Banco Santander
Bank of America
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
J.P. Morgan Chase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the
Wolfsberg
Group

Wolfsberg Guidance on Sanctions Screening

Introduction

Sanctions screening is a control employed within Financial Institutions (FIs) to detect, prevent and manage sanctions risk. Screening should be undertaken as part of an effective Financial Crime Compliance (FCC) programme, to assist with the identification of sanctioned individuals and organisations, as well as the illegal activity to which FIs may be exposed. It helps identify areas of potential sanctions concern and assists in making appropriately compliant risk decisions.

In light of the continuous expansion and growing complexity of international sanctions regulations, the objective of this paper is for the Wolfsberg Group[1] to provide guidance to FIs as they assess the effectiveness of their sanctions screening controls, whether automated, manual or both. The paper assumes that the reader has a basic understanding and familiarity with sanctions controls terminology, much of which is also covered in the Glossary.

Most FIs will deploy two main screening controls to achieve their objectives: transaction screening and customer screening.[2] Transaction screening is used to identify transactions involving targeted individuals or entities. Customer or Name screening is designed to identify targeted individuals or entities during on-boarding or the lifecycle of the customer relationship with the FI. Together, transaction and customer screening are designed to form a robust set of controls for identifying sanctions targets. It should be recognised that there are a number of limitations in the way in which these controls are managed and should always be employed as part of a wider FCC programme.

As with the management of all financial crime risks, an FI should first identify and assess the sanctions risks to which it is exposed and implement a sanctions screening programme commensurate with its nature, size and complexity. In doing so, consideration needs to be given to:

- The jurisdictions where the FI is located, and its proximity - geographically, culturally and historically - to sanctioned countries

[1] The Wolfsberg Group consists of the following financial institutions: Banco Santander, Bank of America, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, MUFG Bank, Société Générale, Standard Chartered Bank and UBS.

[2] For definitions, refer to Glossary, page 14

- What customers the FI has – international or domestic, where those customers are located and what business they undertake
- The volume of transactions and distribution channels
- What products and services the FI offers and whether those products represent a heightened sanctions risk, for example, cross-border transactions, foreign correspondent accounts, trade related products or payable-through accounts

This guidance sets out the use of sanctions screening as a control, the fundamentals of which are derived from legal and regulatory requirements and expectations, as well as global industry best practice. It is not intended to suggest all FIs should apply all elements in this guidance to the same level, rather, it attempts to demonstrate where sanctions screening can be an effective part of a wider sanctions compliance programme, where it has limitations as a control, and where a risk based approach is required,[3] notwithstanding the strict liability nature of sanctions compliance.

Consideration has been given to topics such as what is meant by sanctions screening, looking at both reference data and transaction screening, the timing of screening, technology and the use of automated systems, the criteria for alert investigation, as well as testing and quality assurance.

1. What is Sanctions Screening?

Sanctions screening is a control used in the detection, prevention and disruption of financial crime and, in particular, sanctions risk. It is the comparison of one string of text against another to detect similarities which would suggest a possible match. It compares data sourced from an FI's operations, such as customer and transactional records, against lists of names and other indicators of sanctioned parties or locations.

These lists are typically derived from regulatory sources and often supplied, updated and maintained through external vendors specialising in the amalgamation, enhancement, formatting and delivery of these lists. FIs may also augment these with lists of sanctions relevant terms, names or phrases, identified through their own operations, research or intelligence.

The generation of an alert as a result of the process of screening is not, by itself, an indication of sanctions risk. It is the first step towards detecting a risk of sanctions exposure, which can be confirmed or discounted with additional information to evaluate whether the similarities in the text reveal a true sanctions match.

While this concept sounds simple, it can be complex when it comes to determining what actually constitutes a "true match" across a range of variables such as alphabets, languages, cultures, spelling, abbreviations, acronyms and aliases. When screening is automated, additional complexities are introduced such as "fuzzy matching" algorithms, workflows and match rules.

2. A Programmatic Approach to Sanctions Screening

While this guidance focuses on screening as a control to manage sanctions compliance risk, screening as a control is not sanctions specific and should be deployed as part of an integrated risk based FCC programme.

