GUIDANCE NOTES (AMENDMENTS) ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

Issued by the Cayman Islands Monetary Authority
Pursuant to section 34 of the Monetary Authority Law (2020 Revision)

These Guidance Notes amend the Guidance Notes issued on December 13, 2017
(the "GN of December 13, 2017")

February 2020

This document is intended to provide general guidance to Financial Service Providers ("FSPs"). It should therefore, not be relied upon as a source of law. Reference for that purpose should be made to the appropriate statutory provisions. However, FSPs should be aware of the enforcement powers of the Supervisory Authorities under the Anti-Money Laundering Regulations (2020 Revision) ("AMLRs") and amendments thereto as they relate to supervisory or regulatory guidance.

Contact:
Cayman Islands Monetary Authority
171 Elgin Avenue, SIX, Cricket Square
P.O. Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel: 345-949-7089
Fax: 345-945-6131

Website: www.cima.ky
Email: CIMA@cima.ky

1. These Guidance Notes may be cited as the **Guidance Notes (Amendment) (No.3), February 2020**.

2. The GNs of December 13, 2017 are amended to include Section 15 in **Part II**, as follows:

Section 15

TARGETED FINANCIAL SANCTIONS

A. INTRODUCTION

1. This section of the Guidance Notes is to be read and applied in conjunction with Part II, Section 13 – Sanctions Compliance and the relevant Sector Specific Guidance Notes ("SSGN") that are provided in PART III to PART VIII hereof. FSPs should also read the Financial Reporting Authority's (FRA) issued *Industry Guidance on Targeted Financial Sanctions*[1]. Sanctions queries should usually be directed to the FRA.

B. OVERVIEW

1. Financial sanctions 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[2] to persons or entities. They are generally imposed to:

   (1) Coerce a regime, or individuals within a regime, into changing their behaviour (or aspects of it) by increasing the cost on them to such an extent that they decide to cease the offending behaviour;

   (2) Constrain a target by denying them access to key resources needed to continue their offending behaviour, including the financing of terrorism or nuclear proliferation;

[1] http://www.fra.gov.ky/contents/page/1[fra.gov.ky]

[2] According to FATF, the term "***funds or other assets***" means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.

(3) Signal disapproval, stigmatising and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or

(4) Protect the value of assets that have been misappropriated from a country until these assets can be repatriated.

2. Targeted financial sanctions (TFS) are a specific type of financial sanction with stated objectives, one of which is the prevention of terrorist financing and proliferation financing.

3. The term TFS means both asset freezing and restrictions and directions to prevent funds or other assets, including virtual assets, from being made available, directly or indirectly, for the benefit of designated persons and entities. In establishing an effective counterterrorist and proliferation financing regime, consideration is also given to respecting human rights, respecting the rule of law, and recognising the rights of innocent third parties.

4. TFS entail the use of financial instruments and institutions to apply coercive pressure on specific parties[3] in an effort to change or restrict their behaviour. Sanctions are targeted in the sense that they apply only to a subset of the population – usually the leadership, responsible elites, or operationally responsible persons. The sanctions are financial in that they involve the use of financial instruments, such as asset freezes, blocking of financial transactions or financial services. They are sanctions in that they are coercive measures applied to effect change.

5. Where the financial sanction takes the form of an asset freeze, it is generally prohibited to:

(1) Deal with the funds or other assets, belonging to or owned, held or controlled by a designated person or entity;

(2) Make funds or other assets available, directly or indirectly, to, or for the benefit of a designated person or entity; or

(3) Engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions.

[3] Usually, government officials, elites who support them, or members of non-government entities, but this is not exhaustive.

C. RELEVANT SANCTIONS

1. Two key international bodies that impose international sanctions measures are the United Nations (UN) through resolutions passed by the UN Security Council ("UNSCRs") and the European Union (EU) through EU regulations[4].

2. His Excellency the Governor (the Governor), through local designations, can impose domestic financial sanctions in the Cayman Islands.

