Jersey Financial Services Commission

Sanctions

Financial Sanctions

Practical Guidance

Issued: January 2011

Last Updated: 2 December 2016

FINANCIAL SANCTIONS PRACTICAL GUIDANCE

Introduction

In general terms, local sanctions measures apply to all natural and legal persons: (i) located in Jersey; (ii) operating in or from within Jersey; (iii) incorporated or constituted under Jersey Law. This guidance has been produced in an effort to assist institutions in producing policies and procedures to address their legal obligations under sanctions legislation.

Overview

Institutions should aim to have proportionate systems and controls in place to reduce the risk of a financial sanctions breach occurring. How those systems and controls are formulated will depend on the business model, profile and customer base of each institution. Institutions should focus their resources and systems and controls on assessing where and how their particular business is most likely to breach sanctions.

From the outset, it is important that the proportionate systems and controls put in place are not based on the common misconceptions about financial sanctions highlighted in the general information section at: http://www.jerseyfsc.org/pdf/Sanctions_General_Information.pdf

A diagrammatic overview of how to comply with sanctions, summarising the key messages contained in this guidance is available at: http://www.jerseyfsc.org/pdf/Sanctions_Compliance_Overview.pdf

In order to assist institutions in achieving proportionate systems and controls, this guidance is divided into the following areas:

1. Implementing policies and procedures regarding sanctions
2. Providing staff training in sanctions matters
3. Risk assessing sanctions vulnerabilities
4. How to screen customers to prevent sanctions breaches
5. How to make customer screening more effective
6. Systems for investigating a match
7. Action required on discovering a confirmed or potential target match
8. Information you may be required to provide
9. Obtaining a licence
10. International Obligations

Appendix: Examples of good and bad practice

1. Implementing policies and procedures regarding sanctions

1.1 Institutions should have written policies and procedures in place to deal with sanctions screening. Regular reviews and updates of sanctions policies and procedures should take place to ensure they remain fit for purpose and are enforced. The information in the following sections is an outline of areas that should be taken into account in formulating sanctions policies and procedures.

2. Providing staff training in sanctions matters

2.1 Staff should be trained on an ongoing basis in respect of sanctions matters. As the sanctions arena is constantly evolving it is important for staff knowledge to be kept current. Training can be carried out separately or alongside anti-money laundering training so long as it is:

- Appropriate, accessible and routinely provided.
- Targeted to specific roles. Detailed training may be given to those involved in customer take-on and monitoring, with more general training to other members of staff.

3. Risk assessing sanctions vulnerabilities

3.1 Breaching financial sanctions is an absolute offence so the decision to take a risk-based approach is in itself a risk-based decision. If formulated properly, however, it is appropriate to take a risk-based approach to sanctions screening. If a risk-based approach is taken, an institution should be satisfied that its approach is appropriate and sufficient. With that in mind, it would be wise for an institution to have a formally documented risk assessment covering sanctions with a clear rationale for the approach taken.

3.2 In order to conduct a comprehensive risk assessment, a business needs to have a good understanding of the financial sanctions regime and the risks posed by particular customers, transactions, services, products and jurisdictions.

3.3 A proper risk assessment should consider how an institution may become involved in breaching sanctions. Relevant factors an institution may take into account in formulating its risk assessment are:

- customer, product and activity profiles;
- distribution channels;
- complexity and volume of transactions (recognising that one prohibited transaction alone would be a breach);
- processes and systems;
- operating environment;
- screening processes of intermediaries;
- geographic risk of where it does business; and
- whether trustees, settlors, beneficiaries, directors and beneficial owners of legal persons and third party payees are screened to ascertain whether there is a risk of indirect benefit to a sanctioned person.

3.4 Where, as part of a risk assessment, an institution identifies a particular vulnerability the institution should consider looking to ascertain the following information in order to better identify sanctions targets:

- **For individuals**: place of residence, country of birth, country of origin, citizenship, source of wealth, occupation and countries to or from which transactions are made, known associates.
- **For entities**: location of business, country in which incorporated, nature of business, beneficial owners of the business, directors, countries from which transactions are made and entities with which transactions are effected.

4. How to screen customers to prevent sanctions breaches

4.1 When screening customers attach significance to:

- Screening new customers at take-on against personal identifying information on the UK Consolidated List. The UK Consolidated List can be accessed here: http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

- Periodically screening existing customers, within a reasonable time of notified changes to the UK Consolidated List.
- Including United Kingdom based customers in search parameters.
- Screening for full name, date of birth, address and aliases.
- Screening existing customers when data changes e.g. change of director.
- Ensuring payments are not indirectly made to, or for the benefit of, a target person. Thus screening of directors, beneficial owners, trustees, settlors, beneficiaries and third party payees against the UK Consolidated List is important.
- Considering the nature of the business generally and any potential sanctions pitfalls as a result. In considering the nature of the business, non-financial sanctions such as those relating to the import and export of goods may be relevant depending on the business in question.
- Maintaining an audit trail of screening.

