# Effective sanctions list management

## a seven-step guide

By **Nicolas Stuckens**
Head of Sanctions Compliance Services at SWIFT

For compliance professionals on the front line of managing sanctions lists and updating sanctions filters, the challenges associated with constantly changing lists and inconsistencies in data format and structure will not be unfamiliar.

In an increasingly complex sanctions environment, how can financial institutions ensure effective compliance without impacting efficiency and cost?

First of all, firms must choose between appointing a dedicated team of people to source and manage their lists – an approach which brings considerable overheads – or appointing a 'one-stop shop' vendor to deliver the complete file each day.

Choosing a sanctions list provider is an important task, as the institution will rely on the data provided to flag up target names while minimising false positives.

At the same time, switching between providers can be both costly and inconvenient. It is therefore important that financial institutions spend some time understanding the differences between the lists available, as well as the possible pitfalls, before coming to a decision.

When weighing up the available options, financial institutions should therefore take into account a number of different factors, from the benefits of enrichment to the hidden costs of poor or badly formatted data.

By following these seven steps, institutions will quickly reap the benefits of better sanctions list management.

1

## Seek out the services of a third-party list provider

Why should an institution use a third-party provider instead of simply sourcing data from the relevant regulators? Going directly to the regulatory sources might seem like the most obvious choice: after all, this is where the data originates. In practice, however, downloading lists from regulatory websites can be an unwieldy task which involves accessing information from multiple sources and in various different formats.

Even once it has been collated, data accessed directly from regulatory sources may be poorly structured or may not be in a useable format, making it necessary for banks to enter data manually. It is also worth noting that if banks access data directly from the regulatory source, they will not benefit from any support.

Third-party list providers, in contrast, put everything together in one place and in a single format, providing consistency and convenience, as well as offering support – all of which can provide advantages over using regulatory sources. They may also enrich list data with missing information such as BICs to support the screening process.

However, institutions should also be aware of some other considerations. For one thing, banks need assurance that the aggregator has picked up all of the relevant data and represented it in the same way as the individual source. Banks also need to ascertain that their chosen provider is a good fit for the bank's own risk appetite.

It is also worth noting that while putting everything together in one place can be seen as an advantage, it takes time for vendors to do this – particularly when the file is enriched. It is therefore not unusual for vendors to take over 24 hours to make a file available to an institution: a speed to market which some institutions may find problematic.

2

## Understand the hidden costs of poor list data

Suboptimal list data can result in a number of hidden costs. Take false positives, for example. A significant number of false positives may result from vendors either adding additional (and sometimes unnecessary) entities and aliases, or failing to remove previously deleted entities.

When source data is not well-structured, such as when all elements of a given name are grouped together rather than separated into individual parts, the number of false positives increases as well. The higher the number of false positives, the greater the number of staff required to handle them.

On the other hand, different vendors have different 'editorial policies': some may remove certain information to reduce the number of false positives. While this might reduce the workload for their customers, there is a risk that organisations using those lists will fail to catch certain names.

All too often, businesses focus on budget-related costs while overlooking the costs involved in time wastage. Where lists are concerned, financial institutions may simply assume that dealing with list

data takes a certain amount of time. But if organisations can avoid time being wasted as a result of poor list data, they may be able to redeploy people's time more effectively, for example by training them as fraud or AML investigators.

3

## Guarantee your list provider is selling you good quality data

The only way to determine this is by running a full comparison of the vendor's list against the regulatory list. Some vendors provide point in time assurance reports to customers to demonstrate process quality.

That said, it is important to note that even regulatory lists, in an attempt to aid institutions in their screening, can contain imperfectly structured data. For example, a target name as provided by the regulator may include additional 'metadata', such as country names or location as part of the main name.

Some vendors address this issue by moving the location metadata into a different field, which can have the advantage of reducing false positives and thereby reducing the institution's costs and the headcount required for the task.

While this may help to eliminate false positives, there is also a risk that a like-for-like comparison with the regulatory source may lead to the belief that a few names are missing because the filter is, for example, looking for a combination of six words instead of three.

