Guernsey Financial Services Commission

Sanctions

Thematic Review - 2021

Published: 11 May 2022

Executive Summary

During 2021 the Commission undertook a thematic review to assess the effectiveness of banks', fiduciaries' and fund administrators' monitoring of, and compliance with, targeted financial sanctions. The field work undertaken clearly predates the Russo-Ukrainian War and thus has not assessed the hard work firms have put in to robustly implement sanctions on Russia since the middle of February.

A sanction is a measure imposed by a government to apply restrictive measures against a country, regime, individual, entity, industry or type of activity believed to be violating international law. Sanctions are imposed as a result of United Nations Security Council Resolutions aimed at preventing the proliferation of weapons of mass destruction (nuclear, biological and chemical) and disrupting terrorist operations. Sanctions are also used to satisfy United Kingdom foreign and national security goals, such as the unprecedented number of sanctions imposed on Russian individuals and organisations, following the invasion of Ukraine. The Bailiwick's sanctions regime mirrors that of the United Kingdom and it is imperative that sanction targets' funds, assets or other economic resources are immediately frozen and reported to the States of Guernsey's Policy and Resources Committee.

86% of all Bailiwick firms subject to AML/CFT supervision[1] place reliance on automated sanctions screening systems to identify sanction targets. However, firms should be alive to the risk of placing over reliance on these systems and accept that the process is often complex, with many different systems, databases and staff interacting with one another in order to generate alerts of potential sanctions matches.

The effectiveness testing was extensive and those subject to our testing were responsible for over 260,000 business relationships with the banks tested responsible for 99.8% of inward transactions and 99.6% of outward transactions in/out of the Bailiwick during 2021[2]. The results showed that the sanctions screening systems of those tested were effective, with only a small minority of firms in need of material improvements to demonstrate that their systems are effective. These firms are now subject to risk mitigation programmes set by the Commission.

We noted many examples of good practice and it was encouraging to note the strong performance by banks in the effectiveness testing, particularly the main clearers. This is mainly as a result of outsourcing to Group centres of excellence and the significant attention given to sanctions by the large banking groups operating in the Bailiwick. However, the Commission is aware of previous failures with automated systems and therefore local firms need to

[1] *According to data collected through the Commission's annual Financial Crime Risk Return*
[2] *According to data collected through the Commission's quarterly Financial Flows Return*

ensure they consider and document their sanctions risks, the screening process, and the testing of the effectiveness of the sanctions screening systems employed.

Moreover, only 56% of the fiduciary and investment firms surveyed screen underlying assets and of those firms which are screening underlying assets, some are only doing so on vessels despite these not being the only asset types of relevance. Therefore, 44% of these firms may be at risk of breaching sanctions, although we have been impressed with the efforts firms have put into Russian sanctions implementation since the Russo-Ukrainian War broke out.

Effective sanctions screening is only one part of a firm managing its TF and PF risks, firms also need to understand what TF and PF threats their business is exposed to, and instil adequate controls in respect of: (i) the identification and verification of customers, and their ultimate beneficial owner(s), (ii) understand where their customers' source of funds and wealth originate from and (iii) perform ongoing monitoring of transactions and activity, to mitigate these risks fully.

We wish to thank the 175 firms which participated in the thematic review through completing the thematic questionnaire, and additionally those firms which participated in the effectiveness testing and onsite inspections.

Whilst this thematic review did not capture all sectors, all firms are obligated to manage sanctions risk and we hope that this report will also be of interest to firms in every sector as they are under the same obligations in respect of sanctions screening. Furthermore, given that sanctions compliance transcends our Handbook requirements, sanctions risk is also pertinent to those writing general insurance, for example the marine general insurance sector through its risk of breaching PF related sanctions[3] or the kidnap and ransom insurance sector through its risk of breaching TF related sanctions[4], and as such this thematic review will also be relevant.

The Commission will consider how firms have incorporated the findings from this report as part of its ongoing supervision in addition to the exceptional work it has been undertaking with firms to ensure the thorough implementation of the sanctions on Russia.