4.2 Sanctioned parties are known to use false personal information to try and evade detection. In addition, information held by an institution may not exactly correlate to information recorded on the UK Consolidated List.

4.3 The table below gives examples of how the wording or format of a customer name held by an institution may be different from the wording used in the UK Consolidated List.

Version in the Consolidated List	Version used by a institution
Revolutionary People's Liberation Army	Revolutionary Peoples' Liberation army/front
Pavlichenko, Dmitry Valeriyevich	Pavliuchenko, Dmitry Valeriyevich
Rockmans, Limited	Rockman Ltd
Salim, Ahmed Fuad	Amed Fuad Salim

4.4 To maximise screening, seek to incorporate variables such as:

- Different spellings of names (e.g. Abdul instead of Abdel);
- Name reversal (first/middle names written as surnames and vice versa);
- Shortened names (e.g. Bill instead of William);
- Maiden names;
- Removing numbers from entities; and
- Insertion/removal of full stops and spaces.

5. How to make customer screening more effective

Generally

5.1 To ensure customer screening is more effective, attach importance to:

- Implementing a written screening policy to incorporate the frequency of screening and quality of screening.

- Ensuring that effective sanctions screening has taken place by an intermediary, if relying on an intermediary to carry out screening. Depending on when sanctions screening took place by an intermediary, it may be necessary to re-screen to ensure the position has not changed or obtain reassurance that an intermediary's screening for sanctions is ongoing.
- Keeping customer information up to date. Complete and current customer information will improve the effectiveness of screening and reduce the amount of false positives.

Automated screening

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

- Understanding the capabilities and limits of the particular automated screening system.
- Ensuring the system is calibrated to the institution's needs.
- Checking the matching criteria is relevant and appropriate for the nature and the size of business to ensure less false positives are produced.
- Ensuring screening rules are appropriately defined e.g. allow for the use of alternative identifiers.
- 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.
- Ensuring prominent flagging of matches so that they are clearly identifiable.
- Keeping calibration and automated systems under regular review to ensure they are fit for purpose.

5.3 Further information on screening practices may be found in a report published by the Commission in August 2014.

6. Systems for investigating a match

6.1 An institution should implement internal procedures for investigating whether a match against the UK Consolidated List is an actual match or a false positive.

6.2 In formulating such policies consider incorporating the following actions:

- Staff seeking sufficient information to enable them to confirm or eliminate a match.
- If necessary, staff making further enquiries of an intermediary, counter-party bank or the customer, or all of the above.
- The notification of potential target matches to senior management, particularly in cases where it cannot be determined if a potential target match is an actual target match.
- A process by which the Minister for External Relations is notified of confirmed matches or potential target matches that cannot be confirmed after investigation and escalation.
- Provision for a clear audit trail of potential target matches and decisions/actions taken.

7. Action required on discovering a confirmed or potential target match

7.1 In the case of a confirmed match, or a potential target match where further investigations and escalation procedures have not confirmed the position either way:

- Freeze assets.
- Block the provision of any financial service.
- Report the match to the Minister for External Relations. Where there is a requirement to make such a report, the relevant legislation will provide that such a disclosure is without prejudice to any duty of confidentiality or professional secrecy.
- Informing a customer that they are, or appear to be, subject to sanctions does not necessarily constitute tipping-off. The names of sanctioned individuals are publically available.
- Holding an account for a sanctioned party or processing a transaction involving a sanctioned party is not in itself grounds for filing a Suspicious Activity Report (**"SAR"**) with the Joint Financial Crimes Unit. With the exception of persons subject to terrorism related sanctions, only file a SAR if there is a particular suspicion of criminal activity beyond the fact the individual or entity in question is the target of sanctions.
- If you file a SAR about a sanctioned individual, then disclosing that you have filed a SAR will in the majority of cases constitute tipping-off.
- The filing of a SAR does not provide protection in respect of offences that may have been committed under sanctions legislation.

8. Information you may be required to provide

8.1 Following a report made to the Minister for External Relations, the reporter may be asked to provide:

- Information or other matters on which the knowledge or belief reported is based.
- Any information held about the designated person by which the person can be identified.
- The nature and amount or quantity of any funds or economic resources held by, or for, the designated person.

9. Obtaining a licence

9.1 A licence is written authorisation to allow an activity that would otherwise be prohibited by financial sanctions legislation, for example the release of funds to pay for legal representation. A licence may have conditions attached to it, such as reporting obligations. If an institution wishes to carry out an action contrary to a financial sanction, they should request, in writing, a licence from the Minister for External Relations before any action is taken.

