alessa

Definitions, Obligations and Best Practices

Sanctions Screening and Watchlist Filtering

Introduction

In 2019, Standard Chartered Bank (SCB) was ordered to pay $1.1 billion for conspiring to violate the International Emergency Economic Powers Act (IEEPA) and other international money laundering controls. It included a criminal conspiracy involving some 9,500 transactions worth a quarter of a billion dollars to the benefit of sanctioned Iranian entities.

More than half of the transactions were the result of deficiencies in SCB's compliance program, which allowed customers to request U.S. dollar transactions from within sanctioned countries.

"When a global bank processes transactions through the U.S. financial system, its compliance program must be up to the task of detecting and preventing sanctions violations—and when it is not, banks have an obligation to identify, report, and remediate any shortcomings" said Assistant Attorney General Benczkowski on the Standard Chartered case.

Not just banks in the U.S. are facing the penalties for transacting with sanctioned entities. Less than two weeks later, U.S. officials fined one of Europe's largest banks, UniCredit Bank AG (UCB AG), more than $1.3 billion for processing nearly $400 million for sanctioned entities and countries, including Iran, Libya and Cuba.

UCB AG not only did business with sanctioned entities, they even altered their screening to strip sanctioned countries from transaction information in a conspiracy run by compliance staffers.

Prosecutors said the bank "engaged in this criminal conduct through a scheme, formalized in its own bank policies, designed to conceal from U.S. regulators the involvement of sanctioned entities in certain transactions." In one instance, the bank actually used its sanctions screening software to find and release illegal transactions to blacklisted regimes.

According to the Manhattan District Attorney's office, since 2009, eleven banks have forfeited more than $14 billion in settlements for U.S. sanctions violations and violations of New York State law, including:

- **Standard Chartered Bank** for $327 million in 2012 and $720 million in 2019
- **Société Générale** for $162.8 million in 2018
- **Crédit Agricole Corporate and Investment Bank** for $312 million in 2015
- **Commerzbank** for $342 million in 2015
- **HSBC Bank** for $375 million in 2012
- **ING Bank** for $619 million in 2012
- **Barclays Bank** for $298 million in 2010
- **Credit Suisse AG** for $536 million in 2009
- **Lloyds TSB Bank** for $350 million in 2009

This white paper looks at how to monitor and screen individuals, entities and transactions as well as best practices to optimize the results in order to avoid some of the penalties and fines associated with sanction violations.

Screening Guidance from Industry Body

The Wolfsberg Group recommends that financial institutions (FIs) should first identify and assess the sanctions risks to which it is exposed and to implement a screening program that considers the following:

- Jurisdictions where the FI is located and its proximity or relationship with sanctioned countries
- What international and domestic customers the FI has, where they are located and what businesses they conduct
- Volume of transactions and distribution channels
- What products and services the FI offers and whether those products represent a heightened sanctions risk, through cross-border transactions, foreign correspondent accounts, trade related products or payable-through accounts

According to Wolfsberg, the fundamental pillars of a Financial Crime Compliance (FCC) program should include:

- **Policies and procedures** - defining requirements for what must be screened and how alerts should be handled and judged.
- **Responsible person** - ensuring appropriate skills and experience in understanding sanctions requirements and how these might influence screening outcomes and decisions.
- **Risk assessment** - applying risk based decisions to determine what to screen, when to screen, what lists to use and how exact or "fuzzy" to set the screening filter.
- **Internal controls** - FIs are expected to document how their screening systems are configured and demonstrate that it is reasonably expected to detect and manage the specific sanctions risks.
- **Testing** - validate that the screening system is performing as expected and assess its effectiveness in managing specific risks.

The group also points out that a risk-based approach means understanding sanctions screening can never detect every possible risk. That means the effectiveness of screening will vary among FIs, even when they are using the same screening protocols and solutions.

While designing and configuring the screening process, Wolfsberg recommends the following:

- **Articulate** the specific sanctions risk that the FI is trying to prevent or detect
- **Identify** and evaluate potential exposure to sanctions risks through an FI's products and services and its relationships with customers
- **Ensure** the screening tool includes a well-documented understanding of the risks and how they are managed

FIs must ensure screening includes information in a format that makes screening more effective. For example, screening based on transactions containing only the International Securities Identification Numbers (ISIN) may be insufficient to raise an alert or distinguish between a true match and a false positive.

Screening and a Risk-Based Approach

According to the Financial Action Task Force (FATF), "a risk-based approach means that countries, competent authorities, and banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk."

Taking a risk-based approach means understanding that it is not possible to detect every possible risk. However, regulators expect financial institutions to perform regular risk assessments and update their policies and procedures to meet changing levels of risk.

To adopt a risk-based approach, first FIs need to examine their business risks which includes

- Customer risk
- Product risk
- Jurisdiction risk

Organizations should also look at their risks associated with changing regulatory rules and expectations of regulators.