[3] *Wolfsberg Guidance on a Risk Based Approach for Managing Money Laundering Risks* (2006), https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf

2.1 Sanctions Screening Programme

Fundamental pillars of an FCC programme, including key enabling functions, should be applied to screening, not in isolation, but in conjunction with other financial crime risk prevention and control processes:

- Policies and Procedures - defining requirements for what must be screened, in what context and at which frequency, and how alerts should be adjudicated, paying particular attention on how to resolve alerts where information is unavailable, incomplete or potentially unreliable.

- Responsible Person - ensuring appropriate skills and experience in understanding the nuances of often arcane sanctions requirements and how these might influence screening outcomes and decisions, as well as the technical capabilities of screening software.

- Risk Assessment - applying risk based decisions to resolve specific questions of what data attributes to screen, when to screen, what lists to use and how exact or "fuzzy" to set the screening filter. The decision making and governance structure needs to be clearly articulated, documented and supported by analysis and testing. This is addressed in more detail in Section 2.2 below.

- Internal Controls - implementing screening control processes requires an understanding of the various methodologies and technologies available and their operational consequences. There is no clearly defined approach to technology or configuration that is better or worse, and each will have its own strengths and limitations. Understanding those strengths and limitations is critical. FIs are expected to document how their screening systems are configured in order to demonstrate that the configuration is reasonably expected to detect and manage the specific sanctions risks to which the FI is exposed and, importantly, to ensure transparency of any system limitations or risk based decisions which the screening controls are not designed to detect.

- Testing - conducted to validate that the screening system is performing as expected and to assess its effectiveness in managing the specific risks articulated in the FI's Risk Assessment. Regular testing of the system should be supported by metrics, analysis and reporting.

2.2 Applying a Risk Based Approach

Sanctions screening can never detect every possible sanctions risk due to the wide range of variables in which a string of text could be altered and still convey the same meaning. Sanctions screening is dependent on a range of factors, including the type, availability, completeness and quality of data, as well as the inherent sanctions risks to which an FI, its products, customers and services are exposed.

Consequently, the effectiveness of screening as a control will vary between FIs, even where FIs are using the same third-party screening solution, and screening is not necessarily appropriate for all products and services. Screening, therefore, requires a programmatic approach through which each FI must assess its own risks in order to define the manner, extent and circumstances in which screening is employed. This process of evaluating the risk to the design, configuration and maintenance of a screening programme is built around the following core principles:

- Articulate the specific sanctions risk the FI is trying to prevent or detect within its products, services and operations. For example, a global FI may determine that its policy is to prohibit any dealing with any party sanctioned by the U.S., the U.N., the E.U., its home country and any number of its core jurisdictions of operations. A smaller FI operating only in one country, however, may determine that its policy is limited to complying with the sanctions laws of the sole jurisdiction in which it operates.
- Identify and evaluate the inherent potential exposure to sanctions risk presented by the FI's products, services and customer relationships. For example, screening may be more meaningful to mitigate sanctions risk in the context of cross-border payments between a potentially wide range of parties, as opposed to payments between parties within the same jurisdiction, where all account holders are required by law to be compliant with that jurisdiction's sanctions and KYC requirements. In the latter, the KYC, on-boarding processes and regulatory requirements are known and consistent, lessening the incremental value of transaction screening as a control.
- A well-documented understanding of the risks and how they are managed through the set-up and calibration of the screening tool. For example, with list based sanctions programmes, the red flag is the presence of the sanctioned party's name, which is readily available to detection through screening of customers and transactions. By contrast, for certain Sectoral Sanctions programmes,[4] only a defined subset of activities is prohibited, and screening payments for targeted parties will not detect the sectoral sanctions risk without further additional information about the specific underlying activity and, therefore, may not be appropriate or effective.[5]
- Assess where, within the FI, the information is available in a format conducive to screening. For example, transactions solely containing International Securities Identification Number (ISINs). In some cases, an FI may identify that the information within its operations is insufficient to assess a screening alert and distinguish a true match from a false match. In these cases, the FI may need to consider alternative controls or adopt new business processes. In other cases, the FI may decide not to screen a category of information because this specific information, while in a format conducive to screening, is not sufficiently actionable to manage sanctions risk. In these situations, the FI should implement alternative controls to identify and manage the sanctions risk.

3. Screening Technology and Generating Productive Alerts

What is often thought of as a simple name-matching process can be a complex set of processes in which data is transferred from several, often disparate, technology systems and sanctions lists for comparison, using matching algorithms and risk based alert creation rules intended to ensure compliance with multiple regulatory regimes.