3. The UK imposes its own financial sanctions and restrictions under the following legislation:

   (1) Terrorist Asset-Freezing etc. Act 2010 (TAFA 2010);

   (2) Counter Terrorism Act 2008 (CTA 2008); and

   (3) Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001).

4. The UK's Office of Financial Sanctions Implementation ("OFSI") publishes a consolidated list of sanctions that provides information to help FSPs decide whether they are dealing with a person or entity that is subject to financial sanctions. It lists full name; any known aliases; honorary, professional or religious titles; date of birth, place of birth; nationality; passport details; national identification numbers; address; any additional information that may be useful; title of the financial sanctions regime under which the designated person or entity is listed; the date when the designated person or entity was added to the list by HM Treasury; when the information regarding the designated person or entity was last updated by HM Treasury and a unique reference number relating to the designated person or entity.

5. Additionally, the UK Government passes Orders in Council implementing UN, EU and UK sanctions and extending such sanctions to its Overseas Territories through Overseas Orders in Council (OOICs), namely:

   (1) The Isil (Da'esh) and Al-Qaida (Sanctions) (Overseas Territories) Order 2016, and successors;

   (2) The Afghanistan (United Nations Measures) (Overseas Territories) Order 2012, and successors;
   (3) The Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2012, and successors; and
   (4) The Iran (Sanctions) (Overseas Territories) Order 2016, and successors.

6. It is important for FSPs to note that OOICs have the force of law in the Cayman Islands.

---

[4] The FRA's Industry Guidance provides some detail on how sanctions are imposed. http://www.fra.gov.ky/app/webroot/files/2017-12-15%20FRA%20Guidance%20Targeted%20Financial%20Sanctions(1).pdf

7. It is the responsibility of every FSP to keep itself updated on and comply with the TFS in force in the Cayman Islands. Official sanctions orders applicable in the Cayman Islands are published in the Cayman Islands Gazette.

8. The FRA's website provides a link to the consolidated list of financial sanctions targets, issued by the UK's OFSI, applicable to the Cayman Islands. [5][6] Additionally, the FRA maintains a Cayman Islands domestic consolidated list of designated persons by the Governor. The Authority, however, does not guarantee that these lists are accurate, complete and up to date, therefore FSPs need to ensure that they are kept up to date with all applicable sanctions.

D. RELEVANT AUTHORITIES

9. His Excellency the Governor (the Governor) is the competent authority for the implementation of TFS in the Cayman Islands. All reports relating to TFS should be made to the Governor through the FRA.[7]

10. Effective November 15, 2017, the Governor of the Cayman Islands, delegated the function of receiving reports to the FRA pursuant to:

(1) Articles 7(2) – 7(4) of The Isil (Da'esh) and Al-Qaida (Sanctions) (Overseas Territories) Order 2016;

(2) Articles 22(1) – 22(3) of The Afghanistan (United Nations Measures) (Overseas Territories) Order 2012;

(3) Articles 6(2) – 6(4) of The Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2012;

(4) Articles 8(2) – 8(4) of The Iran (Sanctions) (Overseas Territories) Order 2016; and

(5) Paragraph 20 of Schedule 4A of the Terrorism Law (2018 Revision).

11. The FRA is the Cayman Islands' Financial Intelligence Unit (FIU) with responsibility for receiving, requesting, analysing and disseminating disclosures of information concerning the proceeds of criminal conduct, money laundering and the financing of terrorism.

12. The Sanctions Coordinator (SC) of the FRA is responsible for coordinating the implementation of TFS with respect to terrorism, terrorism financing, proliferation and

---

[5] http://www.fra.gov.ky/contents/page/1

[6] The direct link to the OFSI website is https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

[7] A Compliance Reporting Form (CRF) must be completed when making a report to the FRA. The CRF should be used when reporting suspected designated persons, frozen assets, and suspected breaches of financial sanctions

proliferation financing. The SC will take a holistic approach to ensuring compliance with the sanctions regime to cover the whole lifecycle of compliance. For example: promote compliance by publishing financial sanctions and engaging with the private sector and enable compliance by providing guidance and alerts to help them discharge their own compliance responsibilities. The SC will also perform a central and proactive role in the making of recommendations for designation to the Governor.

