Sanctions Screening Systems – “Plug-and-Play” Is a Thing of the Past

Issue

Institutions with deficiencies in their Office of Foreign Assets Control (OFAC) compliance programs and/or violations of the OFAC requirements and other global sanctions programs are increasingly in the crosshairs of regulatory enforcement actions. While poorly chosen or configured sanctions screening technology has not been the root cause of all of the financial services industry's sanctions problems, it is often a contributing factor. This is leading many financial institutions to abandon manual sanctions compliance efforts and various inefficient “home-grown” and first-generation sanctions screening systems in favor of more sophisticated technologies.

Financial institutions evaluating new sanctions screening technologies on the market should keep in mind that technologies with apparent “plug-and-play” capabilities and promising out-of-the-box functionality are, without question, not the right approach to meeting the expectations of regulators. While a touted plug-and-play, “set-it-and-forget-it” approach sounds appealing, institutions that fail to customize their sanctions screening software will see increased costs and operational risks (e.g., additional personnel to clear excessive false positives) and a higher risk of noncompliance.

Challenges and Opportunities

In our experience, the challenges of implementing a new sanctions screening system and enhancing an “out-of-the-box” one are similar. These challenges have less to do with the technology aspects of implementation (e.g., hardware, user interface design, etc.) and more to do with the complexities of matching functionalities and processes needed to calibrate the technology to the risk profile of the institution. Some of the most common and critical challenges to ensuring maximum effectiveness and efficiency from sanctions screening systems are detailed below:

- **Assessing the adequacy of system functionality:** A vendor solution may offer a set of advanced matching algorithms, which the institution may conclude to be comprehensive without taking into consideration the ethnic diversity of its customer base, potential misspelling of names when accounts are established, special characters (e.g., vowel and diacritic representations, non-standard word splitting, concatenation), etc.

- **Determining sanctions lists:** A vendor solution may include the option of using multiple sanctions lists, e.g., country-specific lists in addition to OFAC, United Nations sanctions, etc. Many institutions rely on these vendor-suggested lists, finding it too difficult to understand or decide which lists actually apply. The result may be unnecessary screening of superfluous lists, which the institution may not be required to scan its customers against, or, conversely, increased risk that the institution has not captured all required sanctions.

- **Consolidating watch list names:** When institutions use multiple lists, there is a high probability that the same entity will appear on more than one list. This can result in multiple, unnecessary hits against the same name and the need to resolve each duplicate hit, unless names are consolidated across the multiple lists used.
• **Identifying adequate matching rules:** Out-of-the-box configurations are often limited to matching entity names against the respective watch list names. The watch lists often contain additional attributes (e.g., date of birth, identification number, country of citizenship, etc.) that can be leveraged for identifying potential hits in a more effective manner (i.e., reduce the number of potential matches generated by applying the additional attributes against customer information, as part of the matching criteria).

• **Determining threshold settings using a systematic approach:** Matching rules generate hits when the score of matching criteria exceeds the pre-determined threshold value (commonly referred to as a matching score). Financial institutions relying on the out-of-the-box settings frequently experience an excessive volume of false positives, all of which must be reviewed and resolved; or, conversely, the system fails to generate hits, due to incorrect setting of the matching score. Regulators expect sanctions screening processes to be risk-based (i.e., commensurate with an institution’s risk profile), but reliance on out-of-the-box thresholds makes this difficult to support.

• **Lack of complete screening coverage of customers/transactions:** Failure to identify and include all data feeds (e.g., customers from various lines of businesses, types of transactions, etc.) that should be scanned by the sanctions screening system can result in a gap in the sanctions screening program.

• **Use of multiple sanctions screening systems:** More often than not, institutions lacking a centralized sanctions screening strategy end up deploying multiple sanctions screening systems (e.g., different lines of business implementing their own sanctions screening systems). This results in multiple versions of the same watch lists, disparate matching rules and varying threshold values, leading to potentially incomplete and unreliable sanctions screening and possible regulatory compliance issues.

Unfortunately, the challenges of implementing a customized system do not end here. Dealing with the sophistication of the logic of sanctions screening systems requires considerable time to configure, as well as a thorough understanding of the institution’s business operations and risk profile/tolerances. Awareness of these challenges can ensure that an effective, efficient, and appropriately risk-based global sanctions compliance program is developed and can facilitate the ongoing management of the system.

The items below detail some of the specific benefits that can be incurred from implementing a customized system correctly:

• **Increased effectiveness:** Customizing the various sanctions lists, identifying the appropriate matching algorithms, tuning targeted rules parameters and adjusting thresholds to identify potential matches all result in increased system reliability.

• **Increased efficiency:** The increased effectiveness of the system also helps to reduce the volume of obvious false positives. This in turn allows the institution, and alert adjudicators in particular, to focus on sanction hits that are more likely to be true sanction matches. As a result, adjudicators are able to refine investigation techniques, expedite review processes, and ensure time spent investigating potential matches is more meaningful.

• **Enhanced confidence through validation:** By independently validating the vendor-supplied system, the institution can gain confidence that the system is working or identify shortcomings that should be mitigated.

• **Centralized sanctions screening strategy:** By expending efforts to understand business operations, the institution’s risk profile and the data feeds responsible for sourcing customers and transactions, the institution is able to articulate a comprehensive centralized sanctions screening strategy that enables more targeted sanctions screening systems.
Our Point of View

The challenges of managing an effective sanctions screening system, and subsequently, a global sanctions compliance program, are not limited to the output and resolution of potential matches. There are a number of significant considerations across the entire lifecycle of the system that the institution must take into account. These include critical stages like vendor selection, calibration, implementation, ongoing tuning, and enhancement of the adjudication process of potential matches.