For larger or more complex FIs, there is an expectation that the screening programme will require the use of a technology application that includes certain core functionalities to ensure appropriate alert creation by, and governance over, the screening process. Such functionalities include the capability to implement risk based screening rules, generate good quality alerts for review, provide relevant metrics and reporting, ensure data integrity and facilitate independent testing and validation. A robust

[4] For definition, refer to Glossary, page 14

[5] For further information on Sectoral Sanctions see OFAC FAQs, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#ukraine

operating model employs expertise from IT, Operations and FCC working together to ensure appropriate alert generation and adjudication.

3.1 Principles for Generating Productive Alerts

Identifying and implementing risk based screening decisions, in order to maximise alert quality and minimise the number of low quality or irrelevant alerts, should be undertaken prior to the deployment of a new screening system and thereafter on an on-going basis. Risk based decisions may include:

- Lists - an FI may establish criteria and technology processes to ensure that lists are only screened against a subset of data relevant to a specific jurisdiction (see section 6, List Management)
- Exclusions – the addition of a party that poses low sanctions risk to a list of parties omitted from screening; or the use of conditional screening rules using list data or source data attributes
- Suppression - use of suppression rules or "Good Guys" lists to manage common false positive alerts requiring unnecessary manual review
- Data - removal of reference data from screening once the data is no longer risk relevant

A governance framework should contain the documented rationale for risk based decisions, such as those made in support of the creation of screening rules and threshold settings, as well as the risk acceptance or remediation efforts in relation to material deficiencies or changes.

3.2 Alert Generation and Review

The core aspect of any screening application is alert generation. The screening application must clearly present an alert for review by trained sanctions personnel. While the application's workflow may vary according to many factors, including reviewer expertise or an FI's risk tolerances (for example, whether the review process involves a maker-checker/four-eye requirement[6]), the application must present all relevant data from the FI and the sanctions lists for decision making and allow reviewers to make a decision based on the validity of that data and, thereafter, record relevant rationale.

3.3 Metrics and Reporting

Personnel with responsibility for governance and oversight of the screening application and processes should receive risk-relevant metric reporting that enables the identification of sanctions and operational risk, as well as any data integrity issues. Such metrics may include, for example, the number of alerts generated by list, by jurisdiction, by business, or the identification of unintended data and list omissions.

This reporting and documentation should be used to disseminate relevant information to stakeholders.

3.4 Independent Testing /Validation

FIs should deploy an independent risk based testing regime to ensure that the screening application generates expected alerts, threshold settings and/or screening rules to forego or suppress undesirable

[6] For definition, refer to Glossary, page 14

alerts in accordance with the FI's risk appetite. Similarly, the accuracy and completeness of the data used in the screening process should be reviewed to ensure the integrity of data uploaded.

Independent testing may be carried out by qualified teams with appropriate technology expertise in internal audit, an independent group within the FI's compliance division, a third-party vendor engaged for this purpose or a combination of these. The screening application may also be submitted for consideration as a model and, if so considered, any associated governance framework.

The results of testing should be reviewed at a minimum by the team within the FI with primary responsibility for sanctions compliance, which should determine whether risk acceptance or remediation is appropriate with respect to any relevant findings.

3.5 Data Integrity

The aggregation of data from multiple sources for sanctions screening creates the possibility that data integrity issues may arise. An FI should consider establishing processes to ensure source and list data used in the screening process is both accurate and complete.

3.6 Internal Technology Build or Vendor Selection

Successful implementation of a sanctions screening application requires an FI either to build the screening application internally or to source it from a vendor. As each FI's size, geographic presence, business and technology environment are unique, this determination must be derived from an analysis of identified sanctions risks and functional requirements.

Elements to be considered from a risk standpoint include:

- The sophistication and configurability of the matching software
- Availability of screening rules to optimise alert creation/suppression
- Support for the screening or transformation of data in non-Latin characters
- Ad hoc, one-off or manual screening functionality
- Workflow configurability
- Availability of metrics reporting

From a functional standpoint, consideration should be given to the volume of data to be screened; support for multiple local or a single centralised installation; the existence of, or support for, data integrity processes, and the ability of the application to integrate effectively within an FI's technology infrastructure.

Once risk and functional requirements have been identified, an FI should achieve a balance between the standard vendor functionality and configurability of a purchased solution against the cost to build and maintain a more bespoke application internally. It is critical to understand whether sufficient compliance and technology expertise and resources exist within the FI or chosen vendor (and will continue to exist) to sustain the design, build and/or implementation processes, while remaining well-informed on emerging sanctions risks that arise as a result of evolving regulatory frameworks or business expansion and strategy.

