Information paper

Sanctions filters: the expert guide

A practical guide to maximising the effectiveness of your sanctions filters

Contents

How regular testing and tuning can help you achieve peace of mind.

The poll results in this paper reflect audience voting during the webinar.

Executive Summary

In the current regulatory climate, it is essential that institutions screen their customers and transactions against relevant sanctions and PEP lists. Simply having the correct tools in place is no longer sufficient, however. Institutions are expected to configure their sanctions filters properly and test the filters to confirm that they recognise sanctioned names and name variants effectively. Filter tuning is important to maintaining optimal efficiency, particularly given the constant evolution of sanctions lists. And compliance teams need to demonstrate an overall understanding of their filter environment and operation, underscoring the importance of proper training.

This paper summarises a panel discussion involving senior compliance experts from Citi, JPMorgan Chase, PwC and SWIFT as part of the ACAMS webinar series. The panellists addressed evolving regulatory expectations around sanctions compliance, including the growing expectation by regulators that banks should have a detailed working knowledge of sanctions filter operations.

The role and importance of technology was considered, as was its importance in embedding filter testing, assurance and optimisation into business as usual processes.

With compliance costs on the rise, panellists noted that institutions that want to tune their filter settings to reduce the number of false positive hits must do so without impacting filter effectiveness in ensuring that sanctioned individuals and institutions are detected correctly.

The panel concluded that regular systems testing and model validation are vitally important in order to ensure correct filter operation.

PANEL MEMBERS

Vikas Agarwal, Partner, Risk Assurance Services, PricewaterhouseCoopers LLP

Brandon Corchinski, Executive Director, AML Model Risk Management, JPMorgan Chase

Crystal Noe, SVP - Sanctions Screening Solutions, Citigroup Inc

M. Babar Shameem, Global Head - Anti-Money Laundering and Sanctions Screening, Citigroup Inc

The panel was moderated by John Pattenden, Sanctions Testing Product Manager, SWIFT.

The webinar took place on 17 March 2016 and a free recording is available at www.ACAMS.org

Regulatory Expectations

How regular testing and tuning can help you achieve peace of mind.

In the area of sanctions, expectations from regulators are becoming more stringent, with fines recently imposed not only on banks, but also on other types of organisation including payments companies and casinos. As such, many organisations are staffing up in order to meet their requirements in this area – either by bringing in outside expertise, or by gaining more expertise internally.

A key topic is the use of sanctions filters to screen transactions and customers against sanctions lists. Regulators are increasingly focused on making sure that such filters are used correctly, and are looking at three key areas:

- The quality of the data which is going into the filter – is the data complete and accurate?
- The filter itself – are names being matched appropriately?
- The quality of the output – how is this being investigated and monitored?

Regulatory expectations in this area are becoming more demanding. For one thing, regulators are showing less tolerance for errors than in the past.

Meanwhile, the scope of sanctions filtering is expanding to include not only the matching of names, but also elements such as address and date of birth. Sanctions compliance as a whole is increasingly complex, with some sanctions regimes forbidding transactions with companies because their boards or beneficiaries include sanctioned individuals, even though the companies themselves are not on sanctions lists.

Know your filter

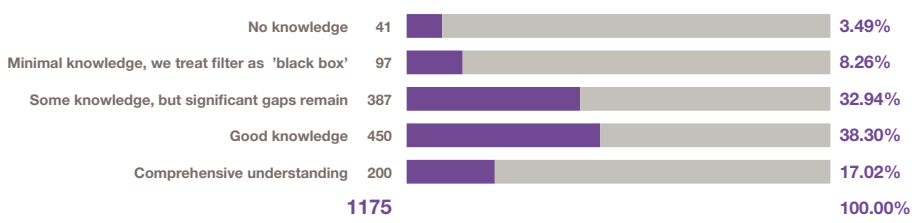
Having an appropriate filter in place is critical, but in recent years there has been a growing need for institutions to gain a greater understanding of the filters they use. In the past, institutions would typically set the parameters of their sanctions filters in accordance with instructions from the vendor. Today, this approach is no longer seen as acceptable: regulators expect institutions to know how their filters operate instead of relying on vendors. This has implications both for banks, who need to increase their knowledge of these systems, and for vendors, who need to open up their systems to allow clients to understand them better.

It is likely that this trend will continue in the future. The industry has already seen a shift from simply having a tool in place to knowing and understanding that tool. Going forward, this may expand to include reviewing how well institutions are preparing their teams to manage their tools.

> When the Patriot Act came in, we saw a lot more AML tools enter the space. One question from regulators was, 'Are you automated or manual?' Then it was, 'What tool do you have?' Now the question is, 'How well do you know your tool? How well do you know your data? How well do you understand your risk?'

> You need to have the vendor provide as much clarity as possible. Regulators want you to understand how the filter works. The way you do this is you have your vendor provide the information. It has to be shared.

