Sanctions screening filters: improving efficiency without compromising effectiveness

How a detailed understanding of your filter's performance and its alignment with policy can deliver more efficient operations

Sanctions screening filters play a crucial role in tackling financial crime by enabling banks to screen transactions against different jurisdictional sanctions/watch lists. However, in the last few years the way in which financial institutions use filters has evolved considerably – not least because regulatory expectations have become more demanding.

As such, regulators are looking for evidence that the lists and data going into filters are accurate and that filters are flagging up the appropriate names. Regulators are increasingly classifying screening environments as models, a distinction which brings with it the scrutiny of internal model risk teams and the need to understand and document models.

At the same time, regulators are less tolerant of mistakes than in the past. They are looking for evidence that banks are carrying out robust implementations and ongoing testing to make sure that their sanctions screening filters are working appropriately. They expect banks to understand filter performance in detail, explain how this aligns with compliance policies and risk appetites, and demonstrate that changes made for efficiency gains do not negatively affect screening performance.

Consequently, whereas previously banks tended to follow vendor guidelines when setting the parameters of their filters, regulators increasingly expect institutions to have – and be able to demonstrate – a thorough understanding of how their filters operate. They also expect banks to configure their filters in accordance with their specific requirements.

Financial institutions will therefore need to make some critical decisions when setting up their filters. Central to these decisions is how the bank approaches the competing goals of filter effectiveness and filter efficiency.

The more effective a filter is, the less efficient it is likely to be, and vice versa. While this sounds like a balancing act, in practice banks want to ensure that their filters do not fall below the required level of effectiveness, while tuning for greater efficiency where possible.

Nicolas Stuckens
Head of Sanctions Compliance Services, SWIFT

Nicolas Stuckens heads SWIFT's Sanctions Compliance Services team. In this capacity, he is responsible for SWIFT's portfolio of hosted sanctions utility solutions, including Sanctions Screening, Name Screening and Sanctions Testing. Nicolas also manages SWIFT's relationship with a number of industry associations, such as The Wolfsberg Group, and is responsible for the SWIFT Sanctions Advisory Group.

Testing and data quality solutions

Sanctions Testing

Sanctions Testing is a secure, hosted tool that enables banks to test their sanctions filters and lists and optimise screening performance, either at scheduled intervals or on demand.

As well as delivering independent quality assurance of banks' transaction, customer and PEP filters, the service assesses filter models, fuzzy matching and false positives in order to improve performance iteratively. Peer Assessment, an optional add-on, enables users to evaluate the performance of their filters against data from other participating users.

Payments Data Quality

Payments Data Quality is a SWIFT-hosted data analytics service for correspondent banks. The solution enables banks to obtain a single, global overview of their SWIFT payment messages and evaluate and improve the quality of the originator and beneficiary information.

Better data helps sanctions screening systems function more effectively, and delivers operational and business benefits, including enhanced straight-through processing (STP) and payments processing efficiency.

Effectiveness versus efficiency

The role of the filter is to screen transactions and flag up any items that appear on the relevant sanctions/watch list(s). While achieving this is essential from a compliance point of view, in practice almost all of the alerts issued will be false positives. It is therefore important that the alerts issued are understandable and worthy of escalation.

A system which is highly effective is also likely to be inefficient. The more false positives the filter produces, the more people will be required to process those false positives – and the higher the risk that human error will result in a potential match being missed. Additionally, if more people are required to handle the higher number of alerts, this will result in higher personnel costs as well as associated costs for items such as additional premises space and IT infrastructure and equipment.

For banks, it is therefore important to decide how to find the right balance between having too many alerts and having the right quality of alerts. Under no circumstances, however, can the filter's effectiveness be compromised. Above all, the system must continue to be aligned with the bank's internal policy and risk appetite.

This means the filter needs to achieve the required level of effectiveness before any steps are taken to make it more efficient. In addition, any changes made for efficiency purposes need to be fully aligned with institutional policies for compliance and risk, and this needs to be documented.

Achieving effectiveness

Filter performance is determined by many factors, including the quality of the list and transaction data being used. Filters are set up on the assumption that data quality will be high, so any errors in data – such as missing letters, added letters or transposition of letters – can affect the filter's detection capabilities.

At the same time, the way in which effectiveness is measured can vary. Even if a bank were to stipulate that the filter's effectiveness rate needs to be 100%, the definition of 100% might not be the same for every financial institution. Some banks will intentionally exclude certain elements from screening – so if the only items that are missed are those that have been missed intentionally, the hit rate will still effectively be 100%. The choice to exclude some elements from screening will be related to the institution's risk decisions, the geographies served by the institution and the capabilities of the system in place.

Incremental changes

Once the system is operating effectively, the institution will be in a position to seek opportunities for efficiency improvements. Before doing so, however, they should have a detailed understanding of filter behaviour based on a broad range of test factors and data points. With such understanding in hand, banks can make small adjustments to filter configuration parameters in order to increase efficiency in a controlled and incremental way. This involves making a small change and then retesting the filter in order to assess whether its performance has been impacted before making another change. Not all changes will produce the desired results, so it is important to limit the scope of each iteration and to document the configuration settings used for each iteration.

This iterative approach is crucial to making sure that the system continues to operate at the required level without compromising the filter's effectiveness. Banks should document which changes are made, and why, and ensure that these are aligned with internal policy and risk appetite.

