



Information paper

**Transaction filtering,  
systems testing and  
annual certification:  
driving business  
benefits**

## Introduction

The new DFS anti-terrorism transaction monitoring and filtering programme regulation has significant implications – but it also brings some interesting opportunities.

Banks operating in New York State will soon be required to comply with new regulations which require them to test, ensure and certify that their transaction monitoring and filtering programmes are operating effectively.

While many banks are already largely compliant with these requirements, others will need to amend their processes in order to comply with the new rules. This paper outlines the implications of the new rules – and why banks can view the changes as an opportunity, rather than a burden.

Simply focusing on the new rules as a tick-box compliance exercise could result in higher costs. On the other hand, the regulation provides financial institutions with an opportunity to develop an ongoing programme of review that improves systems and processes, increases their effectiveness and creates business efficiencies.

## Overview of the changes

On 30 June 2016, the New York Department of Financial Services (DFS) – which supervises financial institutions and insurance companies – [announced the adoption of a risk-based anti-terrorism and anti-money laundering regulation](#).

### The new regulation has four main components. Banks need to:

- Maintain an appropriate transaction monitoring programme
- Maintain a watch list filtering programme
- Perform tests and ongoing analysis to ensure that systems are working correctly
- Submit an annual board resolution or senior officer compliance finding stating that the bank's transaction monitoring and filtering programmes comply with the regulation.

While the regulation specifically applies to financial institutions operating in New York State, it has implications for banks headquartered in other markets. The new rules could also indicate the direction which other regulators may take in the future.

Although the first board resolutions or compliance findings are not due until 15 April 2018, the regulation comes into effect on 1 January 2017. As such, banks will need to act now in order to make sure they are compliant as from that date.

In order to meet the DFS certification requirements, banks will need to have appropriate testing and validation procedures in place for their transaction monitoring and watch list filtering programmes. Watch list filtering can refer to screening of transactions against public sanctions lists, as well as screening customers against sanctions and politically exposed persons (PEP) lists.

Testing and validation are key to an effective sanctions compliance process, providing assurance that the bank's key processes and controls are aligned to the relevant risks and the bank's risk appetite. They provide assurance that internal processes are being completed correctly, and that any weaknesses are promptly identified and remedied.

In some cases, global banks delegate authority for testing and validation from the head office prime control function to local money laundering reporting officers (MLROs) or country heads.

### The local money laundering reporting officer or country heads will be responsible for the following:

---

Appropriate arrangements must be in place for the regular testing of internal processes and controls.

---

The processes may include internal quality assurance testing, as well as thematic reviews by teams such as group compliance or risk functions.

---

These must take place often enough to provide the required level of assurance and manage risks in a timely manner.

---

A breach reporting system must be established to record breaches of internal procedures, as well as those involving a breach of legal requirements.

---

A programme must be in place for reviewing the depth, quality and consistency of investigations and decision-making on name matches.

---

Any weaknesses identified must be remediated without delay.

---

Independent assurance of the overall sanctions control environment will be periodically sought via group audit.

## Understanding and evidence

Although banks have long been expected to maintain transaction monitoring and watch list filtering programmes, the new regulation taps into two regulatory themes which are becoming increasingly important.

The first is about understanding how controls work and being able to demonstrate that they work correctly. The second is about senior management taking personal responsibility for the bank's systems and processes.

Many compliance systems are 'black-boxes', leaving institutions with the challenge of understanding how they operate and how parameter settings can be used to conduct maintenance and tuning over time.

In recent years, however, US regulators have begun to stipulate that financial institutions have to understand how their systems and controls actually operate. This theme also features in other jurisdictions and in the European Union's Fourth Anti-Money Laundering Directive.

In this context, banks need to know what settings are being used for their transaction, customer and PEP screening filters, and whether these are appropriate for the outcome they seek to achieve.

They will also need to test that their filters are operating correctly, and regularly tune their filters to keep pace with evolving sanctions lists and related requirements.

It also includes understanding the limits of a system and whether suitable controls are in place to mitigate those limits. For example, if a filter is not enabled to catch short single names, are there other controls in place to mitigate any associated risk?

### Demonstrating compliance

In the US – and globally – regulators regularly examine the quality and effectiveness of banks' compliance systems and processes. The concept of annual certification takes this one step further: banks are required to demonstrate that internal audits and independent testing are being carried out on a regular basis – and that senior management certifies that their transaction monitoring and filtering programmes comply with the regulation.