How well does your institution understand the operation and control of your customer / transaction screening filter(s)?



Filter Effectiveness and Model Validation

It is important to make sure that any sanctions filters used are operating as expected. Many different factors may affect the way in which a filter operates – including changes by upstream systems, which can have unintended consequences.

Testing can provide assurance that a screening tool is working today as well as it did yesterday and that it is providing the necessary protection.

This includes making sure that there are no unintentional effects as part of upgrades, system patches or environmental changes between a user acceptance testing (UAT) environment and production.

As a first step, when assessing the effectiveness of a filter, institutions should document the functionalities of the model or tools used for screening. It may be helpful to split these into the functionalities that suppress alerts, and those which are more administrative in nature. Functionalities which are used for suppression will be reviewed more rigorously by model validation teams from regulatory environments.

For both internally developed and vendor provided software, regression testing should always be performed as part of any implementation. Institutions should validate regularly that functionality is working correctly. Suppression logic that comes into effect post-filtering should also be included in any testing programme, as this will impact the output of the model itself.

Data quality

The quality of data is crucial when it comes to the effectiveness of a sanctions filter. While everyone has 'bad data', it is important to understand where an organisation's data weaknesses are and to make sure that the settings on the sanctions system are tailored to those weaknesses.

Organisations should consider performing a data quality assessment, whereby data elements which are critical for the screening process are identified and rules are created for those data elements – such as not having the word 'corporation' in an individual's name. Such rules can then be automated to trigger a process for data improvement.

Model validation

Model validation is used to check that changes to filter configuration will deliver predictable – and correct – results. This involves the following steps:

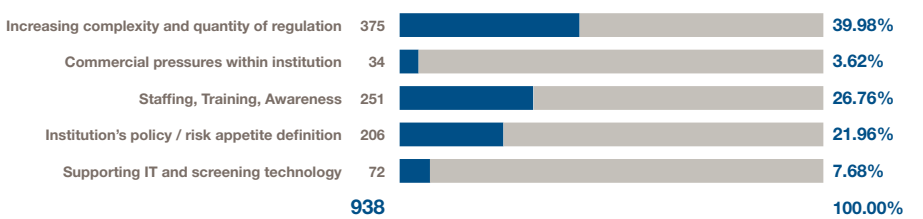
1. Have a well-defined validation plan with step-by-step, repeatable processes, such that anyone could pick up the document and perform the test.
2. Make sure that sample sizes are large enough to give the final conclusions statistical significance.
3. Ensure that customers and transactions are properly segmented and represented by geography.
4. Provide evidential support of all the analysis that has taken place.

"As it relates to data quality, there will always be issues that arise. It's important that you have data flows that map from the filter back to the source system – the system of record at your institution – so that you can identify where issues may have occurred.

"Regulators today expect institutions to really understand the risks that they have, the client profile, the geographic regions that they have, and use those parameters to drive how their filter setups are happening. It's really on the institutions to do that, and not on the vendors.

Top sanctions compliance challenges

Which of the following is your #1 challenge in terms of ensuring that sanctions controls are working?



How regular testing and tuning can help you achieve peace of mind.

Organisations typically use different filters to meet different needs. An institution might have one or more filters in place for screening dynamic information such as payments and trade transactions, and other filters for screening databases, such as customers, accounts and politically exposed persons (PEPs).

Technology plays an important role in helping institutions test the effectiveness of their filters. Organisations can use standardised testing platforms to carry out regular validations. The platforms will generate a set of test cases which can be run through the filter. The results are then fed back to the test platform, which performs an analysis of the results and indicates the effectiveness of the filter. In some cases, this may include benchmarking the organisation's results against other institutions.

Best practice in this area includes having a 'golden set' of complete, up to date, accurate test data, and fuzzy variants of this data, whereby a number of scenarios are entered into the system to see how it reacts. Institutions can also carry out parallel testing using a second system, enabling them to compare results.

Know your filter

Resources are often tight in this area, and sanctions is a niche area of expertise. Matching names and understanding what needs to be screened across complex lines of business requires significant expertise.

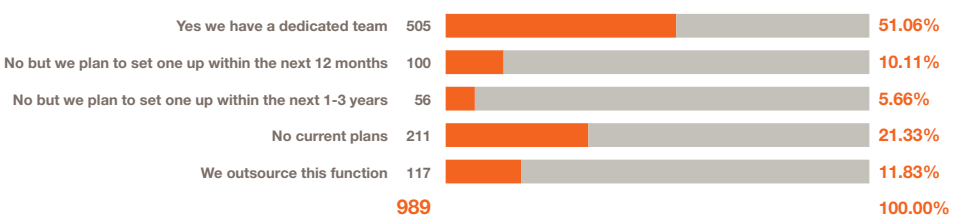
Where possible, it can be helpful for institutions to build internal training programmes so that subject matter experts can pass on their knowledge to others within the organisation. By institutionalising knowledge in this way, organisations can make sure that the relevant information is retained in-house, despite staff turnover.