First and foremost, the institution needs to determine the objectives of the tuning project – for example, addressing the issue of false positives. The institution should then review the different configuration options available to identify changes which could meet the defined objectives. The testing process will typically include the following types of test:

- **Baseline testing**
  This is broader in scope, providing a before and after comparison of a configuration change. Baseline tests can be used to check that a configuration change will not affect the behaviour of the filter in an unexpected way.

- **Tuning focus testing**
  Focusing on specific scenarios, these tests measure the success of different configuration options compared to the institution's tuning objectives. The results should be reviewed after each iteration.

- **Impact testing**
  This measures the impact of the configuration change on hit rates. While artificial data can provide an indication of impact, tests should use a sample of real production data in order to provide accurate results.

There are a number of different ways in which the filter can be adjusted. Possible changes include adjustments to the parameters of the filter, as well as to the process data quality and the list quality, and might even include addressing specific false positives.

For example, if a person trying to open an account shares a name with someone included on a sanctions list, they will generate a hit. The financial institution can adjust the filter so that no further hits are generated when the person opening the account begins making transactions.

In other cases, filters may generate hits against short names of less than four letters or single name aliases. If required, banks can choose not to have these controls in place. It is important to remember that every filter – and indeed every version of every filter – works differently, and that a vast range of controls are available. As a result, managing the different controls can be a costly exercise which requires considerable resources to manage.

Approaches to sanctions testing

In practice, this iterative testing process is difficult to carry out without access to the right resources: each iteration can take time to complete and banks may find they need to make compromises in terms of the scope of the exercise.

Some banks will have a dedicated team in place to carry out testing while others may seek external input. Banks can use standardised testing platforms, some of which may enable them to benchmark their testing results against those of other institutions. However, it is important to note that some testing techniques are more effective than others. In many cases, institutions use their customer data for testing purposes – but this data is unlikely to contain many sanctioned individuals, so the value of this method of testing may be limited.

A more effective method is to test with a complete set of data including all of the lists in scope, and all of the entities from those lists, which is the approach taken by SWIFT's Sanctions Testing service. Providing independent reporting and assurance, Sanctions Testing is a community developed tool which is used by over half of the world's top 50 banks. The service enables banks to demonstrate robust filter performance by carrying out comprehensive, on-demand testing based on live sanctions lists.

Banks using the service can choose to test a number of different systems or configurations, or can test the same system repeatedly in order to monitor changes over time. The ability to track test results provides a valuable audit trail, while graphs and charts can be used to gain a visual understanding of the results. Tests can be customised with different sanctions list data and can be provided in different message formats such as SWIFT MT, ISO 20022, Fedwire, CHIPS and customer record formats. The service also includes Peer Assessment, an optional add-on which enables institutions to compare the performance of their own filters against that of peer institutions with similar business and risk profiles.

Ongoing review

Optimising a filter is not a one-off exercise. Even when the filter is operating as needed, banks should be aware that any adjustments made to the filter may be affected by other developments over time. As in the example above, institutions can mark a specific name as approved in the filter so that the name will no longer generate alerts – but changes in the system could cause approved names to be re-alerted in the future. Likewise, changes to the jurisdictional list for an entry might mean that a name previously marked for exclusion now generates an alert.
As such, banks should carry out assurance testing to check that their tools continue to work as expected. This may include conducting regression testing to ensure that filters continue to detect not only all the necessary items, but also those specifically marked for exclusion – particularly when new releases take place. By running production data through the new release in a user acceptance testing environment, institutions can check that the only differences compared to the production filter are those expected as a result of the new release.

SWIFT's sanctions compliance services

Sanctions Screening
This fully-managed, securely hosted service lets you screen incoming and outgoing transactions against all leading watch lists, Sanctions Ownership Research lists from Dow Jones, and your own private lists.

Name Screening
Hosted by SWIFT, Name Screening enables you to screen individual customer names (and soon customer and PEP databases) as part of your ongoing compliance process.

Sanctions Testing
Enables customers with their own sanctions filters to test and certify the performance of their transaction, customer and PEP filters.

Sanctions List Distribution
Packages up-to-date public watch lists with additional BIC enrichment for download in standard and advanced XML format.

Conclusion

The cost of having a filter which is not fully effective is not to be underestimated. Banks may face regulatory repercussions if the controls they have in place are found to be inadequate, and this can also lead to reputational damage. But the costs of inefficiency can also be considerable, from the financial implications of having a larger team carrying out manual processing to the risks associated with greater levels of human intervention.

While no bank will want to make changes that weaken filter performance, it is still possible to optimise screening operations by making incremental changes and re-testing after each change has been made. In this way, banks can make controlled efficiency improvements based on a comprehensive understanding of filter performance while documenting the rationale behind every change.

Tools such as SWIFT's Sanctions Testing service can enable banks to carry out this type of testing quickly and robustly based on a broad data spectrum – thereby improving the performance of the filter and keeping costs under control. By approaching the process in this way, banks may be able to achieve greater efficiency while still ensuring that their filters are performing at the required level.

About SWIFT

SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community's access and integration, business intelligence, reference data and financial crime compliance needs. SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

www.swift.com/complianceservices

57285 - June 2017