

Client Screening: Sanctions Lists

As time evolves, in regard to globalization and advancement in technology, the fight against money laundering and terrorist financing (ML/TF) is becoming more complex. As such, it is increasingly important for Regulated Entities, especially financial institutions, to screen their clients against sanctions lists administered by multiple jurisdictions and agencies. Accordingly, this newsletter will focus on the importance of screening clients and provides guidelines on managing sanctions risks.



The Importance of Screening Clients

The screening of transactions and clients is an essential component of an effective compliance program for the following reasons:

- To assist in identifying suspicious activities which may be indicative of ML/TF;
- To identify politically exposed persons (PEPs);
- To assess and understand your entity's risk profile and client demographic and composition;
- To manage reputational risk confidently; and
- To comply with legal and regulatory requirements.

How Often Should A Client Be Screened

The number of global sanctions/watch lists continue to grow and their data change almost on a daily basis, which may complicate the task of keeping up-to-date information and managing an efficient screening program. Therefore, it is vital for regulated entities to screen their clients prior to offering any products or services and continuously throughout the business relationship.

Regulated entities should apply a risk based approach to checking their clients against sanctions lists. To do so, each client must, firstly, be risk rated. Thereafter, high risk clients should be screened at least every one (1) to three (3) months, while, low to medium risk clients should be screened every three (3) to nine (9) months.

Screening Process



The following outlines steps to screening a client or entity:

- i. Obtain the client's personal information (full name, address, contact number, date of birth, occupation, etc.) via application forms or questionnaires. Two (2) pieces of identification documents (IDs) and a proof of address verification document should also be collected to verify the information provided on the forms. In the case of corporate clients, a business licence and incorporation documents should be collected to establish ownership and the nature of the business/company. Additionally, the personal information, as well as, IDs and proof of address verification documents should be obtained for each beneficial owner and director of the business/company.
- ii. Screen each client (also director and beneficial owners) against the sanctions lists. Some entities are equipped with systems that automatically screen their clients against sanction lists on a regular basis, while other institutions manually conduct their searches via a due diligence software; either option is viable once the checks are consistently completed.
- iii. Are there any hits? Compare the hit with all information provided on the client to rule out any 'false positives'.
- iv. Approve, deny, escalate, or collect more information on the client depending on your findings.

Topics Discussed:

- ⇒ **The Importance of Screening Clients**
- ⇒ **How Often Should A Client Be Screened**
- ⇒ **Screening Process**
- ⇒ **Identifying False Positives**
- ⇒ **What To Do If There Is An Actual Hit**
- ⇒ **Applying Enhanced Due Diligence**
- ⇒ **Why A Customer May Appear On A Sanctions List**
- ⇒ **Notable Sanctions Lists**
- ⇒ **Due Diligence Software/Systems**
- ⇒ **References**

Identifying False Positives

A False Positive refers to a situation where a client is incorrectly identified as a match against a record on a sanctions, risk, or PEP register due to similarity in names.

Legitimate clients are sometimes flagged as problematic due to “false” hits, causing entities to spend time, money and resources investigating these ‘false positives’. To rule out a false hit one should:

- i. Firstly compare the clients full name to the match. If the client’s first, middle or surname does not match the record on the sanction list, then it is likely that it is a ‘false positive’.
- ii. Other factors such as date and place of birth, gender and address can also be used to identify a ‘false positive’.

What To Do If There Is An Actual Hit/Match

Subsequent to analyzing the hit, if it is determined that the client is actually a match, then the entity’s Compliance Officer should become involved. Depending on the findings of the search, the Compliance Officer should determine whether the entity would carry on business with the client.

In situations where the client is wanted by law enforcement or was charged/convicted for crimes such as embezzlement or ML/TF, it is advised that any business relationship with that client be discontinued. Depending on the severity of the crime, the Compliance Officer should also file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit. Be mindful that the client should in no way be tipped off on the findings of your investigation.

In other cases, where it is determined that the business relationship with the client will be maintained, then enhanced due diligence procedures should be employed.

Applying Enhanced Due Diligence (EDD)

The following highlights some recommended enhanced due diligence procedures:

- Source of Funds/Wealth Forms — clients could be asked to complete a Declaration Form in cases where the source of funds/wealth is difficult to establish.
- Monitoring of Transactions — to ensure that clients’ transactions are consistent with their income and expected activity.
- Employing the services of an independent Due Diligence Service Provider to perform a detailed background check on the client.
- Ensuring that the customers IDs and other verification documents are up to date at all times.

Why A Customer May Appear On A Sanctions List

A customer may appear on a sanctions list for various reasons, such as:

- * Narcotics trafficking;
- * Involvement in terrorist activities;
- * Tax evasion;
- * Embezzlement;
- * Fraud;
- * Committing other criminal offenses (such as homicide, theft, etc); or
- * The individual is a PEP.



Notable Sanctions Lists

The following is a list of notable global watch/sanctions lists.

- OFAC Specially Designated Nationals (SDN) & Blocked Persons
- FBI Most Wanted Terrorists & Seeking Information
- FBI Top Ten Most Wanted
- INTERPOL Most Wanted List
- Bank of England Sanctions List
- OSFI - Canadian Sanctions List
- United Nations Consolidated Sanctions List
- Politically Exposed Persons List
- European Union Terrorism List
- World Bank Ineligible Firms



Due Diligence Software/Systems

Regulated entities are encouraged to use a due diligence software such as World Check, Dogpile and World Compliance. These software programs are designed to consolidate the findings from the sanctions lists noted above.

For small entities, where cost is a factor, Google searches can be conducted to unveil any ‘bad’ media articles on the client. In cases where derogatory information is uncovered through these searches, additional information should be collected to determine whether to accept or continue business with the client.

Reference:

- *Anti-Terrorism (Prevention of Terrorist Financing) Regulations (ATR), No. 47 of 2011.*
- *Anti-Money Laundering Regulations (AMLR), No. 46 of 2011.*
- <https://www.lawsociety.org.uk/support-services/advice/articles/checking-the-sanctions-list/>
- <https://www.cgi.com/sites/default/files/white-papers/cgi-sanctions-compliance-whitepaper.pdf>