4. Reference Data/Customer or Name Screening

4.1 What is Reference Data Screening?

Reference data screening is the process of screening the information an FI collects and maintains on the parties it does business with, or specific types of products and services it offers. While it is often referred to as "name" or "customer" screening, the concept of reference data screening encompasses any data set within the FI's operations, separate from its transactional records, that may present a relevant sanctions risk indicator and be conducive to detection through screening on a periodic basis.

The most common types of reference data relevant for sanctions screening include:

- Customers, including all parties, whose identity is collected by an FI to meet its Know Your Customer (KYC) and Customer Due Diligence (CDD) standards, such as beneficial owners and related or connected parties
- Employee data
- Third-party service providers, for example, vendors, landlords of FI-occupied premises, tenants of FI-owned premises
- International Securities Identification Numbers ("ISIN") or other sanctions-relevant identifying features of assets held in custody by the FI
- Recipients of the FI's corporate donations or sponsorship

4.2 Determining Sanctions Relevant Attributes in Reference Data

Not all the data elements within an FI's records are relevant for sanctions screening. When determining what reference data should be screened, an FI should identify and differentiate the data within its operations and records that are relevant to sanctions risks, how they are relevant, and ensure they are conducive to effective screening. For example, the names of individuals and entities with whom the FI has a relationship are relevant for screening against name based sanctions lists; however, they are not relevant for geographically based sanctions programmes.

While the data elements contained in the addresses for these parties (most commonly, cities and countries) are relevant for screening against geographic sanctions programmes, these same address attributes are also relevant as identifiers in name based, list based programmes to differentiate a true name match from a false name match.

An FI should also define other data elements that may be relevant for sanctions screening in some situations and not others. Date of birth, for example, is relevant as a distinguishing factor to assess a true match from a false match on an individual and might be used for screening in combination with another attribute, such as name. In each case, FIs should weigh up the relative incremental value of screening the data element against the reliability of the data, and whether an alert against the data will meaningfully assist in detecting or preventing a sanctions risk that would not be reasonably detected through other controls, or by screening different data attributes.

4.3 Manner, Timing and Frequency of Sanctions Screening

An FI's reference data is typically maintained in electronic files. It is most effective when screened through an automated process and repeated at defined intervals. The use of manual screening can be considered when the risk is sufficiently low, and where the reference data cannot be sourced reliably, either electronically or in a format necessary for automated screening. For example, if an FI has identified only a small population of names requiring screening, it may choose to forego investing in an automated screening system and instead manually input these names into an online screening filter.

An FI's policies and procedures should clearly define when reference data screening takes place. As a general principle, screening should be done when establishing a new relationship, to ensure the relationship is permissible, and then at regular intervals, either upon a trigger event or as customer and/or list information changes, to validate that the relationships remain permissible. Where either internal or external data sets change frequently, periodic screening may be as often as daily, but longer intervals between periodic rescreening may be acceptable in situations where change is less frequent or the risk of a potential sanctions exposure is low.

5. Transactions/Message Screening

Transaction screening refers to the process of screening a movement of value within the FI's records, including funds, goods or assets, between parties or accounts.

5.1 Transaction Screening, including Payments and Trade

In order to determine the scope of transaction screening relevant for sanctions risk management, an FI should focus on those transactional records necessary to the movement of value between parties and at a point in the transaction where detection of a sanctions risk is actionable to prevent a violation. Consideration should be given to higher sanctions risks factors, such as:

- Cross-border transactions
- The currency used as part of the transaction
- The routing of the transaction

Screening cross-border payments prior to completing the transaction is common practice and known as screening in real-time. By contrast, screening domestic payments in real-time may be unnecessary for FIs that are subject to the same local regulatory requirements, including the jurisdictions' local sanctions and KYC requirements when on-boarding clients. For these FIs, imposing screening at the time of each transaction is likely to be duplicative and less likely to identify any new or additional risk indicators. However, an FI that is also subject to a different jurisdiction and regulatory mandate would likely want to assess its applicable requirements and decide to screen its transactions to address that specific risk. An FI also may decide to screen a defined set of transactions, where it assesses the sanctions risks within the local economy or financial system to be outside of its own risk tolerance.