Nick Herquin

Deputy Director

11 May 2022

[3] *UK National Risk Assessment of Proliferation Financing - September 2021*

[4] *Bailiwick of Guernsey 2019 National Risk Assessment Report on ML and TF - Jan 2020*

Summary of areas for improvement

Screening of underlying assets *(page 13)*	**Issue:** we found that only 56% of the fiduciary / investment firms surveyed are screening underlying assets.
	Action: consider whether those underlying assets (including subsidiaries) could be subject to sanctions and document what mitigation is appropriate.
Efficiency & Effectiveness *(page 17)*	**Issue:** we found some firms focussed more on the efficiency than the effectiveness of their automated screening systems.
	Action: be aware of the risk of over tuning the system to make it more efficient to reduce resource drain, but in turn missing sanctions targets.
Understanding & mitigating sanctions risk *(page 18)*	**Issue:** we found that only a few firms were able to provide details of how their customers and products and services were exposed to sanctions.
	Action: assess the sanctions risk of your customers, products and services and determine the appropriate mitigation.
Screening policies & procedures *(page 19)*	**Issue:** we found some firms' screening policies and procedures were lacking in basic details such as why a screening method is used and who was responsible.
	Action: document the fundamentals of the process (including the thresholds/settings to be used).
Understanding systems *(page 20)*	**Issue:** we found some firms had a limited understanding of how the customer data and sanctions screening systems interacted.
	Action: ensure that the sanctions screening systems (including the flow of data between the customer and screening systems) are understood and correctly configured.
Outsourced functions *(page 21)*	**Issue:** we found some instances of heavy reliance on Group or external vendors and varying degrees of understanding locally of who was responsible for the screening systems within a Group.
	Action: obtain sufficient evidence to be assured that outsourced systems are working effectively. Maintain documentation which clearly sets out who is responsible for the sceening systems within a Group and maintain access to that function.
Compliance Monitoring *(page 22)*	**Issue:** we found that some of the compliance testing was not sufficiently robust.
	Action: ensure that tests are checking that the system is appropriately generating alerts and that the correct customer data is being screened.

Glossary of Terms

AML/CFT – Anti-Money Laundering and Countering the Financing of Terrorism

Bailiwick – Bailiwick of Guernsey

BIC – Bank Identification Code

Board – Board of directors (or the senior management where it is not a body corporate)

CDD – Customer Due Diligence

CMP – Compliance Monitoring Programme

Commission – Guernsey Financial Services Commission

EU – European Union

FATF – Financial Action Task Force

FCRR – Commission's annual Financial Crime Risk Return

Firm – A financial services or prescribed business subject to the requirements of Schedule 3 and the Handbook

Handbook – The Handbook on Countering Financial Crime and Terrorist Financing

ML – Money Laundering

NRA – National Risk Assessment of ML and TF

OFAC – US Office of Foreign Asset Control

OFSI – UK Office of Financial Sanctions Implementation

P & R Committee – The States of Guernsey's Policy and Resources Committee

PEP – Politically Exposed Person

PF – Proliferation Financing

SWIFT – Society for Worldwide Interbank Financial Telecommunications

Schedule 3 – Schedule 3 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999

TF – Financing of Terrorism

UK – United Kingdom

UN – United Nations

UNSCR – United Nations Security Council Resolution(s)

Contents

Section 1: Background

1.1 The Bailiwick's sanctions regime

A sanction is a measure imposed by a government to apply restrictive measures against a country, regime, individual, entity, industry or type of activity believed to be violating international law and could include:

(a) the freezing of funds;
(b) the withdrawal of financial services;
(c) a ban or restriction on trade or travel; or
(d) suspension from international organisations.

The ultimate objective of a sanction varies according to the situation. Sanctions may also be aimed at preventing the proliferation of weapons of mass destruction, disrupting terrorist operations, or trying to change the policies and actions of the target in accordance with UNSCRs. Sanctions are also used to satisfy foreign and national security goals.

The Bailiwick has enacted numerous pieces of legislation which implement sanctions measures. This is the responsibility of the P & R Committee and this legislation transcends the rules and guidance in the Handbook. The P & R Committee administers the Bailiwick's sanctions regime however the Commission has responsibility for the supervision of firms' controls in this respect. Chapter 12 of the Handbook contains rules requiring firms to have in place:

- *Appropriate and effective policies, procedures and controls to identify, in a timely manner, whether a prospective or existing customer, or any beneficial owner, key principal or other connected party, is the subject of a sanction issued by the UN, UK or the States of Guernsey's Policy and Resources Committee*;

- *A system and/or control to detect and block transactions connected with those natural persons, legal persons and legal arrangements designated by the Bailiwick's sanctions regime*; and

- *Compliance monitoring arrangements which include an assessment of the effectiveness of the firm's sanctions controls and their compliance with the Bailiwick's sanctions regime*.

