White Paper

Meeting the Operational Challenge of Sanctions Compliance

The rapid growth in the number of transactions and watchlists mean that the operational cost of sanctions compliance is doubling every four years

Highlights

- Use of sanctions growing, lists expanding and alerts increasing
- Regulatory scrutiny increasing
- Operational costs and pressure on resources rising
- Need for transaction and list data to be improved
- New testing capability an integral part of compliance ecosystem

Executive Summary

Sanctions compliance within financial institutions is increasingly seen as the front line in the fight against money laundering and terrorist financing. As a result, regulators worldwide have intensified their focus on banks, which need to demonstrate that they have in place adequate and effective measures. Failure to comply risks punitive fines as well as reputational and commercial damage.

This presents a series of challenges to the industry. A consistent global sanctions infrastructure demands robust technology and operations, and the ability to manage imprecise data sets that are growing rapidly and changing almost daily. Banks must also be able to regularly test their processes so that they can "re-prove" the effectiveness of their systems. This was made clear by the Financial Action Task Force in the FATF Recommendations 2012, published in February.

Banks need to better understand their operational environment so that they can keep pace with change, while improving the information carried in each transaction to ease sanctions screening processes. Additionally, list providers must also look to improve the quality of data contained within watchlists so that searches can be more precise and the number of false alerts is reduced.

With banks under pressure to manage their exposure to risk and to reduce costs, having efficient systems and processes in place is critical, as the operational cost of managing alerts could double every 4 years.

Meeting the operational challenge

The sanctions environment: increasingly complex

Sanction screening complexity is a function of a variety of factors, including the number of transactions being processed, the many types of transactions (for example, trade messages compared to payments), the number of watchlists being screened against and the amount of entries on each list.

Sanctions lists themselves are not particularly large, amounting to about 40,000 distinct names and synonyms. However, when you apply possible fuzzy matching to searches (to account for potential misspellings, phonetic similarities, etc.), this generates an equivalent of 4,000,000,000,000 possible names that filters must screen.

- 40,000 names and aliases on lists
- 20% increase in names and aliases in less than a year
- Lists updated virtually every day
- New categories, such as aircraft, are being added

Additional complexity arises from the multi-jurisdictional requirements of sanctions screening and the dynamic nature of lists; there are changes on a daily basis. Lists vary in format, and language variants pose significant transliteration problems. Moreover, which lists must be applied depends on jurisdiction and currency. Different lists require different outcomes and treatment, and have to be managed across multiple systems and locations with varied controls. Equally, filters are complex; their parameters often remain unchanged because banks are uncertain what impact this may have.

- Regulatory focus on banks and the penalty for failure is intensifying
- Failure to comply has cost the industry $2.5 billion in fines in recent years
- The cost of remediation can be up to 15 times the cost of the fine
- Regulatory action also carries reputational and commercial risk

Calibrating such systems is not easy. If a bank generates too few alerts, it runs the risk of missing real matches against sanctions lists and faces harsh penalties. If there are too many alerts, banks risk information overload and must rely on an ever-increasing number of staff to review cases. And the more manual intervention required, the greater the risk of human error. If there are too many alerts for a bank to process, it faces rising latency in the system. This leads to operational slowdown, which could impact on the timeliness of transactions.

Managing this environment in a consistent and effective way that meets regulators' requirements is becoming more and more difficult.

Rising regulatory expectations

We estimate that the number of alerts –and therefore the operational cost– is going to double every four years. Using the compounded annual growth rate (CAGR) of all SWIFT FIN volumes between 2003 and 2011, we know that the number of transactions is growing at 7.5% annually. Similarly, based on the CAGR of the OFAC SDN List between 2010 and 2012, we know that sanctions lists are growing at a rate of 9.6% annually. Because the amount of investigation resources required is in direct proportion to the number of alerts generated, the rise in alerts serves as a proxy for the rise in operational cost (see Figure 1, below).

Additionally, there are market developments such as the migration to a Single European Payment Area (SEPA) that could exacerbate the challenge of sanctions compliance. The final deadline for full SEPA implementation is 2014. By then, the distinction between domestic and international transactions in Europe should have disappeared, but how transactions within SEPA should be treated by banks' compliance processes has not yet been outlined by regulatory bodies.

Many banks are concerned about what screening regime they will need to apply to SEPA formats. Will regulators recognise the SEPA construct and agree that all transactions within SEPA can be treated as domestic? If not, will it be possible for banks operating within SEPA to separate domestic and cross-border payments? Across the industry, it is typically estimated that 2-5% of transactions processed (and screened) by banks are cross-border. If regulators decide that banks must err on the side of caution – screening all SEPA transactions – this would mean a huge additional number of transactions flowing through sanctions filters.

Caution is already leading to the practice of over-screening and tougher internal policies. The punitive regulatory reviews and enforcement actions over the past few years have lead banks to become more risk averse and to apply screening across a broader range of transactions than strictly necessary: better to capture too much than too little. Internal SLAs to put list changes live into production may only be a few hours. This is leading to more alerts and higher fuzzy logic matches, and a heavier burden on compliance infrastructure.