5.2 Data Elements within Transactions

An FI should initially assess which transaction types are relevant for sanctions screening. In the same way as reference data, it should then identify which attributes within those records are relevant for sanctions screening and the context in which they become relevant. Names of parties involved in the transaction are relevant for list based sanctions programmes, whereas addresses are more relevant to screening against geographical sanctions programmes and can be used as identifying information to help distinguish a true match from a false match. Other data elements, such as bank identification codes, may be relevant for both list and geographically based sanctions programmes.

In a sanctions context, some data elements are more relevant when found in combination with other attributes or references. For example, detection of sectoral sanctions risk typically requires detection of multiple factors, such as those where both the targeted parties and the prohibited activities are involved. Many controls may not be capable of detecting both factors simultaneously and, therefore, may not be effective.

In addition, certain data elements offer little or no risk mitigation through screening, for example, amounts, dates and transaction reference numbers have no relevance from a screening perspective.

Some of the most common transactional attributes screened include:

- The parties involved in a transaction, including the remitter and beneficiary[7]
- Agents, intermediaries and FIs
- Vessels, including International Maritime Organisation (IMO) numbers, normally in Trade Finance related transactions
- Bank Names, Bank Identifier Code (BIC) and other routing codes
- Free text fields, such as payment reference information or the stated purpose of the payment in Field 70 of a SWIFT message
- International Securities Identification Number (ISINs) or other risk relevant product identifiers, including those that relate to Sectoral Sanctions Identifications[8] within securities related transactions
- Trade finance documentation, including the:
  - Importer and exporter, manufacturer, drawee, drawer, notify party, signatories
  - Shipping companies, freight forwarders
  - Facilitators, such as insurance companies, agents and brokers
  - FIs, including Issuing / Advising / Confirming / Negotiating / Claiming / Collecting / Reimbursing / Guarantor Banks
- Geography, including a multitude of addresses, countries, cities, towns, regions, ports, airports, such as:
  - Within SWIFT Fields 50 and 59
  - Place of taking in Charge / Place of Receipt / Place of Dispatch / Place of Delivery / Place of Final Destination
  - Country of origin of the goods /services / country of destination / country of transhipment
  - Airport of Departure / Destination

5.3 Manner, Timing and Frequency

Transaction screening should be performed at a point in time where a transaction can be stopped and before a potential violation occurs. This typically occurs at a number of points in the lifecycle of a transaction, but certainly prior to executing any commitment to move funds. Particular attention should be directed to any points within the transactional process where relevant information could be changed, modified or removed in order to undermine screening controls.

[7] For more information on parties to transactions in international payments, see *Wolfsberg Group Payment Transparency Standard* (2017), https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf

[8] For definition, refer to Glossary, page 14

Transactional records are typically found in large volumes and within business processes predicated on speed of execution. These transaction types are generally in electronic form and conducive to systemic, automated screening. Some transaction types, however, still rely on documentation in various formats and varying methods of presentation. These may require manual screening processes, where relevant information is physically added into a system for screening.

Trade finance documents often require this type of manual screening, although, more advanced information capture techniques are increasingly available, including Optical Character Recognition (OCR), where documents are scanned and then automatically transposed into a system prior to screening. OCR requires quality assurance validation to ensure the information has been captured fully and accurately.

Certain paper based transactions, such as paper cheque clearing, where the volumes can be high and the manual screening process creates high rates of errors, may rely on controls other than screening, such as KYC processes, where the sanctions risks for the product are assessed as being low.

6. List Management

Screening is dependent on data sets and lists of sanctions indicators, against which an FI looks for potential matches within its reference and transactional data. These lists must be accurate, reliable, up-to-date, refreshed frequently and relevant to the risks the FI is attempting to manage. These lists are generated both by external authorities and created internally based on the FI's own information and knowledge about its exposure to sanctions risks.

List management refers to the end-to-end process of determining and managing regulatory and internal lists used for screening. Rigorous list management promotes screening which is consistent with the FI's risk appetite, including the identification of potential sanctioned targets.