Based on our past experience assisting institutions with sanctions system implementations and validations, we have identified some of the most important points to consider for effective management of a sanctions screening system. We have broken down the lifecycle of a sanctions screening system into six phases, and detailed in the subsections below the critical considerations relevant during each phase:

Vendor Selection

In order to perform an effective vendor selection, the following questions should be considered:

- **Data volume:** Will the chosen product be able to manage the anticipated data volume? Failure to perform this analysis can result in significant performance bottlenecks.

- **Technology infrastructure:** Given the significant operational cost associated with the deployment and maintenance of a sanctions screening solution, will the selected solution be able to coexist seamlessly in the existing technology infrastructure?

- **Matching algorithm library:** Does the vendor’s solution provide capability to perform matching for non-English names? Does it provide the capability to perform fuzzy matching, and which algorithms (e.g., Levenshtein, SoundEx) are supported by the solution?

Watch List Sourcing

In the initial implementation, this phase addresses the selection of watch lists (both public and internal to the institution) to be used in screening, and the processes necessary to source the chosen lists. As part of ongoing system management, this phase determines the processes used to ensure watch lists are updated timely, accurately and completely.

Matching Rules Identification

Managing a sanctions screening system includes understanding whether an institution’s various processes (e.g., customer onboarding, alert adjudication) can facilitate or support more refined matching rules. More often than not, the institution uses name-only matching rules in the screening system. Since there are additional attributes available both on the watch list and in the customer data, it is imperative that rules are created by employing additional attributes such as date of birth, address, identification numbers, etc., to enable the institution to identify customers who cannot be identified using only a name-matching rule. Additionally, as part of the rule identification process, each rule can be assigned a score to enable investigators to prioritize their workloads.

Workflow Process Identification

The hits generated by the sanctions screening system will need to be investigated, therefore the system must contain an investigation workflow. The workflow should be identified and implemented into the system such that the hits can be investigated according to the business workflow of the institution and the relevant audit trails can be maintained.

Threshold Setting and Tuning

In this step, advanced statistical analyses are used to determine effective threshold values to be applied for each of the identified matching rules for successful execution. Prior to going live with the chosen thresholds from the threshold-setting exercise, a dry run of the matches-generation cycle should be performed to produce matches that can be investigated in the test environment. A successful investigation of these matches can provide insight into the match quality that can be
expected in the production environment. This step is important as it provides an opportunity to perform further threshold tuning before deploying the selected thresholds in production.

**Screening System Validation**

Though this step is not part of the initial implementation phase, institutions, specifically banking organizations, are required to perform an independent validation of the screening system that is currently in production. Below are some tests to consider when performing a validation of the sanctions screening system:

- Extract a statistically valid sample of names from watch lists (Sample 1).
- Extract a sample of names from the institution’s customer base (Sample 2).
- Create variations of sampled names by employing various algorithms like SoundEx, simple permutations, containment, etc.
- Test the system by utilizing a combination of Sample 1 and Sample 2 and their variants.
- Test the system by raising/lowering the matching score threshold values and collect hit statistics.
- Analyze the resulting hits to determine false positive and false negative rates.

The following graphic depicts the phases that constitute the lifecycle of a sanctions screening system:

![Sanctions Screening System Lifecycle Diagram](image)

**How We Help Companies Succeed**

Our AML professionals and our team of modeling experts, including Ph.D.-level professionals with deep quantitative skills, help institutions implement and maintain sound and robust sanctions screening systems. Collectively, we help financial institutions ensure that the configuration of their sanctions screening systems is based on the institution’s specific sanctions screening strategy and is in line with the institution’s risk profile. We have experience with a number of sanctions screening systems on various platforms including but not limited to Bridger Insight XG, FircoSoft and Fiserv, as well as with various home-grown systems. Our Sanctions Screening System services include the following:

- Assisting with sanctions screening system selection
- Development and execution of an effective, ongoing risk-based threshold setting (fuzzy logic) and tuning methodology
- Assessing the accuracy, completeness and effectiveness of the sanctions screening system
- Development and execution of an effective and efficient model validation methodology to independently audit/validate the technology in line with interagency guidance
- Enhancing the end-to-end process for reviewing and clearing potential matches and documenting results
Examples

System Validation

A large bank engaged Protiviti to assist with validation of its multiple sanctions screening systems. Our AML and technology experts worked with the representatives from the bank’s business and IT departments to obtain all pertinent information on the systems’ configuration (e.g., matching rules, score values) and source feeds (e.g., customers, transactions) to understand the configuration of the deployed sanctions screening systems. We used our proven validation and threshold setting methodology and customized it to address the bank’s needs. Upon conclusion of our validation efforts, we provided valuable recommendations on improving matching rules and the threshold values.

System Selection

A multi-bank holding company requested our assistance with assessing multiple systems to identify the optimal sanctions screening software to support its AML and OFAC program. Protiviti developed matrices with weighted vendor, performance, functional and technical criteria to facilitate the comparative analysis of each type of software. The evaluation criteria were based on previous experience with various types of systems, user and system manuals, research, and discussions with the bank’s power users and management. At the end of the engagement, we provided analysis ratings of the different software solutions based on the identified functional and technical criteria to summarize the key strengths and weaknesses of each system.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Carol Beaumier  
+1.212.603.8337  
carol.beaumier@protiviti.com

Shaheen Dil  
+1.212.603.8378  
shaheen.dil@protiviti.com

Bernadine Reese  
+44.20.7024.7589  
bernadine.reese@protiviti.co.uk

Luis Canelon  
+44.20.7024.7509  
luis.canelon@protiviti.co.uk