. Examples of weaknesses/deficiencies noted on the files include:

- a) Identification documents of beneficial owners were expired;
- b) Birth information for the UBO was missing;
- c) Identification documents for the UBO were missing;
- d) Identification documents for the UBO were not certified;
- e) Contact details of the certifier were missing;
- f) Documents verifying occupation(s) of the UBO(s) were missing; and
- g) No documented evidence of sanctions screening performed for corporate entities and their related parties, including UBOs, during onboarding or as part of the Licensee's ongoing monitoring procedures.

16. FSPs, including TCSPs, are required to obtain relevant information or data from reliable sources to evidence that they have identified and verified the beneficial owners and other authorised persons who have an effective control over the customer. This could include (but is not limited to) obtaining a certified copy of a passport or any other government issued identification, utility bills, and/or reference letters from credible sources to verify the identity and addresses of customer.

Ongoing Monitoring

17. Regulation 12(1)(e) of the AMLRs includes that 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 person's knowledge of the customer, the customer's business, and risk profile, including where necessary, the customer's source of funds.
18. As part of the ongoing monitoring process, a Licensee should obtain, verify, and retain supporting documents that ensures that they have an understanding of the customers' business; intended purpose of the business relationship; expected source, volume and value of funds; and customer risk profile.
19. The 2021 Review identified weaknesses in relation to TCSPs' ongoing monitoring with twenty-five percent (25%) of the files showing deficiencies around the frequency and type of monitoring mechanisms that are applied to a customer. The following are some of the client weaknesses noted on files reviewed:
 - a) Failure to consider all the relevant risk factors in risk rating a customer, leading to application of inappropriate risk mitigation and monitoring measures. In some of the files reviewed, a high-risk customer (whose associate is a Politically Exposed Person ("PEP")) was rated medium instead of high;
 - b) Failure to provide documentation to show that client risk assessments were carried out;
 - c) Failure to conduct the risk assessment of the client until after the onboarding of the client was completed; and
 - d) Failure to provide sufficient evidence to demonstrate review of transactions undertaken throughout the course of the business relationship to ensure that transactions being conducted are consistent with the Licensee's knowledge of the client.

Purpose and Intended Nature of the Business Relationship

20. Regulation 12(1)(d) of the AMLRs states that a person carrying out relevant financial business shall understand and obtain information on, the purpose and intended nature of a business relationship.
21. The 2021 Review identified weaknesses in relation to TCSPs' understanding of their customers' nature of business. Three percent (3%) of the files reviewed indicated lack of collection and retention of information on the nature and purpose of the business relationships, which enables the Licensee to have a more insightful description of how the entity operates and a more complete risk profile of the customer.
22. Whilst TCSPs are not yet fully compliant with this requirement, the levels of compliance have improved as evidenced by the decline in the number of files with this weakness noted in 2021 (3%), compared to the 49% observed in 2020.
23. FSPs, including TCSPs, are required to understand the purpose and intended nature of business relationships of their clients, by obtaining information including, but not limited to:
 - a) The reason for the business relationship;
 - b) Background of the business (including financial activity, major customers, beneficial owners, source of funds/wealth and association with high-risk countries);
 - c) Number, size, frequency, and destination of transactions that will pass through the accounts; and
 - d) Turnover of the business.
24. Information obtained should be corroborated with relevant documentation to verify that the customers are who they purport to be. This could include, but is not limited to:
 - a) Audited Annual Financial Reports;
 - b) Evidence from independent sources such as google searches;
 - c) Business cards or company websites to confirm that the nature of the business is legitimate;
 - d) Trade and business licenses;
 - e) Contracts, such as debentures and investment management agreements; and
 - f) Trust deeds.

Source of Funds

25. The 2021 Review identified weaknesses in relation to TCSPs' ongoing monitoring for source of funds/wealth. Ten percent (10%) of the files reviewed indicated a lack of information on source of funds/wealth. Either this was not obtained, verified, or documented, or the documentary evidence was inadequate to substantiate the origin and circumstances of the customers' funds or wealth.
26. The Authority expects TCSPs and other FSPs to obtain sufficient and relevant documents to demonstrate how they have corroborated the source of funds as the customer purports it to be. These documents can include, but are not limited to:
 - a) Copies of audited financial statements;
 - b) Bank statements;
 - c) Independently verified source of funds declarations;
 - d) Confirmation received from independent third-party sources; and
 - e) Data gathered from variable public sources.