13. The Financial Crimes Unit (FCU) is the unit within the Royal Cayman Islands Police Service (RCIPS) with responsibility for investigating all financial crimes within the Cayman Islands. This includes ML investigations, with the exception of ML related to corruption as a predicate offence, which is dealt with by the Anti-Corruption Commission (ACC), and TF investigations.

14. The Authority, in its role as regulator for FSPs, assesses whether persons or entities under its regulatory laws are aware of applicable international TFS and any local designations or directions that are in force; and their compliance obligations including, but not limited to, responsibilities for screening and reporting, ongoing monitoring and staff training. The Authority also reviews regulated entities' reports and returns, paying special attention to persons, entities or countries listed on any autonomous list of designations and applicable international TFS. During an inspection, the Authority will test the effectiveness of systems established by the licensee to observe and comply with TFS in effect.

E. COMPLIANCE FUNCTION

1. FSPs should develop a comprehensive compliance programme to comply with the relevant and applicable laws and obligations and prevent and report ML/TF/PF. Senior management of an FSP should establish a culture of compliance throughout the organisation.

2. During the course of ongoing monitoring of relevant sanctions lists, FSPs may discover that certain TFS are applicable to one or more of their clients, existing or new. Pursuant to the Terrorism Law and the Proliferation Financing (Prohibition) Law, FSPs have certain reporting obligations to the FRA. It is a criminal offence not to freeze funds or other assets belonging to, owned, held or controlled by a designated person or entity, if an FSP discovers a relationship that contravenes an Order or a direction under the Terrorism Law or Proliferation Financing (Prohibition) Law.

3. FSPs are required to have in place procedures for ongoing monitoring of business relationships or one-off transactions for the purposes of preventing, countering and reporting terrorist and proliferation financing; and extend to allowing for the identification of assets subject to applicable TFS.

F. DESIGNATED PERSONS AND ENTITIES

1. Designated persons or entities are established through the designation of sanctions. Financial Sanctions Notices advise of the addition or removal of a designated person

or entity from, or amendments to the consolidated list or local designations made in the Cayman Islands by the Governor and are published on the FRA website.

2. The definition of "designated person" is as prescribed in:

(1) Schedule 4A, paragraph 2 of the Terrorism Law (as amended);

(2) Part I, Section 2 of the Proliferation Financing (Prohibition) Law (as amended); and

(3) The relevant OOICs.

G. OBLIGATIONS OF FSPs

1. FSPs must ensure that they comply with their legal obligations to:

(1) regularly monitor the sanctions in place including local designations[8] made by the Governor;

(2) review their clients against the lists of designated persons or entities and the consolidated list, maintained by the OFSI;

(3) freeze any accounts, other funds or economic resources belonging to, owned, held or controlled by designated persons or entities;

(4) refrain from dealing with funds or assets or making them available to designated persons or entities, unless licensed by the Governor;

(5) report to the Governor, through the FRA, as soon as practicable, if they know or have reasonable cause to suspect that a person is a designated person or has committed an offence under the legislation; and

(6) disclose to the Governor, through the FRA, via the Compliance Reporting Form (CRF)[9], details of any frozen funds or other assets or actions taken in compliance with the prohibition requirements of all applicable sanctions, including attempted transactions[10].

2. FSPs should ensure that they have adequate resources, policies and procedures to comply with TFS obligations. Regular reviews and updates of TFS policies and procedures should take place to ensure they remain fit for purpose and are enforced.

[8] These designations, when made, are published on the FRA's website.

[9] This form can be found on the FRA's website.

3. FSPs are required to foster a culture of compliance and ensure that clear, comprehensive policies and procedures are in place to guide employees in ensuring that their legal obligations and these GNs relating to TFS are being adhered to.

4. FSPs should maintain records of any potential matches to names on sanctions lists and related actions, whether the match turns out to be a true match or a false positive.