1.2 Rationale for the thematic review

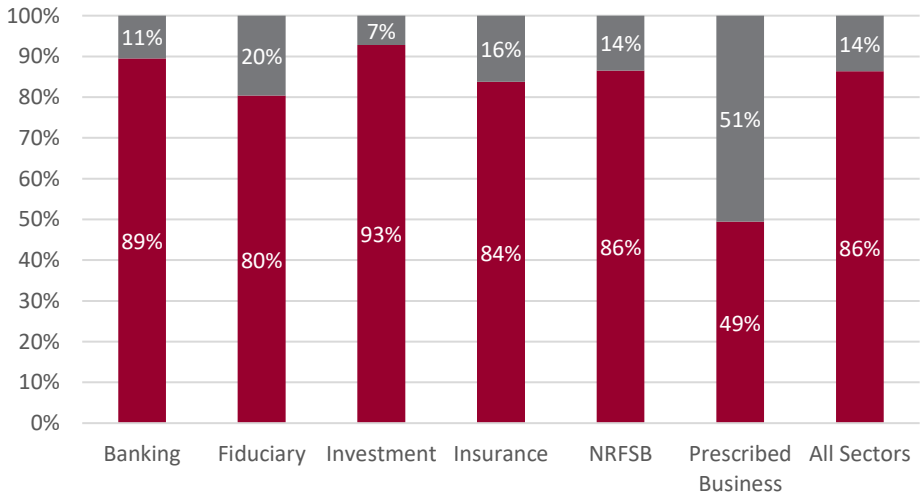
We undertook this thematic review because there have been occasions when screening processes have failed and because sanctions compliance has become more complex and failure costly. In recent years a range of issues have been reported to the Commission by firms regarding failures in their sanctions screening processes, including:

- certain types of customers not being subject to screening;
- outdated data being used in the screening process;
- incoming SWIFT payments not being screened due to being in an incorrect format; and
- insufficient systems access granted to the external screening tool provider.

The Commission imposed risk mitigation programmes on these firms requiring them at a minimum to resolve the problem and, where relevant, to re-screen customers, beneficial owners and/or third parties. The Commission observed that in a number of these cases there was a disconnect between the firm's Board, compliance and IT functions in respect of the expectations each had of the other regarding the effective operation of the sanctions screening systems and related processes. All firms should be alive to the risk of placing over reliance on these systems, as the actual mechanics are often complex, using more than one system and database. It is crucial that staff from the different functions interact with one another in order to minimise the risk of screening failures.

The 2021 FCRR data collected by the Commission indicated that 86% of Bailiwick firms supervised for AML/CFT are now using automated systems to screen their customers, up from 82% in 2020. The process for screening within an automated system can be technical in nature, and bring about various operational and governance challenges, however their use provides a number of advantages, not least efficiency and cost-effectiveness.

Proportion of firms using automated screening systems



The prescribed business sector includes a significant proportion of small firms and typically operates on a one-off basis for a customer (rather than maintaining ongoing business relationships) thus the lower prevalence of automated screening systems. The fiduciaries which are not utilising automated screening systems were typically those with smaller customer bases and/or advised that screening was undertaken upon trigger events such as when updates to relevant sanctions lists are issued. However, during crises (such as the Russo-Ukrainian war) there could be large volumes of new or amended designations being made by sanctions authorities within a short period of time. Firms which are not utilising automated screening systems may face a significant operational challenge in respect of screening a large volume of new designations in a timely manner and in turn risk breaching sanctions.

That is not to say that automated screening systems do not face similar challenges during such periods, as the designations being made may cause a large number of alerts to be generated by the automated systems which require manual intervention to investigate and resolve. Furthermore, firms relying on automated systems should be cognisant of the length of time it takes for external providers to update designations and for these to be incorporated into firms' systems. Consequently, firms may have to install interim measures to mitigate sanctions risks.

Sanctions compliance is becoming increasingly important and complex as countries impose and enforce more sanctions, such as those imposed recently on Russian individuals and organisations following the invasion of Ukraine. The UK, through OFSI, has also been taking a tougher approach as evidenced by its £20.47m fine in 2020[5] on Standard Chartered Bank in relation to breaches of sanctions against persons who threatened Ukraine's sovereignty. The US frequently imposes sanctions to satisfy US foreign and national security goals and, whilst OFAC sanctions are not directly enforceable in the Bailiwick, the reach of OFAC sanctions is extensive as they capture any person trading in US Dollars. Given the increasing media attention regarding sanctions, there could be severe reputational damage to both firms and the Bailiwick as a result of sanctions breaches.

1.3 Purpose of the thematic review

The primary aim of the thematic review was to assess the effectiveness of firms' monitoring of, and compliance with, targeted financial sanctions for both TF and PF by:

1) assessing the frequency and scope of screening;
2) assessing the effectiveness of automated screening systems; and
3) assessing the extent to which Boards have oversight of the effectiveness of their sanctions screening systems.