When looking at customer risk, financial institutions should capture and record data about the customer throughout their relationship in order to create an accurate view of the risks associated with that customer. During onboarding, data that is, or may be, valuable for an accurate customer risk score includes:

- Customer characteristics (name, address, date of birth, profession etc.)
- Corporate entities characteristics (industry, annual revenue, number of employees, geographies, etc.)
- Anticipated utilization and activity of account
- Presence on any sanctions or watch lists including politically-exposed persons (PEP) lists

Once a customer has been onboarded, ongoing monitoring ensure that FIs are alerted to any elevated liabilities or risk scores. Areas that may affect a customer's score include:

- Out-of-pattern activities or transactions
- Foreign wire transactions
- Global trade activities
- Types and amounts of returned credits
- Number of currency transaction or suspicious activity reports
- Number of suspicious activity alerts triggered by the AML solution

Using Sanctions and Watch Lists

Sanction and watch lists are a critical tool for any risk or sanctions screening program. There are several sanctions lists that FIs should rely on:

OFAC and United Nations Consolidated List

The **Office of Foreign Assets Control**[1] (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific.

In addition, the **United Nations Consolidated List**[2] includes all individuals and entities subject to measures imposed by the Security Council. The inclusion of all names on one Consolidated List is to facilitate the implementation of the measures, and neither implies that all names are listed under one regime, nor that the criteria for listing specific names are the same.

Specially Designated Nationals and Blocked Persons

Before an FI starts doing business for the first time with a new customer, it should screen against published lists of known or suspected terrorists for a potential match. One of the most comprehensive and used lists is OFAC's Specially Designated Nationals and Blocked Persons list.

Updated often, it contains hundreds of names of individuals and businesses the U.S. government considers to be terrorists or international narcotics traffickers and others that are covered by U.S. foreign policy and trade sanctions.

[1] *https://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx*

[2] *https://www.un.org/securitycouncil*

Politically Exposed Persons Lists

According to the Federal Financial Institutions Examination Council (FFIEC), Bank Secrecy Act, a politically exposed person (PEP) is classified as:

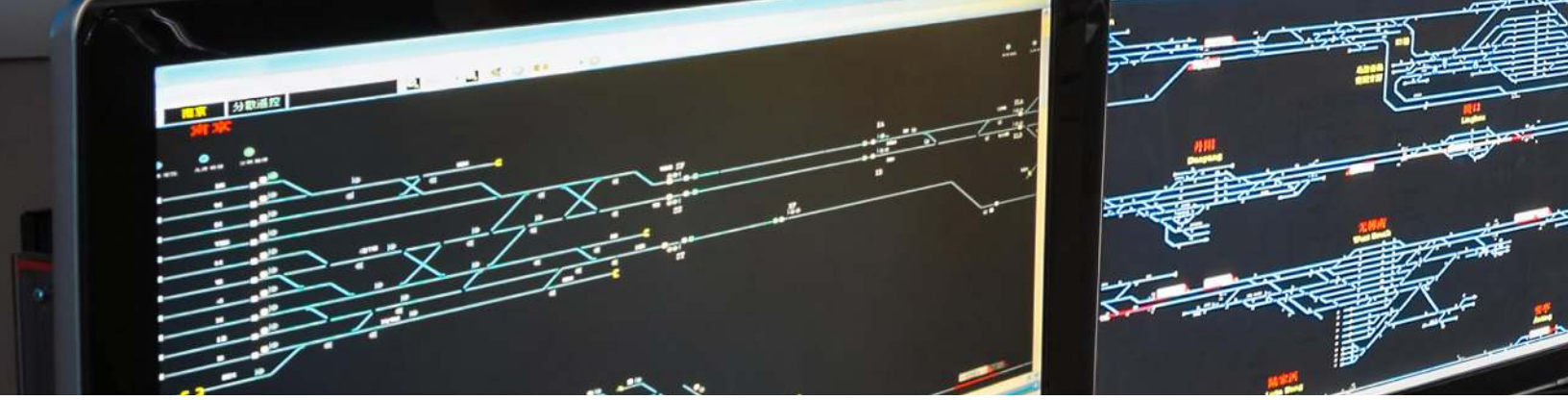
- A current or former:
  - Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not)
  - Senior official of a major foreign political party
  - Senior executive of a foreign-government-owned commercial enterprise
- A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.
- An immediate family member (including spouses, parents, siblings, children, and a spouse's parents and siblings) of any such individual.
- A person who is widely and publicly known to be a close associate of such individual.

Financial institutions should look at the definition of a PEP for each jurisdiction, as these may slightly vary, which adds to the level of complexity when screening for this class of individuals. For some jurisdictions, a PEP is an individual who meets any of the following criteria:

- Heads of State and their deputies
- Heads and Deputies of Regional Government
- Heads of Government Agencies and Cabinet Ministers
- Regional / Provincial Government Ministers
- Members of National Parliament
- Members of Provincial Legislature
- Senior Civil Servants
- Local Government Officials (City Mayors, Councillors, Municipal Managers)
- Senior Embassy and Consul Staff
- Members of House of Traditional Leadership (Kings and Chiefs)
- Senior members of the army and / or influential officials, functionaries, and military leaders and people with similar functions international or supernatural organizations
- Senior members of the police services
- Senior members of the secret services
- Senior members of the judiciary
- Senior and / or influential representatives of religious organisations
- Political leaders
- Labour group officials
- Influential functionaries in the private sector and public services administration
- Key leaders of state owned enterprises
- Private companies, trusts, foundations, or other juristic persons owned or co-owned by PEP's directly or indirectly
- Any business and / or joint venture that has been formed by, or for the benefit of a senior political figure
- Close Family who are defined as individuals who are related to the PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership including:
  - Spouses and life partners
  - Children and siblings
  - Parents and grandparents
  - Uncles and aunts
  - Nephews and nieces
  - Relatives by marriage

The duration that each individual is classified as a PEP will also vary by jurisdiction.