In order to make this certification, senior management first needs evidence of compliance. This evidence is itself the cornerstone to being able to make and assess incremental improvements to performance.

Again, regulators are increasingly focusing on the need for specific individuals within banks to take personal accountability for regulatory compliance. In the UK, for example, the Senior Managers Regime stipulates that senior directors of banks could be personally taken to court and held liable if controls are not adequate.

### Filter testing and validation should aim to answer questions such as the following:

- Does the system detect names which appear on the relevant sanctions lists?
- Do the system settings match the institution's compliance and risk policies and procedures?
- Are the relevant data sources (such as sanctions lists) and flows identified correctly? Are data sources accurate and complete?
- Does the system include appropriate fuzzy matching? In other words, are spelling variations, typing errors and intentional changes to obfuscate names identified?

### Tips for effective testing

When testing their AML and sanctions systems, banks should ask the following questions:

#### Is the testing process independent?

Testing should be carried out independently (by a separate internal team, or an external provider) and to the level and satisfaction of senior management.

#### Does the process support continuous testing?

Testing should be embedded in an ongoing programme of activity to ensure a continuous approach.

#### Is the process repeatable?

Automated tools can minimise human error and provide repeatability.

#### Is the process comprehensive?

Banks should test all items on the relevant sanctions lists, not just a small sample.

#### Does it provide insights which can drive improvements?

Testing should provide insights and understanding leading to incremental effectiveness and efficiency improvements.

#### Does it support peer comparisons?

Users should be able to assess how effectively their systems are performing compared to their peers' systems.

#### Does it provide the necessary evidence?

Testing should provide reporting that can be provided to senior management and overseers as evidence.

## Implications for banks

The implications of the new DFS rules are considerable. As well as requiring greater transparency over AML and filtering systems, the regulation will result in greater downward pressure from senior management for banks to test their systems more rigorously and more regularly. Meanwhile, senior managers may look for industry comparisons in order to increase their own understanding and make sure they are aligned with their peers.

While the new regulation applies to banks operating in New York State, in practice this includes branches of all large global financial institutions, as well as many mid-sized and smaller US banks. Some banks will already have some kind of programme of work in place to undertake testing and validation. For institutions without such controls in place, however, a lot more work may be needed.

The cost of complying with the regulation may also be greater for smaller firms which do not have existing expert teams. Financial institutions should take the time to test their existing systems to have evidence needed for further action. This creates the right environment for tuning and improvement plans if required and provides evidence to make the correct decisions on system upgrade or replacement.

With the right tools in place, banks can perform independent testing in-house, cost effectively and on a repeatable basis. Meanwhile, the new regulation affects the international banking community – and as such, a community approach is needed in response. Industry-defined standards, collaborative services and community-inspired solutions are needed to meet these complex challenges.

### Sanctions Testing

Banks can use SWIFT's Sanctions Testing product to test, fine tune and understand their sanctions filters and list data. Unlike tests which focus only on a subset of data, Sanctions Testing takes a comprehensive approach to assurance and coverage testing by incorporating every dimension of the relevant messages.

This gives greater confidence that all necessary data has been looked at. Sanctions Testing measures effectiveness by building a multi-dimensional performance footprint of the filter. This is done using test cases constructed from dozens of name variation algorithms, designed to measure the breadth and depth of the filter's fuzzy matching capability.

Each variation reveals a characteristic of the filter's behaviour, which identifies the filter's strengths and weaknesses.

This performance footprint methodology has been developed through industry consultation and best practice over a number of years and is continually evolving based on feedback from users. It provides objective measurements that can be mapped to each institution's risk appetite to provide evidence of compliance with policy. Sanctions Testing also helps banks understand the performance of their filters in relation to industry norms, enabling them to undertake targeted tuning and remediation activities as part of a continuous improvement programme. It allows for regular filter testing and tuning, with many institutions using it to perform (automated) testing each time sanctions lists change.

The detailed understanding of filter performance provided by Sanctions Testing enables banks to improve filter efficiency by identifying ways to reduce false positives, and establishes a baseline from which to measure the impact of subsequent tuning iterations on the institution's risk appetite. Detailed reporting demonstrates the impact of changes to filter settings and enables banks to document filter performance to management and overseers.

