Sanctions Screening tools - An AFEP Guide
October 2015

Sanctions screening tools are an essential part of any compliance programme acting as the company's last line of defence against transactions with sanctioned individuals, entities or vessels.

Many tools exist which offer to screen a firm's data and transactions, but the underlying system used to screen the data is often considered to be a Black Box, with vendors not wishing to disclose the details of how their systems operate. This lack of clarity about how data will be screened can cause issues for firms during audits or regulatory visits, particularly if firms are unable to understand the process used by their screening systems. Gaps and deficiencies highlighted by auditors in sanctions systems can be embarrassing for a firm, if they had not compensated for or mitigated any relevant risks.

This guide aims to act as an introduction to the different styles of sanction screening tools and to help prepare AFEP members when dealing with sanctions screening providers. This document cannot prescribe the exact requirements for a firm to screen for sanctions breaches, as this will be entirely dependant upon the firm's risk profile and the products and services which it offers however it will act as a basic introduction to some of the common issues and basic differences between sanctions screening tools

Lists Provided or Self uploading:

The first element to consider is whether the sanctions lists are provided and updated by the vendor, or if data needs to be provided and updated by the firm.

Vendors sometimes offer a screening only service as it removes some of the liability on updating lists, or where they are unable to provide relevant data (for example the vendor may not publish its own PEP list) Vendors may also offer partial lists, for example may cover OFAC and HMT, but may not include HKMA list.

Vendors which do not provide lists may be cheaper, but the firm will be responsible for obtaining updated lists and uploading them into the system. Where sanctions lists are formatted in different ways, firms may have to adjust the format of such lists to make them fit the vendor's system. Firms will need to monitor Sanctions lists and update these as soon as the sanctions list is updated.

Where the vendor provides the lists to the firm, firms should question the speed and timing of updates. Firms should be cautious of vendors who update only weekly, or update only when a single list (Such as the US list) is updated. Firms may find that updates are done

centrally, for example only during US office and working hours and should consider if this delay in update poses a risk. It is good practice to test the vendor's lists for accuracy after each HMT notification.

In House or externally hosted:

Some vendors allow firms to choose between hosting the vendor's software on their own systems, or sending their data to the vendor for screening externally.

Locally hosted software means the firm will need to have a server or similar on which to host the software. The vendor is likely to provide details of minimum specifications of hardware. The Firm is responsible for the maintenance, repair and support of this hardware providing backup in the event that it fails and also updating the software if the vendor makes changes. Locally hosted systems can be used for batch processing at weekends, or during downtimes when they are not in use by the firm.

Externally hosted systems tend to have a cheaper up front cost (less hardware) but may take longer for a response to be received from the vendor to each query. Firms should very carefully review the up times provided by the vendor, remembering that a 99% uptime means that for 3.5 days of the year the system will be unavailable. Firms should also consider whether they are revealing personal data to the vendor and where this data will be sent if the vendor is located outside of the UK.

Automated or manual:

Some vendors offer the ability to do line by line checking of data, which allow firms to screen individual pieces of data that is copied into the system. Such systems are often unable to handle high volume or transaction flow data, or the passing of data from databases, or require a human to input data.

Firms should consider how much time is needed to manually screen individual transactions and also whether they intend to re-screen the standing data in the future. Manual screening systems often have no capacity to review previously screened data, so where there is a change to a sanctions list, existing client data will not be reviewed. Firms with high volumes of transactions will also need to consider if they will be able to screen transaction data fast enough to keep up with the flow of transactions.

Firms utilising automated systems should ensure that transactions are not released until after they have been cleared by the sanctions system. Systems which do not instigate a stop which awaits a response from the screening system or similar may allow transactions to be released to the banking network too early. Firms should also consider how they intend to

maintain an audit trail of who released the transactions if being processed from a queue. Individual staff members working a queue should all have their own logins, rather than a company wide account.

Fuzzy Matching:

The JLMSG Provides some guidance around the use of Fuzzy Matching,

"Fuzzy matching" describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data - whether in official lists or in firms' internal records - is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process"[1]

But provides limited information as to how such a system should work or how accurate such a system should be.

In order to ensure that a firm has a defensible position they should know the advantages of the system they choose as well as the disadvantages and limitations.

Firms should understand what sort of system the vendor uses, such as Jaro-Wrinkler / Levenshtein [2] distance system, phonetic matching system or whether they have a list based system. Other elements such as substitution lists, concatenation and containment will also increase the hit rate of systems, but also potentially increase the number of false positives. Different systems may also be limited in their application, for example may only work with western names, or may not work with translated names.