FIs should examine, as far as reasonably possible, the background and purpose of all PEP transactions. Finally, they should also conduct enhanced customer due diligence (CDD) measures, consistent with the risks identified.



The account opening or onboarding process is the most effective time to obtain the required information needed to open and maintain an account for a PEP. Examples of enhanced CDD measures that could be applied for PEP's include:

- Have appropriate risk-management systems and data lists to determine whether the customer or the beneficial owner is a politically exposed person
- Obtaining additional information on the receiving party (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of the customer and beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining additional information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- The requirements for all types of PEP should also apply to family members or close associates of such PEPs

Many large FIs employ screening technology with risk intelligence lists or third parties to conduct ongoing PEP screening against their customer base to alert them for potential PEP matches.

These potential matches are reviewed to determine whether:

- The individual is a match to the customer.
- The past and / or present political positions listed.

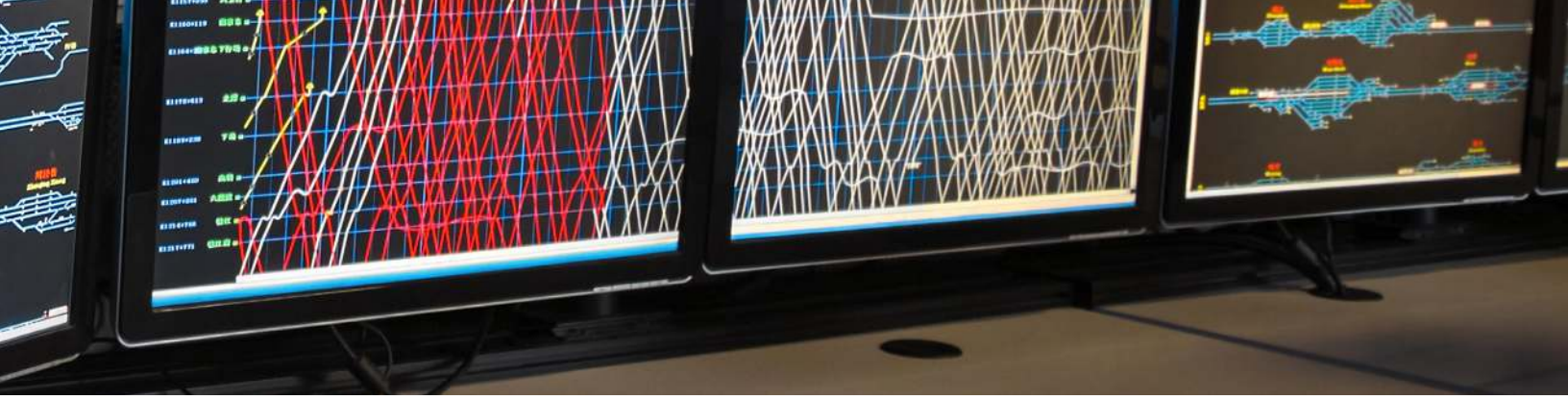
The PEP lists are also sent by supervisory regulatory authorities such as Central Banks or Financial Intelligence Units to the commercial banking and financial institutions network. The excel format file containing the name, surname, position held, date of birth, and related persons can be integrated in the main core system in order to conduct cross checking verifications with the transactions.

Duplicate values of names may exist in rendering cross checking results, but filtering with additional verification features is possible since the information regarding these specific types of customers is more accurate compared to other risk lists.

Ongoing monitoring process of PEPs

Ongoing monitoring of PEPs should be conducted at least every 12 months (periodic reviews) as part of the compliance monitoring process or as a result of a triggering event. Periodic reviews must be completed for all clients, identified as PEP or those clients with an indirect relationship through their association with a PEP. A trigger event could include, but is not limited to:

- A change in PEP's role
- A change in the PEP's residency
- A new application involving the same PEP
- Adverse media report
- The receipt of a court order, subpoena etc, against the client



The following information and documentation must be reviewed, reconfirmed and updated when conducting a periodic review of a PEP client.

- All KYC information
- The relevance of the CDD conducted initially
- Where adverse information such as ongoing litigation or regulatory proceedings was noted as part of the on-boarding information, further checks must be undertaken to ascertain any outcomes or obtain updated information.

Monitoring should include but not be limited to:

- Selecting patterns of transactions that need further examination
- Verifying information on the reasons for performed transactions
- Verifying if the intended nature of the performed transactions make economic sense
- Verifying if the amounts and number of transactions are rational

Domestic Lists

In addition to the above lists, there are many domestic lists that FIs should screen against depending on the products that they offer and their risk tolerance. Below are some examples.

CANADA: OSC (Ontario Securities Commission) warning list

This list contains individuals and companies that appear to be engaging in activities that may pose a risk to investors. The OSC urges investors to be cautious about these individuals and companies.
The list can be found at: *https://www.osc.gov.on.ca/en/Investors_warning-list_index.htm#here*

USA: The New York Department of Financial Services (DFS) for AML regulation 504

The section 504.3(b) states that each regulated institution shall maintain a filtering program, which may be manual or automated, reasonably designed for the purpose of interdicting transactions that are prohibited by the OFAC. To comply with this regulation, FIs should rely on the OFAC list of publications.