As such, Sanctions Testing gives banks the confidence needed to certify compliance with Section 504.3 of the new DFS regulation.

## Beyond compliance

By putting proper processes in place, banks can not only comply with the new rules, but may also be able to use their systems more effectively.

The additional controls needed under the new regulation may make banks more aware of what their systems can actually do. In practical terms, banks may be able to tune their systems more effectively. Banks may also be able to reduce the number of false positives or erroneous alerts coming out of their AML and filtering systems, leading to more efficient and effective processes.

As well as understanding their systems more clearly, banks will need to document how their systems work. This could have the effect of strengthening banks' overall compliance regimes, leading to greater confidence when undergoing regulatory examinations.

### Regular reviews

While the certification element of the new rules is an annual requirement, compliance controls may need to be reviewed more often than once a year. Issues can arise during the course of a year. If these are not identified promptly, banks may not have time to address the issues before they need to re-certify their compliance.

Many financial institutions already choose to undergo testing on a monthly basis or even weekly basis. Rather than creating more work, this can enable banks to catch and fix issues straight away, avoiding the costs and time burden which can arise when a backlog of issues occurs.

### Annual certification

Banks may also be able to derive business benefits from the new requirements. If testing and certification is viewed solely from an audit perspective, meeting the requirements will be a sunk cost: the exercise will provide no additional benefit, while creating a time-consuming annual programme of work.

A better approach may be to regard the new DFS rules as a business opportunity.

This could involve combining the audit with a review cycle which looks at certification requirements together with operational and process efficiencies.

Banks which take this approach may be able to drive efficiency while auditing, strengthening and improving controls. This could lead to greater system transparency, better compliance outcomes and justifiable operational efficiencies which may lead to lower operational costs.

## Act now

With the new DFS rules finalised, banks will need to begin the compliance process promptly.



Although the first board resolutions and compliance findings are not due until 2018, these will relate to the previous year – so banks will need to have everything in place by early 2017.

## SWIFT products

The following SWIFT products can help banks to comply with the new DFS requirements:

### Sanctions Testing

Banks can use SWIFT's Sanctions Testing service to test, fine tune and understand their sanctions filters. As such, Sanctions Testing gives banks the confidence needed to certify compliance with Section 504.3 of the new regulation.

### Sanctions Screening

Sanctions Screening, SWIFT's transaction screening solution, combines a best-in-class filter with a comprehensive database of sanctions lists which is updated automatically. Sanction Screening is tested using Sanctions Testing, giving banks additional transparency as well as the benefits of high-quality assessment reporting.

### Payments Data Quality

Using SWIFT's new Payments Data Quality service, banks can validate that the originator and beneficiary information in their payments messages is correct. As well as helping with straight-through processing, this also increases the efficiency of the filter.

## Conclusion

Complying with any new regulation takes time and resources.

However, the new DFS rules should not be approached simply as a costly compliance exercise. By taking the time to understand the opportunities, banks may be able to improve the effectiveness of their existing systems and processes.

This, in turn, may lead to business efficiencies and, where justifiable, a reduction in operational costs.

Banks should also be aware that they will need to address the new rules promptly in order to meet the compliance deadlines. Independent experts such as SWIFT may be able to provide support during this exercise.

For information on how SWIFT can help, please contact [Sanctions.Testing@swift.com](mailto:Sanctions.Testing@swift.com).



### **About SWIFT**

For more than 40 years, SWIFT has helped the industry address many of its biggest challenges. As a global member-owned cooperative and the world's leading provider of secure financial messaging services, we enable more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, relentlessly pursue operational excellence, and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. We also bring the financial community together to work collaboratively to shape market practice, define standards and debate issues of mutual interest.

SWIFT users face unprecedented pressure to comply with regulatory obligations, particularly in relation to the detection and prevention of financial crime. In response, we have developed community-based solutions that address effectiveness and efficiency and reduce the effort and cost of compliance activities. Our Compliance Services unit manages a growing portfolio of financial crime compliance services in the areas of Sanctions, KYC and CTF/AML.

Financial crime compliance is also a major theme at Sibos, the world's premier financial services event, organised by SWIFT for the financial industry.

[www.swift.com/complianceservices](http://www.swift.com/complianceservices)