[5] *OFSI - Imposition of Monetary Penalty - Standard Chartered Bank*

1.4 Scope of the thematic review

The thematic review assessed those sectors which are considered to pose the highest risk of ML and TF in line with the Bailiwick's NRA: the banking and fiduciary sectors; however it also encompassed all designated administrators of collective investment schemes and several insurers. Where appropriate, our analysis is split by sector. The thematic review was divided into three phases as follows:

Phase 1 – Thematic questionnaire

A questionnaire was issued to 175 firms, which encompassed all licensed banks, fiduciaries, designated administrators and a number of insurance firms, and sought details regarding their sanctions screening processes.

Phase 2 – Onsite inspections

Onsite inspections were undertaken to 21 firms across the sectors above, with a weighting towards banks due to their pivotal role in facilitating money transfers in and out of the Bailiwick. We gathered Board minutes, policies and procedures, and details of any testing undertaken in relation to sanctions screening. The onsite inspections comprised a meeting with representatives of the firms to discuss their sanctions governance, risk and compliance arrangements.

Phase 3 – Effectiveness testing

All firms which were selected for onsite inspections also participated in effectiveness testing in order for a more rounded assessment to be made of firms' sanctions screening processes. This testing was undertaken during a 48-hour window between 14 and 16 June 2021, in conjunction with a specialist third party, which has been used by a number of financial services regulators across the globe, to undertake testing of sanctions screening and transaction monitoring systems employed by regulated firms. Both the customer screening test and the transaction screening for the firms selected comprised 10,100 names of individuals and entities recorded in publicly available sanctions lists published by the UN, OFAC, EU and OFSI.

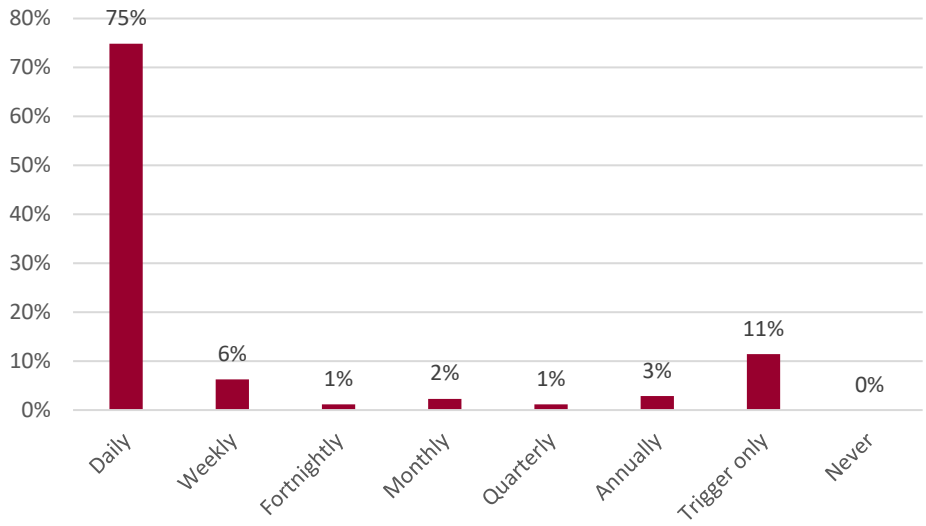
Section 2: Frequency and Scope of Screening

2.1 Frequency of screening customers

Naturally firms and their customers will have varying degrees of sanctions risk dependent on the nature of their customers and the frequency on which firms screen their customers should reflect their own unique level of risk. Screening frequencies set by vendors and/or Group may not be appropriate for the firm's risk profile. For example, there are certain situations where there will be a much lower risk of breaching sanctions such as the provision of a bank account to a natural person resident in the Bailiwick with no other high ML/TF risk indicators. The screening of such a customer may not need to be as frequent as a customer which is a complex legal person, holding multiple assets across the globe, and/or with politically exposed beneficial owners in jurisdictions with active sanctions regimes in place. In these latter scenarios, it would be appropriate to screen on a more frequent basis.