USA: CIA

The CIA list provides information on the US State Department's designated Foreign Terrorist Organizations headquartered in a specific country, which may or may not be a group's country of origin.
The list can be found at: *https://www.cia.gov/library/publications/the-world-factbook/fields/397.html*.
Entities on these lists can typically be found on lists provided by OFAC or data list providers.

USA: FBI

The FBI have published a terrorism list which is found here: *https://www.fbi.gov/wanted/terrorism*. Individuals on these lists can typically be found on lists provided by OFAC or data list providers.

Best Practices When Using Sanctions Lists

When screening an individual against sanctions lists, here are some factors to consider:

Use the updated version of the lists

Usually the lists are updated and amended by the relevant agency / regulatory body managing them. Institutions should be aware to always periodically upload the latest version of these lists in their core system. Usually the list updates are publicised by the relevant governing agency or regulatory body in charge of managing them. A control should be in place to periodically check for list updates.

Use reliable sources

There are numerous sources providing assistance in sanction list screening services. Any institution relying on these services should take into consideration the reliability of the sources of information. The most reliable lists are those directly issued by governing agencies or regulatory bodies.

Assess the accuracy of the list

The sanction lists issued are usually in a format which can be easily edited, erased or modified. Institutions relying on these lists should be diligent in making sure no prior modification has occurred before uploading them into their core system.

Look at geographic scope of list application

Institutions should determine which lists are to be screened in all jurisdictions of its operations and which are to be screened only locally, or within a certain jurisdiction or jurisdictions. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Be aware of common prefixes, secondary names, suffixes

FIs and businesses that receive lists of suspected terrorists from government agencies have learned that screening customer lists for suspected terrorists can be a challenge due to naming customs and protocols, aliases, the use of non-Latin characters and more. For example, when looking at Arabic names

- All names are transliterated from an Arabic script in which short vowels are most often left out, for instance name Mohammed might be written on a financial account as Mohamed or Mohamad.
- Arabic names are typically long. A person's second name is the father's name. If a "bin" or "ibn" precedes the name, it indicates "son of." If a family name is included at the end, it will sometimes have "al" preceding it.
- There is widespread use of certain names such as "Mohamed," "Ahmed," "Ali," or any name with the prefix "Abd-" or "Abdul," which means "servant of," and is followed by one of 99 suffixes used to describe God.
- Many Arabic names begin with the word "Abu." If it is a first name, it is probably not the person's given name, because "Abu" means "father of." "Abu," followed by a noun, means something like "freedom" or "struggle," and is used by both terrorists and legitimate political leaders. Only when "Abu" is a prefix of a surname should it be accepted as a given name.

When screening, do not forget to refer to the "Also Known As" alternative names as well.

Address duplicate values

Sometimes there is no consistency with regard to the format of the identifiable features that exist in these lists for different specially designated individuals or entities and blocked persons. But, these lists are provided based on their intelligence gathered information for each specific individual or entity. In this regard, there can be cases where a particular identifiable feature is missing, in this way leaving potential room for duplicate values to be highlighted when performing searches.

In order to avoid any misidentification based on identifiable features such as repeated names or countries, the system search should follow this logic (example below showcases a Specially Designated Individual):

> *ABDURAKHMANOV, Maghomed Maghomedzakirovich (a.k.a. "Abu al Banat"; a.k.a. "Abu Banat"), Turkey; Syria; DOB 24 Nov 1974; POB Khadzhalmahi Village, Levashinskiy District, Republic of Dagestan, Russia; citizen Russia; Passport 515458008 (Russia) expires 30 May 2017; alt. Passport 8200203535 (Russia) (individual) [SDGT].*

- First search to be performed should be based on the Name (Example: Maghomed Maghomedzakirovich). If duplicate matches exist in the institution's database with other existing customers, the system's logic should move on to the next identifiable feature (Example: Passport Number – 515458008) and so on, by including in the logic other features such as: Date of Birth, POB, Address, Document Expiration Date, etc.
- If such logic can be constructed in the system, there can be no issue with duplicate values. Otherwise, manual checks can be performed by cross-checking all the transactions against the risk lists with spreadsheets.
- Another solution is to consider the services of electronic solutions offered by third parties that have incorporated risk lists, but data system integration is required.

Remember "50 Per cent" rule when looking at entity ownership

According to the Department of Treasury in the U.S., the August 13, 2014 guidance[4] states that if one or more blocked persons or entities own 50 per cent or more in aggregate of a non-listed entity (either directly or indirectly), that entity is also automatically blocked. This section requires U.S. persons and foreign entities owned or controlled by U.S. persons, to refrain from transacting business with (including negotiating and contracting) or investing in a blocked entity and to freeze any property of the entity that they hold.