9.2 The Minister for External Relations has published an Asset Freeze Licence Application Form which should be used by individuals or Jersey regulated entities seeking a licence from the Minister for External Relations to allow an activity or transaction to take place that would otherwise be prohibited under asset freezing (sanctions) measures.

9.3 For all queries in respect of its completion, institutions should contact the Ministry for External Relations at sanctions@gov.je.

10. International Obligations

10.1 As each country's sanctions measures tend to be applicable to nationals/citizens of that country and bodies constituted or incorporated under the law of that country, wherever those persons are situated, it is important to understand any obligations that follow from having links to another country. If an institution operates or is incorporated or constituted outside of Jersey, it should give consideration to sanctions obligations that may arise as a result. For example if you are a United States incorporated company with a branch in Jersey, the branch in Jersey should have regard to United States sanctions (see below). If you are a United States citizen employed in an institution in Jersey, again United States sanctions should be considered.

10.2 Depending on the provider, automated screening software used in respect of customer due diligence may also provide you with international sanctions information. To give an example, "World-Check" searches in relation to a customer should highlight any sanctions measures in place internationally in respect of a person.

10.3 The country profiles on websites such as www.knowyourcountry.com can also provide information on whether United Nations, European Union or United States sanctions are in place in respect of a particular country.

10.4 Although the aforementioned are useful information tools, further research would still required to establish what implications sanctions measures have for any customer business of an institution. If searches were to reveal a customer on sanctions lists in the United States, Canada and Australia, for example, consideration should be given to any way in which the institution, by way of its structure or operation and the remit of legislative provisions in those countries, may be in breach of those sanctions. Establishing that a customer is on a sanctions list in one or more countries is likely to also raise the question of reputational risk to the business and the Island, if business with that person is to be commenced or continued.

10.5 Article 11(3)(e) of the Money Laundering (Jersey) Order 2008 includes policies and procedures to determine whether a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country or territory that is subject to measures for purposes connected with the prevention and detection of money laundering, such measures being imposed by one or more countries or sanctioned by the European Union or the United Nations. The Commission does not consider that this provision requires an institution's policies and procedures to apply all sanctions measures imposed by one or more other countries to their business in Jersey. The reference to measures imposed by one or more countries is intended as a reference to FATF countermeasures as applied by one or more country. The only sanctions measures specifically referred to are those made by the European Union or the United Nations for purposes connected with the prevention and detection of money laundering (i.e. terrorism related sanctions). The Commission does, however, consider it appropriate for institutions to have regard to the way in which their business model may result in (i) breaches of local sanctions legislation beyond those sanctions concerned with terrorism and (ii) sanctions legislation in other countries.

United States Sanctions

10.6 The United States Government maintains a list of designated individuals and entities through the Office of Foreign Assets Control (**"OFAC"**).

10.7 United States financial sanctions are not automatically applicable in Jersey, but they do have far-reaching extra-territorial effect. This means that even if an institution is not operating, incorporated or constituted in the United States, OFAC sanctions may still be applicable. Institutions should be particularly mindful of OFAC sanctions if:

- They employ United States citizens or permanent aliens;
- Transact in US dollars;
- Enter into transactions involving United States operations or accounts; or
- Have United States offices, subsidiaries, branches or agencies or a relationship with a United States firm.

10.8 Some OFAC sanctions measures, for example those in place in respect of Iran, also specifically apply in respect of foreign financial institutions.

10.9 Failure to comply with OFAC sanctions could expose an institution to criminal or civil liability in the United States.

10.10 Institutions may find the following OFAC search tool of assistance:

http://apps.finra.org/rulesregulation/ofac/1/Default.aspx

Appendix: Examples of good and bad practice

Adapted from 'Financial services firms' approach to UK financial sanctions' issued by the Financial Crime and Intelligence Division of the Financial Services Authority (April 2009).

Good Practice	Bad Practice
Screening of directors, beneficial owners and third party payees of corporate customers	Assuming AML customer due diligence checks include sanctions screening
Use of 'fuzzy matching' in automated screening	Failure to understand and tailor a commercially available screening system
Screening entire customer base within a reasonable time following updates to the UK Consolidated List	Screening retrospectively
Regular review of the effectiveness of policy, procedures, systems and controls	Changes to policies, procedures, systems and controls not communicated to staff
Senior management involvement when name match cannot be verified	No or insufficient senior management oversight
Clear audit trail of potential matches, decision and actions with clear rationale	Reliance on firms, consultants or intermediaries to screen without ensuring this is done effectively