Firms should carefully document how they chose a fuzzy matching level, what options they used in order to reduce hits (such as utilising location of individuals or dates of births to reduce matches) and what methods were used to test results. Firms should be careful not to turn down fuzzy matching purely to reduce workload and should ensure that they can demonstrate rigorous testing of the system output before making adjustments.

What Data to Screen:

Early setup of sanctions screening tools is essential. Ensuring that the functionality of the tool, the sensitivity of screening and the frequency of screening is important, but firms must also consider what data they intend to screen.

---

[1] JMLSG Guidance - Compliance with the Sanction Regime
[2] See Jargon Buster at the end

Association of Foreign Exchange
and Payment Companies

The number of fields, for example including any comments or reference fields in your payments will increase the volume of hits, but will also increase the likelihood of capturing forwarding information (where a payment is coded for onward payment by the recipient bank). Firms should consider what information is being sent to their partner bank and how relevant this information is. Screening details of your account reference numbers for example is unlikely to produce any active hits.

Some vendors may be able to have certain data screened against certain fields. For example vessel or PEP information may be excluded from address information fields, or bank fields. Firms should consider the possibility for cross-field contamination. For example data, which is too long for a SWIFT MT103 field, may automatically bleed over into the next field, depending on how the payments gateway is setup.

For example Janice Keihanaikukauakahihuliheekahaunaele (a real name) may appear in a swift message as:

Janice Keihanaikukauakahihuli | heekahaunaele City Point, 1 Ropemaker Street,

With the second part of the surname breaching the address field.

Errors in data input by staff may also result in data being in the wrong fields and so over reliance on field formatting may lead to errors. Firms should consider testing their data to ensure it is correctly formatted before they rely on such systems.

Testing:

Firms should apply rigorous testing of their sanctions screening systems on a periodic basis to ensure that the system is working inside of the parameters the firm has defined.

Fortunately for firms the data required to test Sanctions tools is readily available as the sanctions lists are published openly. One method of testing a firm's systems is to take the name from the list and produce a series of variations on the name which are presented to the system in the hope that it will identify all of the variants. For example ADAM KHAN ACHEKZAI May be tested as:

ADAM KHAN ACHEKZAI   (Original)
A K ACHEKZAI   (Initials)
ADAM ACHEKZAI KHAN   (Names re-ordered)
ADAMKHAN ACHEKZAI   (Concatenated)
ADAM ACHEKZAI   (One Name Removed)

ADAM KHAN ACHEKZI   (Single character removed from name)
ADAM KHAAN ACHEKZI   (Single Character added to a name)
ADAM KHAN ACHEKZ   (Two characters removed from name)
ADAAM KHAAN ACHEKZ   (Two characters added to a name)
ADAM KAHN ACHEKZAI   (Mixing characters on middle name)
ADAM CARN ACHEKZAI   (Sounds like KAHN, Phonetic match)

Records of this testing and the results should be made to prove that it has taken place. Firms may also consider a similar test based on multiple names, including sets of Western, Hispanic, Arabic and Eastern names etc. Firms may find that certain names, such as shorter Eastern names (Fu, Jui, Jung etc) will produce more false positives than longer western names, but this will vary depending upon the settings used by the firm.

The results of this test will of course vary depending upon the setup of the system. It is important to document the setup, so that future testing can take place against the original setup.

For firms who purchase a service with the list auto populated, tests should be carried out on the timing of updates from their vendor. HMT and OFAC provide email updates when updates are made to the sanctions lists. A list of amendments and additions is also provided. Firms should sign consider signing up to these services and when informed of an amendment to the list, conduct a search for new added names. First should choose a reasonable time frame in which they believe updates should take place, and revert to their vendor if updates do not appear promptly.

Jargon Buster:

Black Box - Device, or system, whose inputs and outputs are known, but whose internal structure or working is not supposed to be known because of its confidential nature.

Concatenation - Is the process of joining two strings or words together or removing spaces from sentences. For example John Smith would become JohnSmith.

Containment - Matches when one record's component is contained in another record. For example, "Smith" is contained in "Smithfield.

HKMA - Hong Kong Monetary Authority, the HM based regulator, also responsible for the production, maintenance and enforcement of sanctions screening systems in relation to Hong Kong.

HMT - Her Majesty's Treasury - The UK Government department responsible for producing, maintaining and enforcing a UK list of sanctioned entities.