Consequently:

- Any entity owned in the aggregate, directly or indirectly, 50 per cent or more by one or more blocked persons is itself considered to be blocked
- The property and interests in property of such an entity are blocked regardless of whether the entity itself is listed in the annex to an Executive order or otherwise placed on OFAC's list of Specially Designated Nationals ("SDNs")
- Accordingly, a U.S. person generally may not engage in any transactions with such an entity, unless authorized by OFAC. [Furthermore] U.S. persons are advised to act with caution when considering a transaction with a non-blocked entity in which one or more blocked persons has a significant ownership interest that is less than 50 per cent or which one or more blocked persons may control by means other than a majority ownership interest
- Such entities may be the subject of future designation or enforcement action by OFAC

According to the EU regulations, the EU applies a 50 per cent rule and criteria to establish the ownership and control of an entity to ascertain whether it is subject to sanctions restrictions. If a listed individual has 50 per cent or more ownership of a non-listed entity, EU persons/entities are prohibited from making available funds and economic resources to that entity.

It may also be prohibited to transact with that entity if the listed person can "control" it. In such a case, transacting with the non-listed entity is viewed as an indirect transaction for the benefit of the listed individual and is therefore prohibited.

[4] *https://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf*

OFAC Compliance Program

In addition to providing sanctions lists, OFAC provides compliance regulations. OFAC-issued regulations apply not only to U.S. entities, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. OFAC encourages FIs to take a risk-based approach to designing and implementing an OFAC compliance program. In general, the regulations that OFAC administers require entities to do the following:

- Block accounts and other property of specified countries, entities, and individuals
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals

The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the institution.

OFAC has the following requirements:

Risk assessment

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the FI. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the institution prepares its risk assessment.

Management should structure the AML compliance program to adequately address its risk profile, as identified by the risk assessment. Management should understand the AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control AML risks.

Internal controls

The policies, procedures, and processes should address how the FI will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both.

Blocked transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities.

For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC-designated party to the transaction, it must be blocked. FIs must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

Prohibited transactions

In some cases, an underlying transaction may be prohibited, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected (not processed).

For example, sanctions regulations prohibit transactions in support of commercial activities in a specific country. Therefore, a U.S. bank would have to reject a funds transfer between two companies, which related parties are not Specially Designated Nationals or Blocked Persons (SDN), but involving a transaction to a company in a country listed in specific sanctions.

In some cases, OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives.

Reporting

Institutions must report all blockings to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30). Once assets or funds are blocked, they should be placed in a separate blocked account. Prohibited transactions that are rejected must also be reported to OFAC within 10 business days of the occurrence.

FIs must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

Independent testing

Every institution should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties.

Responsible individual

It is recommended that every FI designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC compliance program, including changes or updates to the various sanctions programs, and the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the bank's OFAC risk profile.

Training

The FI should provide adequate training for all appropriate employees on its OFAC compliance program, procedures and processes. The scope and frequency of the training should be consistent with the bank's OFAC risk profile and appropriate to employee responsibilities.

Dos and Don'ts to Avoid OFAC Sanction Violations

Erich Ferrari, an attorney for Ferrari & Associates, P.C. who specializes in OFAC matters, wrote about the OFAC framework in a blog, spelling out its common causes for sanctions violations in easy to understand dos and don'ts:

Do: Have an OFAC sanctions compliance program.

Do: Consult legal counsel or OFAC sanctions expertise to understand the scope and applicability of OFAC-administered regulations.

Don't: Refer business opportunities to, or otherwise approve or facilitate those opportunities of, your company's foreign based operations and subsidiaries.

Don't: As a non-U.S. person, re-export U.S.-origin goods, services, or technology to sanctioned jurisdictions or sanctioned persons, particularly if you have signed a contract or received other documentation that has informed you that you cannot do so.

Don't: As a non-U.S. person, cause U.S. dollar payments to be remitted through the U.S. or by U.S. persons for transactions that in any way involve sanctioned persons or jurisdictions, and definitely do not in any way try to hide that a cross border U.S. dollar payment is related in some way to a sanctioned person or jurisdiction.

Do: Make sure that your sanctions screening software and filters are adequate, continuously tested, and calibrated to ensure that sanctions risk is being appropriately mitigated.

Do: Good due diligence. Don't slack on the quality of your due diligence, and if you don't have the knowledge or resources to do it appropriately outsource it until you can devote adequate resources and processes to conduct it. Account for ultimate beneficial ownership, geographic risk, and all counter-parties. Also, conduct transactional due diligence and monitoring.

Do: Follow OFAC's Framework and ensure that your sanctions compliance program is addressing sanctions-risk globally and is consistently applied and tested across operations and business lines.

Don't: Engage in strange payment practices. This is particularly true when it comes to receipt or remittance of payments from or to third parties. If the manner of payment requested by a counter-party appears unusual or novel, ensure that the payment can be made through normal channels.

Don't: Be the person at your company that comes up with a novel way to "get around" the sanctions. If you're looking for loopholes, you're looking for trouble. OFAC and other law enforcement agencies are becoming bullish on going after individuals for facilitating sanctions violations of the companies they work for. Don't get the horns – promote compliance before OFAC promotes enforcement.

"OFAC's Framework is a welcome development for many in the sanctions compliance world," Ferrari wrote. But he cautions that the clarity from the regulator means more responsibility for FIs. "That said, it does signal that expectations are being elevated and that organizations need to make sure they have their compliance practices in order now that OFAC has made clear what good practices look like."