5. At a minimum, FSPs should keep the following information about any match:

   (1) the basis or other grounds which triggered the match (e.g. a "hit" provided by screening software);

   (2) any further checks or enquiries undertaken;

   (3) the associated sanctions regime;

   (4) the person(s) involved, including any members of compliance or senior management who authorised treatment of the match as a false positive;
   (5) the nature of the relationship with the person or entity involved, including attempted or refused transactions; and

   (6) subsequent action taken (e.g. freezing of funds).

6. FSPs should always refer to the up-to-date version of the legislation imposing the specific financial sanctions which apply in each case to understand exactly what is prohibited.

7. FSPs should familiarise themselves with their legal and other obligations and where necessary, seek independent legal advice.

8. If an FSP is unsure whether it is dealing with a designated person or entity, then it should consider requesting more information from the client.

Sanctions/Orders Monitoring

9. FSPs are required to have in place and effectively implement internal controls and procedures to, without delay, ensure compliance with the obligations arising from the designation or delisting of a person or entity. This includes putting systems in place to review the financial sanctions notices and consolidated list of designations; and to screen their client databases against those lists immediately after a change to any of these lists occurs.

10. Screening should also take place at the commencement of any business relationship. This includes screening existing customers when data changes, e.g. change of director or signatory on account; when new financial sanctions notices are issued; and when there are updates to the consolidated list.

11. FSPs should ensure that payments are not indirectly made to or for the benefit of, a targeted person or entity. Thus, screening of directors, beneficial owners, trustees, settlors, beneficiaries and third-party payees against financial sanctions notices and the consolidated list is important.

12. FSPs are required to put systems and controls in place to allow for ongoing monitoring of transactions and to ensure that proper records are kept of these transactions.

Asset Freezing/Freezing Mechanisms

13. Once a person or entity has been designated, there is a legal obligation not to transfer funds or make funds or other assets available, directly or indirectly, to that person or entity. FSPs are required to freeze, without delay[11] and without prior notice, the funds or other assets of designated persons and entities.

14. The freezing of assets extends to all funds or other assets, including virtual assets, that are owned, held or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned, held or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned, held or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

15. Funds generally means financial assets and benefits of every kind[12], including but not limited to:

    (1) Cash, cheques, claims on money, drafts, money orders and other payment instruments;

    (2) Deposits with financial institutions or other entities, balances on accounts, debts and debt obligations;

    (3) Publicly and privately traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts;

    (4) Interest, dividends or other income on or value accruing from or generated by assets;

    (5) Credit, right of set-off, guarantees, performance bonds or other financial commitments;

[11] *Without delay* should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorist organisations, and those who finance terrorism, and the need for global, concerted action to interdict and disrupt their flow swiftly.

[12] Including economic resources and virtual assets.

(6) Letters of credit, bills of lading, bills of sale; and

(7) Documents showing evidence of an interest in funds or financial resources.

16. FSPs are prohibited from making any funds, economic resources, other assets or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and/or entities; entities owned, held or controlled, directly or indirectly, by designated persons or entities; and persons and/or entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions.

False Positives

17. False positives are potential matches to listed persons or entities, either due to the common nature of the name or due to ambiguous identifying data, which on examination prove not to be matches.

18. FSPs must take reasonable steps to ensure that a person or entity identified as designated is the same person or entity as that on the consolidated list or the local designation made in the Cayman Islands by the Governor, by verifying the name with other identifying information.

19. Distinguishing between designated and non-designated persons or entities may be difficult even with additional identifiers. In some cases, the funds or other assets of a person or entity that was not the intended target of the restrictive measures will be frozen due to identifiers that match with those of a designated person or entity. As a precautionary measure, FSPs should refrain from entering into a business relationship or conduct transactions with any person or entity that the available identifiers match, unless it is clear that it is not the same as the designated person or entity.

20. An FSP should be aware that if a person or entity whose funds or other assets are frozen, claims that they are not the intended target of the restrictive measures, that person or entity should first contact the relevant FSP that froze the funds or other assets, requesting an explanation, including why the relevant FSP believes they are a target match on the consolidated list or to the local designations made in the Cayman Islands by the Governor . The burden of proof concerning determination of a question of a 'false positive' rests with the person or entity, who should submit documentary evidence to the relevant FSP of their identity and a detailed statement as to why they are not the listed person or entity. If the relevant FSP or the person or entity, after using all the available sources cannot resolve the issue as to whether a customer is in fact the designated person or entity, then either should inform the FRA.