If an institution does not have the in-house expertise needed to create tests, it may be advisable to appoint a third party organisation to carry out the initial validation. As well as meeting requirements, this can provide a valuable opportunity for people within the organisation to educate themselves about the test scenarios being used in the market today.

Peer banks can also be a useful resource. People who use the same technology elsewhere may be more successful in obtaining information from vendors about the technology they are using. Even if the peer bank is working with a different vendor, it can be helpful to understand how the bank in question approaches the testing process. Having open discussions – without sharing sensitive information – can be beneficial for both parties.

> "The maturity that the US sanctions have is recognised around the world. So if you're seen in a positive light in the US from a regulatory perspective, you're going to be reasonably well positioned in dealing with other regulators.

Does your institution have a dedicated team to perform effectiveness and efficiency testing of your filter(s)?



Tuning and Optimisation

Having too many false positives is not a satisfactory situation and can indicate that a sanctions filter needs to be optimised. Other factors can make it necessary to tune the filter, such as the introduction of a new business line or the implementation of a new watch list.

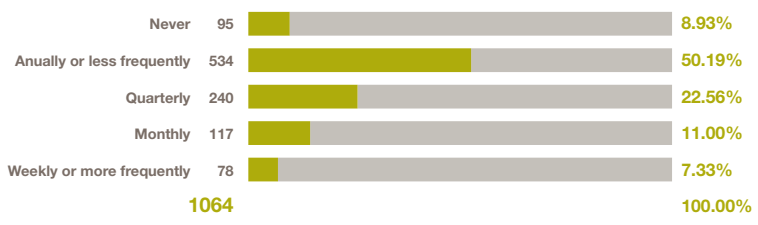
It is important to check that screening settings are appropriate – in other words, that the organisation is screening relevant data against the correct list, and that the correct entity types are being screened against each other. Where possible, institutions should use the filter to screen individuals against individuals, or businesses against businesses, in order to limit false positive alerts.

Tuning may also be appropriate where lists are concerned. Vendors may supply a large number of sanctions lists, but a particular institution may only be concerned with one of those lists. In practice some institutions may be screening against lists which are not really applicable to their businesses. It is therefore important to evaluate what exactly the organisation is screening against to ensure that the appropriate regulatory expectations are being met – but not necessarily exceeded.

“

Testing and spot checks can really help you measure the performance of a system. Those metrics can be about your type one and type two error rates; what's going on in terms of where you're having hits; how close to the line they are; making sure you're monitoring how much data's going into the system and whether there's any drop-off in that data.

How frequently do you test the effectiveness of your institution's filter(s)?



Conclusion

With regulators placing ever greater demands on institutions in the area of sanctions, it is important to gain a deeper understanding of the sanctions filters in place.

Meanwhile, filter testing, assurance and optimisation are becoming part of a business as usual process.

In order to meet growing demands in this area, institutions can draw upon technology to support internal assurance measures and gain the level of understanding increasingly sought by regulators.

Sanctions Testing from SWIFT

Understand and optimise the performance of your screening systems and processes

SWIFT developed Sanctions Testing to help banks understand and demonstrate the operational effectiveness of their sanctions filters.

Sanctions Testing provides independent reporting and assurance based on a secure, SWIFT-hosted testing application; test scenarios using the latest sanctions lists; list validation and alerts; and expert advice from SWIFT consultants. On-demand, automated testing is possible based on live sanctions lists updated in real time.

Sanctions Testing was developed in collaboration between SWIFT and its customers, and this collaborative approach enables the creation of best practices around sanctions compliance. It is used by more than half of the world's top 50 banks.

SWIFT also offers Sanctions Testing Peer Assessment, which enables institutions to compare their filter performance against that of peer institutions with similar business and risk profiles.

For more information, visit www.swift.com/sanctionstesting

SWIFT's Financial Crime Compliance Services Portfolio

SWIFT delivers best-in-class compliance services whose standardisation and economies of scale can benefit all users, regardless of organisational size or geographical location. Community-based pricing and the ability to align compliance processes with market practice are additional benefits of our unique approach.

For more than 40 years, SWIFT has connected the industry, enabled the creation of global standards and provided a collaborative forum to address industry needs. Now, our services are facilitating our customers' sanctions and KYC compliance activities and enabling them to derive unique analytical insights from their SWIFT message traffic.

But we aren't stopping there. Expanding our financial crime compliance services portfolio is one of the three key pillars of our SWIFT 2020 strategy. As such, we are developing three fully-fledged utilities in the areas of Sanctions, KYC and AML.

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 financial crime 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, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

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.

For more information about SWIFT, visit www.swift.com

© SWIFT 2016
57193 - April 2016