Monitoring High-Risk and Other Controlled Jurisdictions

Some countries and jurisdictions pose a high risk to financial entities. These include countries subject to OFAC sanctions, countries identified as supporting international terrorism, jurisdictions determined to be of primary money laundering concern and subject to special measures, and jurisdictions or countries with deficiencies in combating money laundering and terrorist financing identified by international entities such as FATF.

As part of its ongoing review of compliance with the AML/CFT standards, the FATF identifies jurisdictions that have strategic AML/CFT deficiencies or that pose a risk to the international financial system. The FATF reviews jurisdictions based on threats, vulnerabilities, or particular risks arising from the jurisdiction. OFAC's countries list is compiled based on national security and United States foreign policy goals.

FIs must have the updated FATF and OFAC countries lists incorporated into their core systems in order to filter the transactions against these countries periodically. If possible, matching is identified, further analysis in the form of enhanced due diligence should be conducted by evaluating other factors such as:

Initiating and receiving parties:

- Screen the initiating and receiving parties against risk lists for possible matching
- Screen the initiating and receiving parties against the existing database of filed SAR or STR for possible matching
- Make further analysis (if such information is available), on the customer's occupation, nature of business, categorization, beneficial ownership, etc

Transaction amounts: If the amounts significantly deviate from the expected weighted average amounts of the specific historical data the entity has in the particular countries.

Number of transactions: If the number of transactions exchanged between the initiating and receiving parties make reasonable economic sense in a reasonable timeframe.

Nature of transaction: If the transactions involve high-risk countries and product types.

Screening High-Risk Professions and Businesses

Aside from specific individuals and businesses, it is important to screen and apply extra diligence to class of individuals and businesses that are at high-risk to be used for money laundering

Not for Profit Organizations (NPO)

NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". The FATF requires Financial Entities to conduct enhanced due diligence on the NPOs by focusing in the following areas:

- The purpose and objectives of their stated activities;
- The identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information could be publicly available either directly from the NPO or through appropriate authorities.
- NPOs could be required to issue annual financial statements that provide detailed breakdowns of incomes and expenditures.
- NPOs could be required to have appropriate controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPOs stated activities.
- NPOs could be required to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries and associate NPOs and they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations.
- Ascertain if the records of domestic and international transactions are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the organisation.

Charities or non-profit organizations have the following characteristics that are particularly vulnerable to misuse for money laundering:

- Enjoy public trust
- Have access to considerable sources of funds
- Cash-intensive
- Have a global presence, often in or next to those areas that don't have tight controls
- Often subject to little or no regulation and/or having few obstacles to their creation

The following are possible indications for suspicious activity:

- Frequent large cash deposits in the accounts
- High volume of transactions in the account
- Lack of a clear relationship between the NPO activity and the nature of the accountholder's business

Designated Non-Financial Businesses and Professions

Designated Non-Financial Businesses and Professions have the following characteristics that are particularly vulnerable to misuse for money laundering:

- Withdrawal of assets through transfers to unrelated accounts or to high-risk countries;
- Frequent additions to or withdrawals from accounts;
- Cheques drawn on, or wire transfers from, accounts of third parties with no relation to the client;
- Clients who request custodial arrangements allowing anonymity;
- Transfers of funds to the adviser for management followed by transfers to accounts at other institutions in a layering scheme;
- Investing illegal proceeds for a client;
- Movement of funds to disguise their origin;

Professionals that fall within this class include:

- Lawyers, notaries, other independent legal professionals and accountants
- Investment, commodity advisers, trusts and company service providers
- Vehicle sellers
- Precious metals, jewellery, art and antiques dealers and auctioneers

According to FATF recommendations, the following guidelines should be followed when conducting CDD for Designated Non-Financial Business and Professions:

- Require all professionals to provide names and addresses.
- Ask that they sign and date a form that states that the asset was not stolen and that they are authorized to sell it.
- Verify the identities and addresses of new professionals and customers.
- Be suspicious of any item whose asking price is not commensurate with its market value
- Obtain further additional information on the beneficial ownership of the underlying transactions
- Carry out additional information searches (verifiable adverse media searches)
- Make additional checks on the legitimacy of the source of funds
- Make further verifications on the intended nature of the account opening / transactions
- Identifying and verifying the customer's identity using reliable and independent sources of data and information
- Ensure that the transactions being conducted are consistent with the institution's knowledge of the customer

When reviewing transactions of these entities look for the following:

- Structuring cash deposits below the reporting threshold, or purchasing assets/vehicles with sequentially numbered cheques or money orders.
- Conducting successive transactions of buying and selling to produce complex layers of transactions.
- Accepting third-party payments, particularly from jurisdictions with ineffective money laundering controls.

Shell Corporations

A shell company is a company that at the time of incorporation has no significant assets or operations. Shell companies can be set up in onshore, as well as offshore locations, and their ownership structures can take several forms. Shares can be issued to a natural or legal person or in registered or bearer form.