Training and Internal Controls

21. FSPs should have systems in place to ensure compliance with legal and regulatory obligations in relation to TFS. FSPs should develop and maintain adequate internal

controls (including due diligence procedures and training programmes as appropriate) to be able to identify any existing accounts, transactions, funds or other assets of designated persons and/or entities and file any applicable reports with the competent authority. It is essential that FSPs maintain documentation in relation to their sanctions' practices.

22. Regular employee training is required in the identification of persons or entities and assets subject to TFS; as well as the processes to be followed where such persons or entities are identified. FSPs should also provide training to employees to ensure proper and efficient recognition and treatment of transactions carried out by, or on behalf of, any person or entity who is or appears to be engaged in terrorist and/or proliferation financing, or whose funds or other assets are subject to TFS.

23. Ongoing training and assessments of employees should be conducted to ensure that they obtain and maintain adequate knowledge of matters related to TFS, sanctions obligations and compliance standards.

Reporting Obligations to the Competent Authority

24. FSPs are obligated to report to the relevant competent authority, including the FRA through the Governor, any assets frozen or actions taken in compliance with the prohibition requirements of the applicable TFS, including attempted transactions, as soon as practicable. Reports of frozen funds and economic resources should be submitted to the FRA using the CRF.

25. FSPs must report to the Governor, through the FRA, as soon as practicable, all matches identified on the local designations made in the Cayman Islands by the Governor or on the consolidated list. The report should contain the nature and value of any funds or other assets held.

26. FSPs are obligated to report to the Governor, through the FRA, as soon as practicable, if it is aware of have a reasonable cause to suspect that a person is a designated person or has committed an offence under the legislation. The information reported should include the information or other matter on which the knowledge of suspicion is based; any identifying information that is held about the person or entity; the nature and amount of funds or economic resources held by that person or entity.

27. Additionally, FSPs should report, as soon as practicable:

    (1) the results of searches and/ or examinations of past financial activity by designated persons and/or entities;

    (2) the details of any other involvement with a listed person or entity, directly or indirectly, or of any attempted transactions involving those persons or entities;

    (3) the details of incoming transfers or other transaction resulting in the crediting of a frozen account in accordance with the specific arrangements for FSPs;

(4) attempts by clients or other persons to make funds or assets available to a designated person or entity without authorisation; and

(5) information that suggests the freezing measures are being circumvented.

28. Once a person or entity is delisted, FSPs are also required to advise the Governor, through the FRA, of any actions taken in relation to that de-listed person or entity, as soon as practicable.

29. In addition to their reporting obligations under the sanctions regime, FSPs must file a SAR if they suspect or have grounds to suspect criminal conduct separate from the person or entity being the target of TFS.

30. If an FSP files a SAR about a sanctioned person or entity, a disclosure that a SAR has been filed may constitute tipping-off under the POCL.

31. The filing of a SAR does not provide protection in respect of offences that may have been committed under sanctions legislation.

Unfreezing Assets

32. Upon becoming aware or receiving notification advising that a person or entity is no longer designated under a sanctions regime, an FSP must, without delay, confirm whether they have frozen funds or other assets of any such person or entity; verify that the person or entity is no longer subject to the asset freeze; remove the person or entity from the FSP's list of persons or entities subject to financial sanctions; and unfreeze the funds or other assets of the person or entity and reactivate the relevant accounts.

33. The FSP is required to submit notification to the person or entity that the assets are no longer subject to an asset freeze and notify the Governor through the FRA of the actions taken.

H. EXEMPTIONS AND LICENSING

Exemptions

1. In certain circumstances, an individual can make a transfer to a sanctioned person or entity. Freezing obligations are subject to certain exemptions in limited circumstances.

2. An exemption to a prohibition applies automatically in certain defined circumstances and does not require an FSP to obtain a licence from Governor.

