Validating Real-Time Sanctions Screening Systems: Critical Considerations

**Issue**

The majority of financial institutions today rely on third-party screening systems to perform sanctions screening. Banking organizations that provide funds transfer services to their customers are under increased scrutiny to perform real-time scanning against various sanctions lists of all payments going out and coming in on behalf of their customers. Similar to the trend we have seen with anti-money laundering (AML) transaction monitoring systems, regulators expect financial institutions to be able to demonstrate that sanctions screening systems are configured correctly. The challenge for financial institutions is finding the right balance between being able to detect sanctions violations and processing payments for their customers without unnecessary delay.

To meet this challenge, it is important that financial institutions understand their screening environments better and comprehensively validate and tune their sanctions screening systems to make sure that they are effective, efficient and provide the required coverage from a regulatory perspective.

**Challenges and Opportunities**

Financial institutions are presented with a multitude of challenges when it comes to validating and tuning a third-party sanctions screening system successfully. These include:

- **A large number of transaction types.** Typically, banks in the U.S. use either the Fedwire Funds Service or the Clearing House Interbank Payments System (CHIPS). These are the two primary domestic wholesale payment systems used for interbank funds transfers. For cross-border funds transfers, a messaging infrastructure called Society for Worldwide Interbank Financial Telecommunication, or SWIFT, is used. In addition to customer and bank funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections and documentary credits. These transaction types are defined in more than 100 different formats, each denoting a different transaction type. For example, SWIFT MT1nn is used for customer payments whereas an MT2nn format indicates a financial institution transfer. Each message format has unique placeholders for capturing the various data items applicable to that transaction. Identifying these data fields and mapping them accurately to watch lists can be challenging, given the number of different formats.

- **Misconfigured watch lists.** Banks also struggle with choosing the right watch lists for their real-time transaction screening process. Typical problems are scanning against inapplicable watch lists offered by the third-party vendor, scanning against more lists than necessary, and not scanning against relevant lists. These situations can happen if the bank has failed to perform adequate analysis and configuration during the implementation of the third-party system. Some commonly used sanctions lists include the United Nation’s al-Qaeda sanctions list; the Specially Designated Nationals list issued by the U.S. Office of Foreign Assets Control (OFAC); the consolidated list of Persons, Groups and Entities Subject to EU Financial Sanctions; and the
Financial Sanctions list of HM Treasury (UK). Since many of the national sanctions lists are based on sanctions imposed by the UN, names appearing on UN lists can also appear on the lists issued by the EU, OFAC and HM Treasury. Using these watch lists redundantly can result in unnecessary false positives, which can create additional work for investigators and delay payments. On the flip side, not using all the lists that are mandated may result in false negatives, causing transactions involving sanctioned entities to go undetected.

- **Complex proprietary matching algorithms.** Many third-party systems come bundled with complex name-matching algorithms that are difficult for banks to understand. Typically, these algorithms employ various matching techniques to identify records from two sources – the bank’s systems and the third-party watch list – that contain information about the same entity. These algorithms are often proprietary, and the underlying source code is not available to financial institutions to help them understand the underlying methods. Lack of an in-depth understanding of the system negatively impacts the validation strategy and results in financial institutions performing “black box” testing, which doesn’t accomplish the comprehensive validation required from regulators.

These challenges notwithstanding, a comprehensive validation, testing and tuning process of the sanctions screening system is both necessary and possible, with the following benefits to the financial institution:

- **Meeting regulatory expectations.** Periodic testing and tuning of the sanctions screening system allows financial institutions to determine the level of coverage provided by these systems and demonstrate to regulators that their systems and processes are configured in line with regulatory expectations.

- **Reduction in false positives.** Regular testing and tuning helps reduce the false positives the system generates. This improves the efficiency of the sanctions screening process by reducing the number of potential matches an analyst needs to research, increasing productivity and minimizing the risk of delaying a customer’s payment.

- **Maintaining control.** Capturing and reviewing key metrics as part of an ongoing tuning process allows financial institutions to maintain continuous compliance. For example, as a financial institution’s risk profile changes (with the addition of new products and service offerings or with changes in the customer base), the system will be exposed to more and different transactions. By tracking key metrics, such as the “hit” rate (i.e., the number of potential sanction matches), financial institutions can see trends and detect spikes or drops in the hit rate which may be an indicator that the system needs to be retuned or that a data quality issue exists.