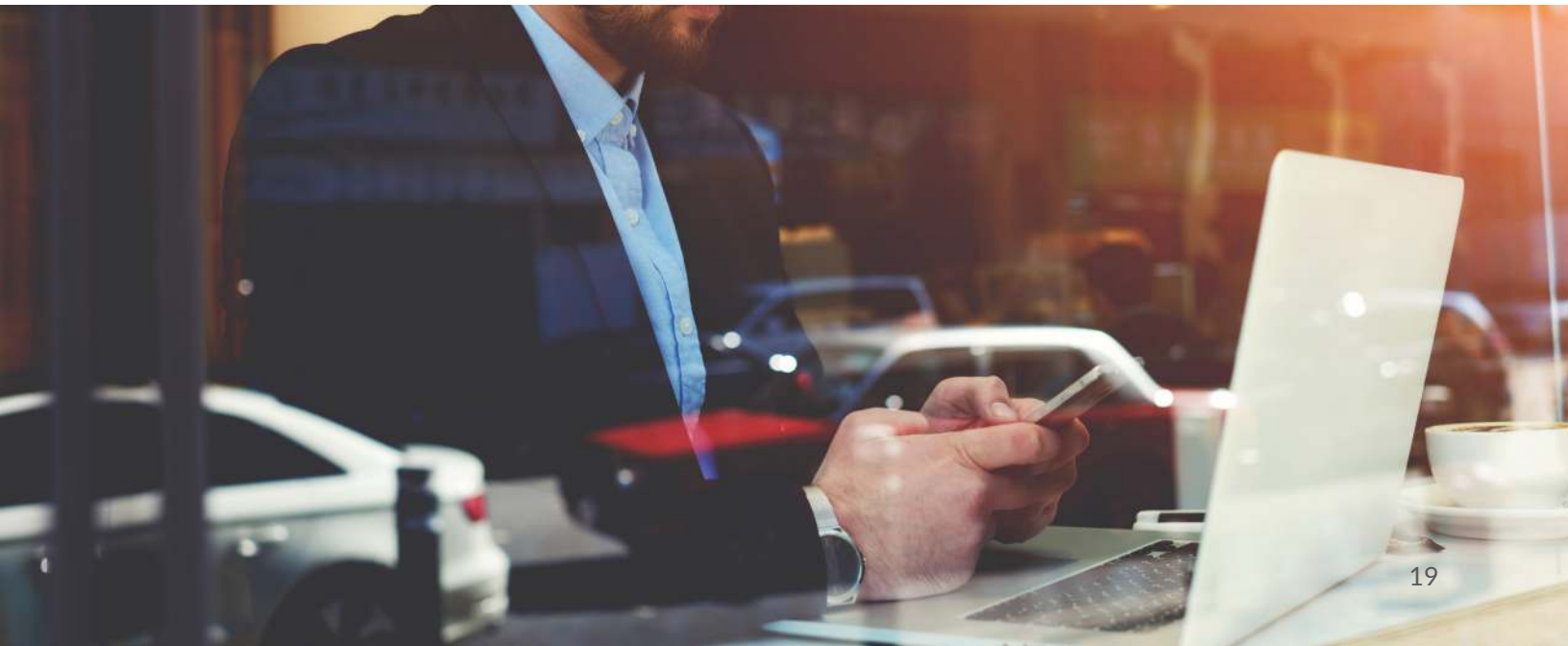
Some companies can be created for a single purpose or to hold a single asset. Others can be established as multipurpose entities. FATF has stated that shell corporations are widely used mechanisms to launder the proceeds from crime. The ability for competent authorities to obtain and share information regarding the identification of companies and their beneficial owner(s) is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering.

Through the use of shell companies, the launderer can create the perception that illicit funds have been generated from a legitimate source. Once a shell company is established, commercial accounts can be created at banks or other financial institutions.

Especially attractive to money launderers are businesses that customarily handle a high volume of cash transactions, such as retail stores, restaurants, bars, video arcades, gas stations, food markets, etc. Illicit revenues can then be deposited into bank accounts as legitimate revenue, either alone or commingled with revenue legitimately produced from the business.

Indications of suspicious activity relatable to shell companies:

- Frequent and unexplainable movements of assets between accounts in various financial institutions;
- Frequent and unexplainable cash flows between financial institutions in different geographic areas;
- Clients for which is difficult to identify the real owner (offshore companies).
- Fictitious business expenses and / or false invoicing
- Paying out fictitious salaries



Cash Intensive Businesses

Most of these businesses might be conducting legitimate business but extra precaution should be exercised with the following (but not limited to):

- Convenience, retail, liquor stores
- Restaurants
- Cigarette distributors
- Privately owned automated teller machines (ATM)
- Vending machine operators
- Parking garages

Aspects of these businesses that make them susceptible to ML/TF include:

- Enable significant volumes of transactions to occur rapidly
- Allow the customer to engage in transactions with minimal oversight by supervisory institutions
- Afford significant levels of anonymity to the users
- Have an especially high transaction or investment value

The following enhanced due diligence measures should be considered when dealing with these businesses:

- Verify and gather information on the purpose of the account
- Verify and gather information on the volume, frequency, and nature of currency transactions
- Assess the risk of the primary business activity, products, and services offered
- Analyse the business structure type
- Assess the geographic locations and jurisdictions of operations
- Assess the availability of information and cooperation of the business in providing information

Pre-paid Card Issuers

Pre-paid cards have the same characteristics that make cash attractive to criminals: they are portable, valuable, exchangeable and anonymous. The cards, many of which are branded by Visa or MasterCard, can be purchased and "loaded" with money by one person and used like regular debit cards by another person to make purchases or ATM withdrawals anywhere in the world.