The thematic questionnaire asked those surveyed firms:

> *"What is the firm's timing for screening its relationship database(s) to identify parties designated under UN/UK sanctions?"*



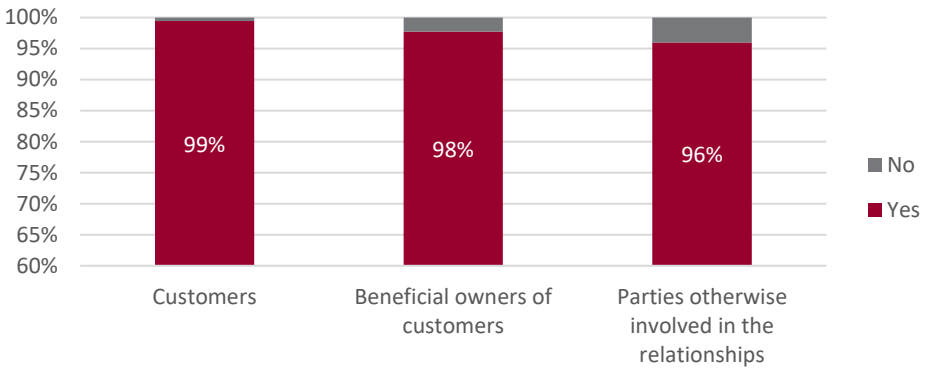
It was positive to note that the vast majority of firms are screening their customers on a daily basis. Screening only on a trigger basis may be appropriate for the 11% of firms shown above, but firms should be mindful that, where screening is less frequent than daily, they run the risk of not identifying sanctions connected relationships in a timely manner. As such, additional controls should be in place such as trigger event screening or manual screening when any new/updated notices are being issued.

2.2 Parties subject to screening

Customer Screening

Chapter 12 of the Handbook requires firms to have in place appropriate and effective policies, procedures and controls to identify, in a timely manner, whether a prospective or existing customer, or any beneficial owner, key principal or other connected party, is the subject of a sanction issued by the UN, UK or the P & R Committee.

Categories of person screened against sanctions lists



Almost all surveyed firms are screening customers, beneficial owners or parties otherwise involved in relationships. One firm explained that its only customer is its head office and therefore it does not screen this relationship. However, there was also a small minority of firms which advised that they were not screening beneficial owners of customers and parties otherwise involved in the relationships for reasons such as these parties not being entered into the firm's customer management system and thus did not feed into the screening system. Failure to screen all customers, beneficial owners and parties otherwise involved in the relationships, heightens the risk of firms not meeting their sanctions obligations. The Commission is engaging further with these outlier firms over their measures for complying with sanctions.

Transaction Screening

The Handbook requires firms to have in place a system and/or control to detect and block transactions connected with those natural persons, legal persons and legal arrangements designated by the Bailiwick's sanctions regime. Whilst non-banks are technically not undertaking wire transfers and are instead utilising the services of banks to enact fund transfers, these non-banks are still raising payment instructions/requests. Furthermore, where non-bank firms are making third party payments to persons that are not within the firms' customer systems, they should note that the legal requirements and the Handbook rules around sanctions apply to their firm, and they should not place reliance on another firm's systems and/or controls to detect and block sanctions connected transactions. The banks surveyed typically explained that all information within SWIFT (or similar) messages is screened including names, BICs, addresses, and references.

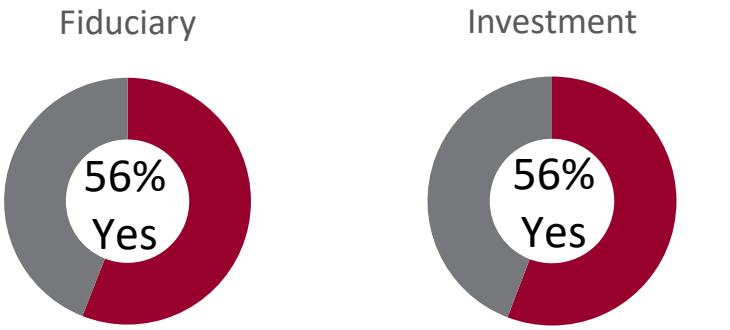
Case Study: Third party payments

One medium-sized firm (non-bank) explained how it previously did not screen third party payments and submitted a payment request to its bankers. The bankers identified sanctions connections through its automated transaction screening processes and refused the payment. Not only did this event increase the risk of a sanctions breach for both firms involved in the transaction, but it also had the potential to cause concern from the bank regarding the non-bank's control framework and risk appetite, and may have undermined the relationship between the two firms. Consequently, new controls were put in place at the non-bank to manually screen recipients of third party payments.