The following considerations are relevant to effective list management, and each should be well-documented and reviewed on a regular basis, to ensure the FI's chosen approach remains in line with its risk appetite:

- List selection - determine which sanctions related lists are relevant for screening. This should include regulatory lists, for example, the OFAC and E.U. lists, as well as other lists designed to comply with regulatory requirements and to manage risk. Such lists may include internal or private lists of individuals/entities/terms known to have a sanctions nexus, lists of geographic terms including cities, towns, regions and ports or banking terms (for example, BICs), lists of prohibited securities and prohibited goods, where applicable.
    - List selection may depend upon multiple variables, including the type of data being screened or whether transactions are domestic or cross-border. For example, screening against lists of prohibited goods is currently unlikely to be conducted outside the context of trade finance transactions, or trade finance transactions likely do not need to be screened against sanctioned securities.
    - FIs should consider the impact that the introduction of new lists and terms, which could generate significant alert volumes, or spikes,[9] may have on operational risk.

[9] For definition, refer to Glossary, page 14

- Sourcing of lists - determine which lists are to be generated internally and which lists are best sourced from external vendors, and the processes for generating/ingesting such lists.
- List maintenance - determine the processes for adding and removing lists or entries to internal lists, where screening is no longer required or where the result is within risk appetite. Determine appropriate controls to ensure lists remain up-to-date and that only appropriate individuals can add or remove lists or list entries.
- Data enhancement - determine whether certain list entries should be modified or enhanced based on additional information.
- Whitelisting - determine the management of rules for automatically eliminating potential hits caused by the interaction of certain list terms and frequently encountered data, for example, customer names which have already been confirmed as false positives.
- Geographic scope of list application - determine which lists should be screened in all jurisdictions of an FI's operations and which, if any, could be screened only locally, within a certain jurisdiction or jurisdictions.
- "Exact matching" versus "fuzzy logic" - determine which lists should be deployed within the screening filter on an exact match basis, and which would use fuzzy matching.
- Frequency of screening - determine the frequency or the triggers for static data screening. For example, additions to lists and changes in customer data.

6.1 Regulatory Sanctions Lists

FIs typically source regulatory lists either from a third-party provider or directly from regulators. The use of a third-party can offer the FI a broad enrichment of data in a standard format and avoids duplicate entries that appear on multiple lists.

FIs should consider the means to ensure the quality and timeliness of updates made to the lists they screen against, including the following factors:

- Delays between regulatory sanctions list updates and vendor provided screening list updates
- Enrichment of listed terms; for example, foreign language name variations or addition of BIC codes for listed FIs

When new designations are published on regulatory lists, the key priority for a list management function is to ensure the names are implemented into screening as quickly and accurately as possible.

6.2 Internal Lists

Internal lists are often referred to as 'Private lists' or 'Grey lists.' These are lists of individuals and entities which may present a financial crime risk to the FI, and have been identified through an FI's internal procedures or intelligence. These names are generated and maintained internally within an FI's risk appetite and, ideally, applied in screening for a set time frame, dependent on the risk.

Long term effectiveness of internal lists often depends on the data quality of entries added. Toward that end, an FI should consider the minimum inclusion criteria for internal list entries to be operationally effective, including minimum data attributes and quality, to complement alert investigation procedures and improve risk identification. Regular reviews of entries are helpful to ensure intelligence does not become stale or outdated.

6.3 Identifying Information and Weak Aliases

Along with entries on a list, certain identifying information is often provided to assist in distinguishing a true match from a false positive. This information does not need to be screened. It is provided to assist with the assessment of an alert. This includes attributes such as date of birth, nationality (where legally permissible) and place of birth.

In addition to identifying information, some authorities provide additional ancillary information of varying utility that can be useful to help distinguish a true match from a false positive. This ancillary information may include "weak aliases," or "low quality aliases," and describes broad or generic names of sanctions targets that often will add little value in confirming a match. These weak aliases may include 'nicknames' and common acronyms. It is not expected, nor is it typically productive, to screen against weak aliases.

Weak aliases can be identified into one of the categories below:

- Character length (shorter strings are assumed to be less effective in screening than longer strings)
- The presence of numbers in an alias (digits 0-9)
- The presence of common words that are generally considered to constitute a nickname (example: Ahmed the Tall)
- References to geographic locations in the alias
- The presence of very common prefixes in a name where the prefix was one of only two strings in a name (example: Mr. Smith)

7 Historical Reviews (Lookbacks)

While the consideration of a lookback is not exclusively a sanctions control, an FI may identify potential sanctions risk where a sanctions related data point may have been previously undetected by the screening system, for example, as a result of a name variation. In these instances, the FI should consider whether or not: (i) changes to the sanctions screening system (for example, configuration or lists) are warranted, and (ii) a historical review ("lookback") should be performed. In considering a lookback to identify transactions that have already been processed, an FI should give strong consideration as to whether such a review would be useful to the FI and/or public policy interests.