The potential risk factors associated with pre-paid cards include:

- Anonymous card holders;
- Anonymous funding;
- Anonymous access to funds;
- High value limits and no limits on the number of cards individuals can acquire;
- Global access to cash through ATMs;
- Offshore card issuers that may not observe laws in all jurisdictions; and
- Substitute for bulk-cash smuggling.

The following are possible indications of suspicious activity:

- Excessive number of cards for single customers
- Excessive shipped cards outside the country of origin / residential area
- Excessive number of failed authorisations
- Consecutive transactions below the reporting threshold
- Frequent changes on activity addresses
- Unexplainable transactions that do not establish a logical economic ground
- Multiple withdrawal transactions performed at different ATMs within the same day

The following enhanced due diligence measures should be considered when dealing with these businesses:

- Assess the accuracy of the provided information by verifying it against open sources searches.
- Analyse the reasons behind the excessive failed authorisations
- Check for numerous cash deposits performed by the same individuals within the same day in different branches just below the reporting thresholds.
- Analyse the reasons behind frequent / excessive customer service calls.
- Analyse the reasons behind frequent / excessive credit refunds from multiple cards in the same account.

Conclusion

As demonstrated by the Standard Chartered Bank (SCB) case, failing to comply with sanctioned entities can result in hefty fines. Financial institutions should apply extra diligence when onboarding new clients and when processing transactions through financial systems to ensure that they are detecting and preventing sanctions violations.

As recommended by The Wolfsberg Group, financial institutions should consider the following when reviewing their sanctions risks:

- Jurisdictions and proximity or relationship with sanctioned countries
- Location and business of international and domestic customers
- Volume of transactions and distribution channels
- Products and services offered and whether they represent a heightened sanctions risk

When using sanction/watch lists, not only look at those offered by OFAC but also relevant domestic lists. Lists provided by third-party providers, such as World-Check, can help to ease the burden when reviewing PEPs, aliases, names in non-Latin characters and more. Best practices include:

- Use an updated version of the list
- Use reliable sources
- Look at the geographic scope of the list
- Ability to handle common prefixes, secondary names, suffixes, non-Latin characters
- Ability to handle duplicate values

Finally, do not forget the dos and don'ts to avoid OFAC sanction violations including:

- Have a program and follow the framework
- Consult legal counsel
- Don't cause U.S. dollar payments to be remitted through the U.S. or by U.S. persons for transactions that in any way involve sanctioned persons or jurisdictions
- Do not in any way try to hide that a cross border U.S. dollar payment is related in some way to a sanctioned person or jurisdiction
- Make sure that your sanctions screening software and filters are adequate, continuously tested, and calibrated
- Don't slack on the quality of your due diligence. If you don't have the knowledge or resources to do it appropriately, outsource it until you do
- Don't be the person that comes up with a novel way to "get around" the sanctions

AML Compliance with Alessa

Alessa provides all the anti-money laundering (AML) capabilities that banks, money services businesses (MSBs), fintechs, casinos and other regulated industries need – all within one platform. Capabilities of the product include:

Customer Due Diligence: To support KYC, CDD, and EDD processes, Alessa combines data from onboarding, transaction monitoring, and other core systems with identity verification and risk intelligence data to provide updated risk profiles and scores that are based on activities and relationships.

Sanctions Screening: Alessa screens individuals and businesses against multiple lists including PEPs, negative news, OFAC, and other sanctions lists. Screening can be done in native characters and in real time, periodically or on demand.

Transaction Monitoring: Alessa can analyze every transaction in real time and, using an extensive library of analytics and scenarios, generate alerts for suspicious activities. These are sent to the appropriate personnel via text or email for investigation and/or reporting.

Regulatory Reporting: All suspicious activity alerts include data needed for regulatory reports. Once it is determined that a Suspicious Transaction Report or a Suspicious Activity Report needs to be filed, Alessa can auto-populate (and electronically file) as many as 70% of these reports. Alessa can also automate as much as 100% of CTRs.

Risk Scoring: Alessa uses data from various sources, including sanctions lists, to provide an assessment of the risks of doing business with an individual or business. The solution also periodically reviews an organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need to perform their responsibilities, and data can be maintained in the cloud or on-premises, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. The data is then cleansed and aggregated to increase its accuracy, and cross-referenced to reveal big-picture insights. Better data means better insights.

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision making.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow compliance staff to drill down into the alerts. Advanced analytics allow for sound decision-making and actions to be taken based on comprehensive information and insights.

To learn more about how Alessa can help with your AML compliance activities, visit *www.alessa.com*

About Alessa

Alessa, by Tier1 Financial Solutions, is a compliance, controls monitoring and fraud prevention solution for banking, insurance, fintech, gaming, manufacturing, retail and more. With deployments around the world, Alessa allows organizations to quickly detect suspicious transactions, identify high-risk customers and vendors and decrease fraud risks that reduces profitability and increases costs. To learn more about how Alessa can help your organization ensure compliance to regulations, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at https://www.alessa.com/.

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

alessa@tier1fin.com

www.alessa.com

alessa
by Tier1 Financial Solutions