Screening of underlying assets

Where firms administer or manage legal persons or legal arrangements, such as holding companies or collective investment schemes, there is a risk that those legal persons/legal arrangements, or the assets thereof, become the target of sanctions. To understand how this risk is being managed, we asked fiduciary and investment firms:

> *does the firm's sanctions screening include subsidiaries and/or underlying assets?*



Area for improvement: Screening of underlying assets

Only 56% of the firms surveyed were screening underlying assets and some of those firms which were screening underlying assets only did so on vessels despite the imposition of sanctions not being limited to these types of assets. A number of firms stated that they would now start screening underlying assets following the thematic questionnaire being issued. One such firm indicated that it was in the process of considering screening subsidiaries active in industries with potential for sanctions exposure such as those operating in the oil/gas sectors. It is expected that firms consider whether the screening of underlying assets (including subsidiaries) for some relationships is warranted given that these could be the target of sanctions. Consideration should be given to the specific types of assets, the jurisdictions in which they are held or are operating in, and the sectors they are operating in. We are re-visiting this area with the 44% of firms which are not screening underlying assets.

Section 3: Effectiveness of Automated Screening Systems

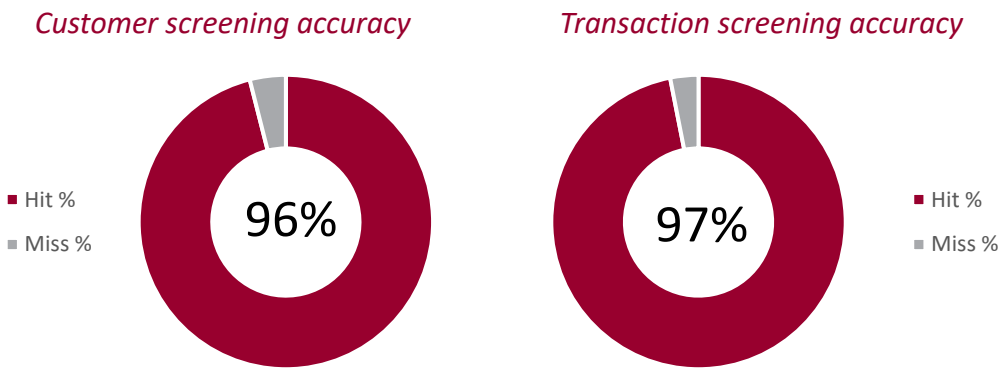
3.1 Effectiveness testing background

We utilised the services of a specialist third party to perform the effectiveness testing aspect of the thematic review. Both the customer screening test and the transaction screening test files comprised 10,100 names of individuals and entities recorded in publicly available sanctions lists published by the UN, OFAC, EU and OFSI. A small number of PEP names were included along with 'clean IDs'. The clean IDs were used to assist primarily with testing the efficiency of the screening tool as these were names not on sanctions/PEP lists and were not expected to generate alerts.

Half of the names within the test files were names exactly as detailed within the relevant sanctions list i.e. unmanipulated (control) data, with the other half being names on these lists which have been manipulated to test the extent of the fuzzy matching capabilities of screening systems employed by firms. The manipulated names were created by applying one algorithmic manipulation to an original name, such as removing one character of a name or swapping characters within the name. These manipulations are designed to represent typical data quality issues that any firm would normally face and also used as examples where customers may purposely submit false/altered names to circumvent sanctions. It was stressed to firms that that all production environment rules, settings and lists were to be used as normal in order to establish a true picture of business-as-usual system performance. Whilst the format of the test data file varied from one firm to another, all firms received exactly the same set of names so that comparative results could be produced.

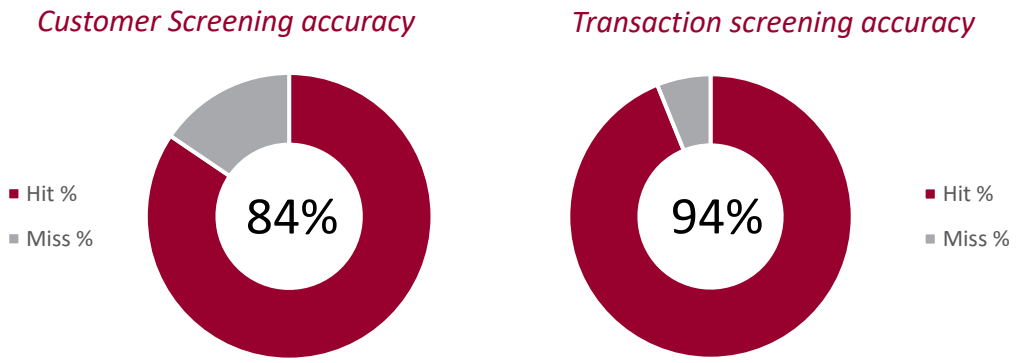
3.2 Test results

Control data test results



Firms broadly performed well in the control data test, with the median scores across all firms tested being **96.25%** accuracy for customer screening and **96.90%** accuracy for transaction screening. These percentages represent the proportion of names within the test data for which firms generated a 'hit'. Median scores have been used as this is more representative than the 'mean' scores due to a minority of poor performing outliers that disproportionately affected the overall results and/or which had configuration/operational issues.