Against this challenging backdrop, regulatory expectations are also continuing to rise. Recent actions by organizations such as the US Treasury's Office of Foreign Assets Control make it clear that institutions need to improve their sanctions controls. Just as importantly, regulators expect banks to monitor their filter's performance. They must be able to continually reaffirm the robustness of their processes through regular, independent tests. This process needs to be transparent and to demonstrate that banks understand the impact of any configuration changes on system performance.

What approach should banks take?

Financial institutions should focus on three areas:

- Improving the quality of information at the source: Banks need to standardize and improve the quality of information contained in transactions. This means searches can be more precise and the quality of alerts generated will be

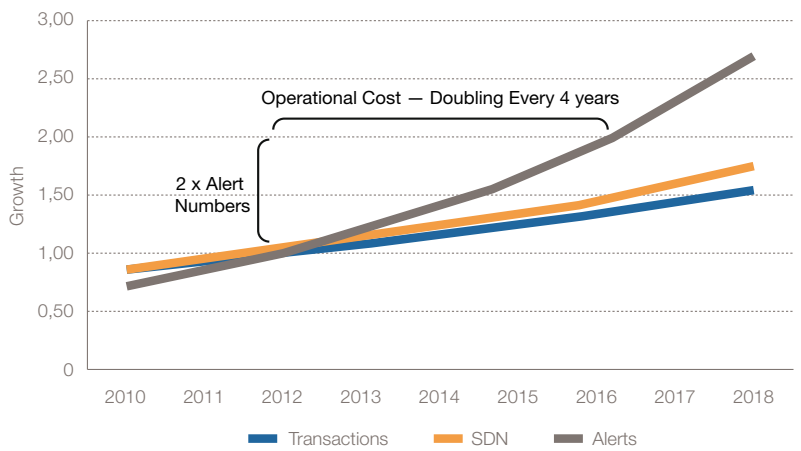

Figure 1: Impact of List and Transaction Volume Growth on Alert Numbers

higher. Regulators, too, need to play their part; the quality of the names on the source list must also be improved to make the screening process more effective.

— Improving understanding of the screening environment: What types of transactions do you process? What is the risk associated with each transaction? How does your filter behave? What optimization rules and settings can you use to improve the searches? How do you get the transparency required to make configuration choices that are aligned to your risk appetite? Knowing the answers to these questions will help banks to build the operational processes to deal with the changing environment.

— Improving the ability to incrementally improve performance: Regular testing will enable banks to characterize filter performance, to progressively improve system performance, and to prove to regulators that their systems and processes are fit-for-purpose and agile enough to manage a constantly evolving environment.

A new testing environment

Banks need to test systems in order to measure the effectiveness, coverage and efficiency of their sanctions filter. Whilst periodic audits offer a valid, point-in-time view of sanctions processes, the ability to be able to self-test on a regular basis gives banks greater control over the compliance environment and improves transparency of the compliance process. Self-testing means banks can iteratively improve their systems more easily and can measure the impact of changes before they make them.

Effectiveness

Banks must ensure that systems are effective to protect the reputation of the institution and avoid the regulatory and commercial impact of fines and bad publicity. Banks need to understand the 'baseline' performance of their systems and the factors that will impact this baseline performance positively or negatively. It may be unreasonable to expect systems to be 100% effective given the imprecise nature of many of the names on watchlists, but banks need to know the percentage of sanctioned entities that their systems are able to detect and ensure that processes are calibrated to fit their tolerance for error.

Coverage

Banks must ensure that systems provide the scope and coverage required to ensure regulatory policy is appropriately implemented. This is highly challenging in a multi-jurisdictional, multi-list environment. Regular testing will make sure that filters are screening what they should be and that processes are consistent with policy.

Efficiency

Banks need to improve the efficiency of filters to ensure that the cost of compliance does not overwhelm the business. Can the case be made for creating a centralized, standardized platform? Can watchlists be consolidated? Regular tests will help to answer these questions. Banks need to put in place a system that measures efficiency and gives banks the tools to make incremental changes to improve efficiency over time.

A successful sanctions compliance infrastructure needs:

— Regular, systematic, automated assessment of filter performance to ensure that systems are working and provide appropriate coverage. Processes must ensure timely response to list changes, assurance of operation, and an assessment of the impact of changes

— The tools to enable progressive improvement of the effectiveness of filters, incremental improvement of filter performance, identification of the sources of false positives

— The ability to encode group compliance policy as part of tests. These must incorporate the bank's business tolerance for error to ensure controls are audited and recorded, and to provide evidence for regulators

SWIFT is the financial messaging provider for more than 10,000 financial institutions and corporations in 212 countries and territories. It partners with Omnicision to deliver its Sanctions Testing service, an application that integrates the testing and tuning of sanctions filters to help banks operate a more effective and efficient sanctions environment.

Earlier this year, SWIFT launched a Sanctions Screening service, which screens messages in real time against public sanctions lists that are centrally managed.

For more information, please contact sanctions.testing@swift.com or your local SWIFT account manager.

00000 - OCT 2012