List Based System - Used to speed up certain search systems, the creator of the list will generate all know misspellings, abbreviations and variants of the name entered, for example the firm may make a list of names, for example: Carly may be - Carlee, Carleigh, Carley, Carlie, Karlee, Karlie. Such systems then search utilising the list, as opposed to calculating phonetic or fuzzy lists on the fly. This poses a risk if the lists are incomplete or not updated frequently.

Jaro-Wrinkler and Levenshtein distances - counts the number of edits (insertions, deletions, or substitutions) needed to convert one string to the other. For example a name may be a single character different from a name on the watch list, for example John versus Joan. This would be a very short hop, versus John and Charlie.

OFAC: The Office Of Foreign Assets Control. The US government department responsible for the development and maintenance of sanctions watch lists in the USA.

Phonetic Matching: Sometimes called Soundex, Metaphone or Double Metaphone matching. These work on a basis algorithm that convert a word into a phonetic representation, assigning each letter a score. Letters which sound alike, N and M for example, are given similar scores. The system then identifies words or sections of words with similar scores. Metaphone scoring is based more closely to the pronunciation of a full name, but only work accurately with western pronunciation of names.

Substitution lists - Substitution lists will automatically search for known misspellings of names, for example Michael is often spelt Micheal. When the misspelling is entered, the system will search for both spellings of the name. This ensures that firms do not miss potential hits as a result of typos by the firm's staff.

SDN - Specially Designated Nationals - The collective term for any individual, company, vessel or entity which is listed on the US OFAC list.

Standing Data - Data which does not typically change, for example the name, address and date of birth of a customer is considered standing data. Transactional information, which may vary for each transaction a customer sends, is not.

Providers:

Below are a list of known providers, provided by AFEP members and associates. AFEP does not endorse these firms, their products or services and does not provide assurances that the systems or products listed will be suitable for member firms. Firms should conduct their own due diligence of products prior to choosing a suitable service.

Accuity Solutions:
http://www.accuity.com/compliance/
0207 653 3800
Sales@Accuity.com
1 Quality Court,
Chancery Lane,
London
WC2A 1HR

CSI - WatchDog:
http://www.csiweb.com/solutions/regulatory-compliance/watch-list-screening
No UK Address or contacts, predominantly US based.
3901 Technology Drive,
 Paducah,
KY 42001
Phone: (800) 545-4274

Detica Netreveal - Part of BAE systems:
learn@baesystems.com

01483 816000

Eastnets:
http://www.eastnets.com/
1st Floor
9 Devonshire Square
EC2M 4YF
London, UK
0203 586 1283
info@eastnets.com

Fircosoft - Part of the Acuity group:
http://www.fircosoft.com/home/
+44 (0)20 7780 6710

St Olaves House,
10 Lloyds Avenue
London
EC3N 3AJ

FIS GLobal - Metavante:
https://watchlistiq.com/
FCS.SUPPORT@fisglobal.com

FISERV-
https://www.fiserv.com/international/index.aspx
0845 013 1200
1 King's Arms Yard
London

Innovative systems:
http://www.innovativesystems.com/technology_solutions/anti_money_laundering.php
020 7422 6310
Innovative Systems Incorporated
10th Floor
30 Crown Place
London EC2A 4EB UK

Lexis Nexis - Bridger Insight:
http://www.lexisnexis.com/risk/products/bridger-insight.aspx
Call 0845 3701234 (Calls cost 7p/min)
+44 (0) 113 226 2065
30 Farringdon Street,
London,
EC4A 4HH

Logica - HotScan:
http://www.cgi.com/en/solutions/hotscan-isl

0845 0707765
Kings Place, 90 York Way
7th Floor
London
N1 9AG

NICE Actimize:
http://www.niceactimize.com/
0148 977 1633
160 Queen Victoria Street,2nd floor
London,
EC4V 4BF

NorthDoor - Sanctions Checker:
http://www.sanctionschecker.com/contact-us/
020 7448 8534
1-3 Dufferin St,
London,
EC1Y 8NA

Oracle:
http://www.oracle.com/us/products/applications/oracle-watchlist-screening-418846.htm
08705 332200
Oracle Parkway
Thames Valley Park (TVP)
Reading, Berkshire
RG6 1RA

Tonbeller - Siron:
http://www.tonbeller.com/en/solutions/
Fair Isaac Germany GmbH
+49-6251-7000-0
Werner-von-Siemens-Str. 2
64625 Bensheim
Germany

Worldcheck:
Http://risk.thomsonreuters.com/
020 7542 9550

Thomson Reuters - London
30 South Colonnade
Canary Wharf
London E14 5EP