**Our Point of View**

Validating and tuning a sanctions screening system that scans real-time transactions is a multistage process requiring significant time and effort. Based on our experience, we have identified the following key steps to this process:

**Performing a data integrity audit.** Most organizations store their data in multiple locations in a variety of formats. In order to perform the required validation, financial institutions must ensure that the sanctions screening system is able to access all these different systems and automatically integrate the data sourced from them. For example, payment transactions typically are sourced from the institution’s in-house payment system, while the watch lists are sourced from external list providers; data anomalies or missing data in either of these sources can negatively impact the results of the testing. Thus, auditing all data and checking it for inconsistencies are crucial prerequisites to the validation process.

**Identifying transaction types to be scanned.** To begin the validation process, financial institutions must identify the various transaction types they use in order to ensure proper coverage for the sanctions screening program. Based on their products and service offerings, financial institutions can use any number of SWIFT message formats to provide transactional services to their customers.
The following table, which is intended to be illustrative and not all-inclusive, lists some of the commonly used messages and the scanning requirements for them.

<table>
<thead>
<tr>
<th>SWIFT Message</th>
<th>Description</th>
<th>Scanning Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT0nn</td>
<td>System messages</td>
<td>No</td>
</tr>
<tr>
<td>MT1nn</td>
<td>Customer payments</td>
<td>Yes</td>
</tr>
<tr>
<td>MT2nn</td>
<td>Financial institution transfers</td>
<td>Yes</td>
</tr>
<tr>
<td>MT3nn</td>
<td>Treasury markets</td>
<td>Yes, if used for currency exchange and security trades</td>
</tr>
<tr>
<td>MT4nn</td>
<td>Collection and cash letters</td>
<td>Yes, if used to purchase a monetary instrument</td>
</tr>
<tr>
<td>MT5nn</td>
<td>Securities market</td>
<td>Yes, if used for security trades</td>
</tr>
<tr>
<td>MT6nn</td>
<td>Treasury markets – metals and syndications</td>
<td>Yes, if used for security trades</td>
</tr>
<tr>
<td>MT7nn</td>
<td>Documentary credits and guarantees</td>
<td>Yes, if used for letters of credit</td>
</tr>
<tr>
<td>MT8nn</td>
<td>Traveler’s cheques</td>
<td>Yes</td>
</tr>
<tr>
<td>MT9nn</td>
<td>Cash management and customer status</td>
<td>Yes, if used for a wire transfer</td>
</tr>
</tbody>
</table>

**Identifying and mapping the critical transaction data fields.** The data fields of various formats must be matched accurately to ensure proper validation. Funds transfers present an increased degree of risk for financial institutions due to the number and dollar volume of transactions, the geographic locations of originators and beneficiaries and the fact that not all originators and beneficiaries are bank customers. Typically, international funds transfers are performed using one of the global SWIFT formats (e.g., MT103, MT202), and the domestic funds transfers are performed using the Fedwire format. Regardless of the format of the transaction, the following data fields are critical and need to be mapped accurately for testing:

- Originating party’s name
- Originating party’s country and address lines
- Originating bank
- Originating bank’s country and address lines
- Intermediary banks involved in the transaction (first, second and so on)
- Beneficiary bank
- Beneficiary bank’s country and address lines
- Beneficiary party’s name
- Beneficiary party’s country and address lines

**Selecting test samples.** A watch list sample set consisting of both “good” and “bad” samples needs to be created for various systems and comparisons testing. The “good” sample should consist of names which have a very low probability of reconciling to a regulatory watch list. Typically, these are the financial institution’s actual customers who are known to be low risk. The “bad” sample should consist of a statistical sample of names and/or other supporting fields from all the regulatory watch lists that are in use by the third-party system.

**Applying name-masking algorithms.** The “bad” sample should be further expanded to include several variations of a single name. This is done in order to test the capability of the system to apply “fuzzy logic”
to match the altered names against the same entity in the watch list. Some commonly used algorithms include:

- **Soundex.** Soundex is a phonetic algorithm for indexing names by sound, as pronounced in English. The goal is for names that are pronounced similarly to be encoded to the same representation so they can be matched despite differences in spelling. For example, Mary can be matched to Marie, and Carmen can be matched to Carman. The purpose of this test is to verify whether the system is robust enough to recognize a misspelling of a name based on pronunciation.

- **Containment.** The objective of the containment algorithm is to provide only a portion of the name while performing the list matching. For instance, Matthew can be truncated to Matt, Robert to Rob, etc. The purpose of this algorithm is to ensure that the sanctions screening system is able to identify a customer based only on a portion of the name.