In making this determination, consideration should be given to:

- A clear understanding of what is the root cause
- Whether the matter is an isolated, one-time event or is it likely to occur again, in order to inform the necessary activity and the consequences if it is repeated
- Does the risk warrant mitigation? If yes, what steps need to be taken to mitigate the risk? For example, configuration changes, list content, non-screening controls
- Is there a public policy or law enforcement interest in the identification of historical transactions and subsequent disclosure of those transactions/parties involved?
- Mitigating factors for potential enforcement actions and regulatory disclosure

- Detecting possible conduct issues
- Identifying customer behaviour or patterns that pose increased sanctions risk

8. Conclusion

In summary, sanctions screening is a key control in the prevention of financial crime risk which FIs may otherwise be exposed to. It is essential that it is implemented and maintained as part of a wider set of financial crime compliance controls and within the risk appetite of the FI.

While recognising the need to meet regulatory and legal obligations, and demanding the highest standards of effectiveness in identifying sanctioned parties and locations, the Wolfsberg Group believes FIs should seek to adopt a risk based approach to sanctions screening and to consider all aspects of a comprehensive sanctions screening control framework, as follows:

- The FI must have a robust FCC programme with a clear strategy in respect of sanctions screening, to mitigate the risk of being exposed to sanctioned parties and countries.
- The FI's approach should recognise that while sanctions screening is a primary control, it has its limitations and should be deployed alongside a broader set of non-screening controls to be truly effective.
- It is important for FIs to document their systematic approach to screening by linking it directly to their risk appetite statements.
- The accuracy and completeness of the FI's own data is central to an effective and efficient sanctions screening process.
- Technology remains a key enabler in the effectiveness of identifying financial crime risk through screening, more efficiently and on a real-time basis.
- Robust governance and oversight mechanisms must be put in place across the FIs to ensure transparency of risk decisions to key stakeholders and risk owners.
- The FI should ensure that people involved in the end-to-end risk event management are suitably trained, supervised and that the appropriate levels of quality control and assurance are in place to ensure compliance with requirements.
- Robust management information should be made available to management to report effectiveness, trends and performance.

Glossary

Alert Spike is a substantial increase in the number of alerts generated. A spike could be caused by, for example, remediation exercises, changes or updates to policies, procedures or Watchlists.

Four-Eye Review means that a certain activity, for example, a decision/transaction must be approved by at least two people (**Maker** and **Checker**). This dual control mechanism is used to increase transparency and ensure quality of reviews and subsequent decisions.

Fuzzy Matching is a varied and algorithm based technique to match one name (a string of words), where the contents of the information being screened is not identical, but its spelling, pattern or sound is a close match to the contents contained on a list used for screening.

Customer or Name Screening is the screening of full legal name and any other name provided by the customer, such as known aliases, against applicable official sanctions lists.

Operational Risk is the risk of potential reduction, deterioration or breakdown of services provided by an FI caused by deficiencies in information systems or internal processes, human errors, management failures or disruptions from external events.

Sectoral Sanctions – in July 2014, the U.S. Office of Foreign Assets Control (OFAC) and the European Union introduced new Ukraine and Russia-related sanctions programmes prohibiting certain types of transactions with targeted entities in the finance, energy and defence sectors, as well as entities owned by 50% or more by the targets. OFAC refers to these sanctions as Sectoral Sanctions Identifications.

Sectoral Sanctions Identifications aim to identify persons operating in sectors of the economy that may be subject to sectoral sanctions, deals and transactions that are prohibited.

Transaction Screening is the process of screening a movement of value within the FI's records, including funds, goods or assets, between parties or accounts. In order to mitigate risk associated with trade finance transactions and international wire transfers, FIs conduct real-time screening of cross-border transactions against Sanctions Lists, where any of the Sending Bank, Originating Bank, Receiving Bank, Intermediary Bank or Beneficiary Bank are located in different countries.

True Match is a screening result, where the characters contained within the information being screened match the details of a designated entity on a list that is in scope for screening.

Weak Aliases/Low Quality Aliases is a term for a relatively broad or generic alias (including 'nicknames' and common acronyms) that may generate a large volume of false hits when such names are run through a computer-based screening system. It is not expected, nor is it typically productive, to screen against weak aliases.