4

## Compare different lists from different providers

Institutions can compare and contrast different vendors' lists by running their files against a particular data set and analysing the results. This process requires skilled investigators to assess the difference in hits between the two lists, to assess the quality of the potential matches and determine whether or not the list is in accordance with the risk appetite of the institution.

SWIFT's Sanctions Testing tool can also assist with this process. While this exercise requires time and effort, it is the most effective way of discovering which list is most suitable for the organisation's requirements.

5

## Understand the difference between enhanced and standardised list data

A lot of list issuers provide an XML file with standardised data. Advanced XML files tend to have data which is categorised more effectively and which appears in more suitable field structures to aid screening. There is also a difference when it comes to file size: advanced XML files are bigger than standard XML files because advanced XML contains more fields.

While authorities such as OFAC and the United Nations as well as some leading data vendors provide advanced XML list les, filter vendors have been slower to leverage these more granular data sets to deliver enhanced screening effectiveness and efficiency. However, if the bank's filter is capable of taking the advanced XML file, this is likely to be the preferable option.

6

## Make sure your lists are fit for purpose

'Fit for purpose' can encompass a number of different elements, such as the degree of enrichment to a file accepted – or required – by the institution.

It is not unknown for vendors to include many variations of a name spelling, over and above those provided by the regulatory list issuer. This can, in turn, generate a large number of false positive hits compared to the standard list.

In order to ascertain whether lists are fit for purpose, institutions should have a policy which includes a risk appetite statement setting out the organisation's requirements for sanctions screening. This statement, as applied to list vendors, may include such considerations as which enrichments the vendor provides, the number of fields the data is broken down into, the scope of lists the vendor is able to provide, and the vendor's proposed list update schedule, to name a few. Ultimately, institutions should conduct tests and analyse the results to see whether the expected alerts are generated.

7

## Weigh up the pros and cons of enrichment

Enrichment is something that vendors do in order to make files more useable and more detectable for names. As such, it is often used as a point of differentiation by list providers. Enrichment can come in different forms: it might involve taking elements of a standard file and putting them into the vendor's own data model in order to improve screening. Enrichment may also mean adding elements to the file to aid the detection of sanctioned identities, such as a BIC.

It is also worth noting that a single vendor may offer a number of different products, so it is important to choose the product which is the best fit for the relevant business problem.

The risk is that banks may buy a product which has irrelevant data which increases operational cost without adding any value. It is also worth noting that some types of enrichment may result in significantly more hits, so may not necessarily benefit the organisation. Again, the easiest way of finding out whether or not enrichments are beneficial is to test the relevant data set against different providers' lists.

## Conclusion

Third-party list providers can offer considerable advantages over sourcing lists directly from regulators. That said, it is important to be aware of the variety of different products and approaches taken by different providers.

Even if a third-party provider can relieve an organisation of a number of cumbersome tasks, they will never cover the full scope of list activities that a firm must go through. For example, banks will still conduct regular impact testing on new list updates ahead of promoting the new entries to their production system. But the time and effort saved can be best invested in developing list expertise that is crucial to support the effectiveness and efficiency of sanctions screening.

Institutions should take the time to understand the types of list available – and the pros and cons of each – in order to obtain data which is fit for purpose and which maximises the effectiveness and efficiency of the institution's sanctions screening activities.

Finally, institutions will want to choose a vendor that works closely with its customers to ensure that its products keep abreast of changing regulatory requirements, and that is committed to providing flexible list data sets adapted to each customer's specific risk appetite and system capabilities.

## How SWIFT can help protect your business

| | |
|---|---|
| Transaction screening | **SWIFT Sanctions Screening**<br>Screen message traffic against the latest sanctions lists and manage alerts using our secure, hosted, cost-effective platform. |
| Customer screening | **SWIFT Name Screening**<br>Screen entire databases and single names against sanctions, PEP, RCA and private lists using a secure hosted platform. |
| Test your screening controls | **SWIFT Sanctions Testing**<br>Test filters and lists and get independent performance assurance for smarter, more effective sanctions, PEP and client screening. |
| Detect and prevent fraudulent transactions | **SWIFT Payment Controls**<br>Stop fraud in its tracks and support transparency with unique, in-network alerting and reporting capabilities. |