Manipulated data test results



The median scores for the manipulated data test were **84.48%** and **93.89%**. These results are expectedly lower than the control data test as the data manipulations intentionally affect the accuracy of the automated screening system.

It was encouraging to note that all firms investigated the results post-testing and provided rationale for the 'misses' encountered, with those firms with poorer test results able to largely explain the causes. Some firms explained that their results were affected by its system not being configured to screen 'weak' aliases of names sourced from OFAC lists in line with the Wolfsberg Group guidance[6], and that domestic transactions are not screened due to being captured within customer screening of the remitting bank and of the recipient bank, given that they are subject to the same screening requirements.

Whilst the effectiveness testing results were largely positive, areas for improvement were identified. Many firms expressed that the effectiveness testing highlighted areas where improvements could be made to the matching capabilities and/or the efficiency of the screening system. A small number of firms performed particularly poorly and require material improvements to be made to their systems to match the effectiveness levels of their peers, although it should be noted that automated screening systems are not the only control in place at these firms.

[6] *the Wolfsberg Group Guidance on Sanctions Screening - 2019*

There were a range of screening systems utilised by the firms, some in-house/Group developed, and some provided by external vendors. We found that the system used was largely irrelevant; the more pertinent point was the way the system had been implemented, maintained and overseen. There were some firms which clearly invested significant time and resource into their screening systems, the related processes and governance arrangements. Conversely, there were examples where this was not the case and screening was less of a consideration.

Case Study: Under-investment in systems

One firm explained how its in-house screening systems were built 10 years ago and had remained largely unchanged since implementation. This firm performed poorly in the effectiveness testing and has since initiated a project to review and potentially replace the current screening system utilised by the whole Group. As an interim solution, the firm undertook an additional ad-hoc screen of its data through bulk upload of names to a screening platform, and will continue to do so on a periodic basis until the new system is in place.

No actual sanctions breaches were found through the above, however under-investment in the ongoing review, maintenance and testing of the systems implemented to mitigate risks may result in these controls being ineffective. It is critical that firms keep such systems up-to-date to ensure they are functioning appropriately and effectively.

3.3 Data integrity

It was highlighted during the testing process that a number of firms' customer screening systems require customer data and sanctions list data to be in a specific format and structure in order for the screening matching system to function properly. In these cases, if firms do not have controls in place to ensure their records are formatted correctly, there is a risk that records will not be screened appropriately within the automated process.

A common solution to prevent this was through hard controls within firms' customer records systems to limit the types of data that can be input into fields (e.g. mandating that all records have at least a first name and a last name entered) and users being required to select from pre-defined values for fields such as nationality and residence. One firm has ensured it has confidence all relevant records have been screened through an automated report being generated of any records failing to load into the screening system. These records are investigated by staff, with any data issues resolved and then re-screened.

3.4 Screening system efficiency

The primary goal of the testing undertaken was to assess the effectiveness of the screening systems employed however it also covered the efficiency of the screening systems through assessing the number of returns the system generated. Most firms produced similar volumes of returns from the testing however some firms generated a much larger number of returns.

In this respect, some firms may be more conservative and content with a larger volume of alerts per name being generated as this 'wider net' may capture more true matches. That said, as mentioned earlier in this report, periods of increased sanctions activity may produce large volumes of alerts and firms should bear in mind when tuning their systems their capacity to investigate and resolve these alerts in a timely manner.

Conversely, some firms may not be so risk averse and are satisfied with tuning the system to reduce the level of 'noise' generated. In this regard, when tuning the system, firms should be alive to the risk of over tuning the system to the point that matching criteria is so narrow that it misses true matches and, ultimately, risk breaching sanctions.

Area for improvement: Efficiency and Effectiveness

We found some firms included automated rules to discount potential matches in order to reduce the level of alerts requiring manual intervention. A typical example of this was automatically discounting potential matches due to the date of birth differing by more than a few years. Where firms are utilising such rules, they should be cognisant that dates of birth, as with other pieces of information, may have data quality issues (e.g. characters being switched around or entered incorrectly) which may impact the accuracy of the screening system. Furthermore, the data provided by sanction authorities may not always be fully complete at the outset and may be updated with additional information which could impact the accuracy of screening using such rules.