Missing or inadequate customer due diligence (CDD) information and documents

27. Regulation 12(1) of the AMLRs includes that a person carrying out relevant financial business shall:
- identify a customer, whether a customer in an established business relationship or a one-off transaction, and whether natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information; and
 - verify that a person purporting to act on behalf of a customer is properly authorized and identify and verify the identity of the person.
28. TCSPs and other FSPs are also required to implement adequate ongoing monitoring systems and controls which will enable them to review and update documents collected under the CDD process prior to their expiration.
29. The 2021 Review identified weaknesses in relation to TCSPs' collection of CDD information and documentation. Thirty-two percent (32%) of the client files reviewed had missing or inadequate CDD information, including documents that were illegible, not properly certified or expired. For example:
- a) The files lacked updated identification documentation for directors and shareholders whose documentation on file had expired;
 - b) The certification details were illegible;
 - c) The information provided by the certifier did not relate to the actual document.
 - d) The CDD/KYC documentation for UBOs, Directors and/or related parties were not adequately certified in accordance with regulatory requirements, for example, the certifier's contact address, signature and telephone numbers were missing;
 - e) The CDD documentation obtained for clients were either not translated or partially translated; and
 - f) The identified Licensees were unable to satisfactorily demonstrate that client file reviews were being conducted on a periodic basis, to ensure that documents, data, or information collected under the CDD process is kept current and relevant to CDD.
30. Although this is a slight improvement on 2020 (38%), this remains a key area of deficiency. All TCSPs should ensure that they maintain appropriate standards of compliance when collecting CDD at the point of onboarding and on an ongoing basis.

Conclusion & Recommendations

31. The results of the 2021 Thematic Review are encouraging, showing a significant improvement in compliance by TCSPs with regulation 12 of the AMLRs. The Authority acknowledges the work done across the sector to strengthen AML/CFT frameworks and manage risk.
32. Nevertheless, the 2021 Review also observes that TCSPs have greater weaknesses in implementing ongoing monitoring measures and collecting accurate, up to date CDD. This includes periodically monitoring transactions and reviewing customer files, maintaining accurate, relevant and up to date information of the customers and/or beneficial owners.
33. By obtaining and maintaining adequate, relevant and up to date information, all FSPs (including TCSPs) will have greater understanding of the controllers and beneficial owners of the businesses they serve, and their respective businesses. This will enable them to know their customers, be in a position to identify any deviations from the norm, and to report suspicious transactions to the Financial Reporting Authority.

34. TCSPs should take note of the 2021 Review findings and act to ensure that their own AML/CFT compliance frameworks meet the standards prescribed, and should periodically assess their AML/CFT compliance programmes to ensure that they are commensurate with the nature, size, and complexity of their businesses.
35. The Authority will continue to promote its supervisory mandate through offsite monitoring and onsite inspection processes. TCSPs are reminded that any breach of the AMLRs, or non-compliance with a 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

The following outlines the scope and methodology for the inspections:

1. The 2021 Review 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 16 different regulated entities and 359 customer files.
2. As part of the onsite inspection process, the sample population of 359 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 12 of the AMLRs. It considered the adequacy and relevance of CDD documents obtained in the identification and verification of natural persons and beneficial owners; information obtained and recorded to understand the purpose and intended nature of a business relationship; adequacy of information and documentation on source of funds and source of wealth; maintenance of up to date documents and frequency of ongoing monitoring procedures. Percentages for findings provided in this document are expressed as out of the total number of 359 files reviewed.
4. The Authority has also prepared individual reports for the TCSPs subject to inspection in 2021.

References

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

[Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands](#)

[AML/CFT Activity Report 2020](#)

[The Anchor Publications](#)

[FATF Best Practices on Beneficial Ownership for Legal Persons – October 2019](#)

[FATF Egmont Concealment Beneficial Ownership - July 2018](#)

[FATF - Misuse of Corporate Vehicles including Trust and Company Services Providers - October 2006](#)

[Regulated Sectors Training Videos](#)