- **Extraneous characters.** The purpose of this algorithm is to introduce stray characters into the name and test whether the system is able to bypass these extraneous characters and match the name against entries in the watch list. For example, the system should be able to match ODonnell and O’Donnell.

- **Permutations.** Permutations are achieved using various combinations of first, middle and last name. For example, switching the last and first name while leaving the middle (if applicable) the same is one possible variation. Another one is taking the first initial of the first name and leaving the rest of the name unchanged.

**Tuning.** Tuning is the essential and crucial next step in the validation process. The results from the iterative testing process should be used as an input to the tuning process. A sensitivity analysis should be performed by executing “above-the-line” and “below-the-line” testing. This is done by changing the score thresholds above or below the current settings to arrive at the optimal scoring threshold to which to configure the system – one where an acceptable balance exists between true and false positives.

**Test Environment.** Last but not least, a fully functional test environment is key to any enterprise system testing. Because automated batch processing is the most efficient way to test sanctions screening systems, the test environment should be configured to allow for that. For example, a sample of transactions with Soundex name variations for the originating parties could be grouped into a single batch and executed as one test.

**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 perform robust, independent validations of their 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 its risk profile. We have experience with a number of AML sanctions screening systems on various platforms, including, but not limited to, Actimize, FircoSoft, Sydel, OFAC Watch, Equifax, TransUnion and Thomson Reuters Accelus, as well as a number of homegrown systems.

Our sanctions screening services include:

- Comprehensive independent testing of the sanctions screening system
  - Filter validation
  - Watch list selection
  - Data validation
  - Lookback
- Filter tuning methodology and approach design
- Threshold setting and tuning

**Example 1: Independent Validation of a Third-Party Sanctions Screening System**

A large foreign bank with operations in the U.S. engaged Protiviti to assist with independent validation of its sanctions screening system supplied by a third party. We developed a systematic testing methodology that took into account the transaction feeds from the core banking application and the various U.S.-required watch lists, as well as the watch list required by the bank’s home country. We created more than a thousand test cases to scan fields on the real-time Fedwire and SWIFT transactions against sanctioned entries on the watch lists. This level of detail allowed us to effectively challenge the system beyond the basic name-matching function and validate the consistency and accuracy of the screening process. We applied masking to introduce variations to names and other elements within the bank’s transactions, enhancing the validation tests beyond the basic actual-to-actual match. We also developed a systematic threshold setting and tuning methodology that involved performing threshold sensitivity analysis to arrive at the right threshold setting for the matching algorithms used by the sanctions screening system.

At the end of our engagement, we delivered to our client a report with identified gaps and other findings, along with recommendations for enhancing the bank’s sanctions screening program. Our final deliverables included the detailed testing procedures, the threshold setting methodology and the recommended thresholds for achieving the right balance between true positives and false positives. By leveraging our services, the bank was able not only to address critical gaps in its sanctions compliance program but also to create a roadmap for future implementation of the recommendations and best practices we provided.

**Example 2: Model Validation of Multiple Sanctions Screening Systems**

A top-25 U.S. bank engaged Protiviti to perform a model validation of the quantitative aspects of its sanctions screening models. The validation scope consisted of eight different list screening systems used across multiple business segments within the bank. We developed a scenario-based methodology, which utilized fuzzy matching techniques, good and bad samples and various combinations of regulatory watch lists to test the performance of each system on a stand-alone basis and relative to other systems. Fuzzy matching techniques were used to mask names and other transaction details to assess the ability of each system to detect small variations of regulatory watch list entries.

Our deliverables consisted of a report with gaps and findings, along with recommendations for tuning the current score thresholds within the bank’s sanctions screening systems. In the report, we identified which transaction components are most predictive of true positives on a system-by-system basis (by matching multiple fields, such as name, address and date of birth, rather than a single field). In addition, we uncovered potential cost savings for the bank by identifying which systems had very similar scoring mechanisms and could be consolidated to reduce screening efforts. Our report included the detailed testing procedures, validation methodology, and analyses of scoring thresholds within each system in terms of true positive and false positive rates. Leveraging our findings and recommendations, the bank was able to address critical gaps in its sanctions compliance and improve the efficiency of its program.
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 40 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

Bernadine Reese  
+44.20.7024.7589  
bernadine.reese@protiviti.com

Shaheen Dil  
+1.212.603.8378  
shaheen.dil@protiviti.com

Luis Canelon  
+44.20.7024.7509  
luis.canelon@protiviti.com

Chetan Shah  
+1.704.972.9607  
chetan.shah@protiviti.com

Amith Satheesh  
+1.704.998.0792  
amith.satheesh@protiviti.com