3. Asset freezing legislation generally permits the following payments into a frozen account without the need for a licence from the Governor, provided those funds are frozen after being paid in:

(1) any interest or earnings on the account; and/ or

(2) any payments due to a designated person or entity under contracts, agreement or obligations that were concluded or arose before the date the person or entity became sanctioned.

4. The legislation also generally permits the crediting of a frozen account with payments from a third party without the need for a licence, provided that the incoming funds are also frozen, and that the Governor is informed of the transaction without delay.

Licensing

5. A licence is a written authorization from the Governor permitting an act otherwise prohibited under the sanctions. The licence can include additional reporting requirements or have a time limitation.

6. The overall objective of the licensing system in terrorist asset freezing cases is to minimise the risk of diversion of funds to terrorism, while respecting including those of bona fide third parties. To this end, the Governor may grant licences to allow exceptions to the freeze. If a licence is being granted under an OOIC, the Governor must obtain the consent of the UK Secretary of State; whereas a licence issued pursuant to the Terrorism Law requires the Governor to consult with the UK Secretary of State.

7. Some common licensing grounds found in the OOICs are for basic needs, legal fees and disbursements, fees or service charges for routine holding or maintenance of frozen funds or other assets, satisfaction of prior contractual obligations of the designated person or entity, and extraordinary expenses.

8. Any person seeking a licence for the release of funds or other assets, which are subject to an "asset freeze", is required to submit an application to the Governor using the prescribed form[13] which is available on the FRA's website. The application must be supported by evidence to demonstrate that all the licensing criteria are met.

9. An FSP must provide evidence to support an application. As such, applicants are required to provide:

(1) the licensing ground(s) being relied upon in the application including supporting arguments;

(2) full information on the parties involved in the proposed transaction including*, inter alia*, the designated person(s) or entities and any financial institution(s) involved;
(3) ultimate beneficiary of the transaction;

(4) the complete payment route including account details; and

(5) the amount (or estimated amount) of the proposed transaction.

[13] The relevant form can be obtained from the FRA's website.

10. In cases where the application for a licence is considered urgent, this needs to be clearly stated. The basis of the urgency and supporting evidence establishing a basis for the urgency should be included in the application. It is important to note that there is no guarantee that the application will be treated urgently. It is at the discretion of the competent authority that an application be treated as urgent.

11. Employees and clients of FSPs need to be clear about the specific permissions contained in the licence as they must be strictly complied with. It is important to note that licences are not issued retrospectively. Additionally, FSPs must be mindful that engaging in transactions or attempting to transact with a designated person or entity without obtaining a licence is a breach of financial sanctions legislation and therefore, a criminal offence.

ADDITIONAL SCREENING GUIDANCE

1. Screen for full name, date of birth, address and aliases.

2. Sanctioned parties are known to use false personal information to try and evade detection. Additionally, information held by an institution may not exactly correlate to information recorded on the consolidated list or the local designation made in the Cayman Islands by the Governor.

3. To maximise screening, seek to incorporate variables such as:

   (1) Different spellings of names (e.g. Abdul instead of Abdel);

   (2) Name reversal (first/middle names written as surnames and vice versa);

   (3) Shortened names (e.g. Bill instead of William);

   (4) Maiden names;

   (5) Removing numbers from entities; and

   (6) Insertion/removal of full stops and spaces.

4. If using automated screening, the following actions may assist to improve screening quality:

   (1) Understanding the capabilities and limits of the particular automated screening system.

   (2) Ensuring the system is calibrated to the FSP's needs.

   (3) Checking the matching criteria is relevant and appropriate for the nature and the size of business to ensure less false positives are produced.

(4) Ensuring screening rules are appropriately defined e.g. allow for the use of alternative identifiers.

(5) The calibration of systems to include the use of fuzzy matching. Fuzzy matching searches for words or names likely to be relevant, even if words or spelling do not match exactly. It can assist to identify possible matches where data is misspelled, incomplete or missing.

(6) Ensuring prominent flagging of matches so that they are clearly identifiable.

(7) Keeping calibration and automated systems under regular review to ensure they are fit for purpose.