Ultimately, there is a balance to strike between efficiency and effectiveness and this will be informed by each firm's own risk appetite and operational capacity. Tuning the system to be efficient is a necessary aspect of operating automated screening systems, however firms should ensure they give adequate consideration as to whether the automatic discounting rules being used are appropriate.

Section 4: Oversight of Sanctions Screening Systems

4.1 Board understanding and consideration of sanctions risk

Sanctions risk should be captured as part of firms' ML and TF business risk assessments, however we found that the understanding and consideration of sanctions risk amongst Boards/senior management was varied. Statements given such as 'we have no appetite to breach sanctions' are not meaningful and do not express the firm's risk appetite or controls appropriately. Rather Boards should be alive to how the firm's customers, products and services may be impacted by sanctions and what controls are in place to mitigate sanctions risk.

Good Practice: Consideration of sanctions risk

Good practice was seen in one non-bank firm which appeared to have considered its sanctions risk in depth and had a member of the local compliance team tasked with being the firm's subject matter expert for sanctions. This firm was able to discuss the different types of funds it administered and how the sanctions risks differed between them. Examples included funds investing into the energy sector being at more risk of sanctions, and investments to and from jurisdictions with active sanctions regimes being subject to additional scrutiny.

Area for improvement: Understanding and mitigating sanctions risk

During discussions it became apparent that only a few Boards were able to provide good detail of the types of customers and areas of its business that are more exposed to sanctions. It was often explained that customer level sanctions risk was considered as part of jurisdictional risk. Assessing sanctions risk solely from a jurisdictional risk perspective is not sufficient. Firms should ensure they have considered sanctions risk appropriately at a customer level as sanctions risk is a relevant risk factor which requires inclusion within ML/TF risk assessments. Specifically, firms should also be assessing the sanctions risk exposure of the products/services provided to the customer and to the type of customer it is providing these to. Customers with relevant connections to jurisdictions with active sanctions regimes in place or customers which are active trading companies dealing in dual use goods and/or providing services in sanctioned countries have an increased sanctions risk exposure.

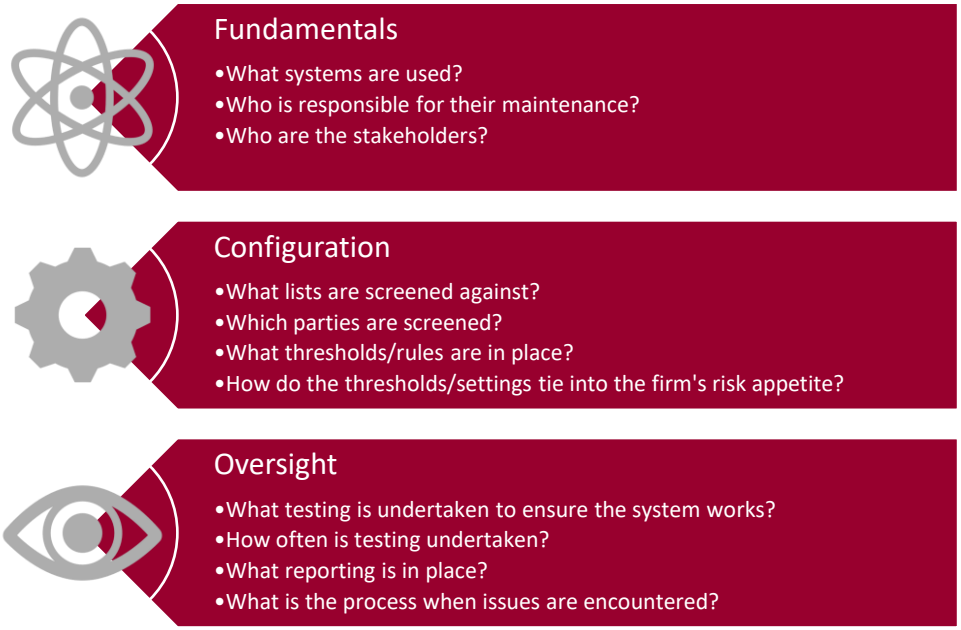
When assessing residual risk, firms should also take into account the firm's controls. Effective sanctions screening is only one part of a firm managing its sanctions risks, firms also need to understand what TF and PF threats their business is exposed to, and instil adequate controls in respect of: (i) the identification and verification of customers, and their ultimate beneficial owner(s), (ii) understand where their customers' source of funds and wealth originate from and (iii) perform ongoing monitoring of transactions and activity, to mitigate these risks fully.

4.2 Sanctions screening policies and procedures

It was positive to note that the policies and procedures provided by most firms had plentiful information about how to investigate and discount alerts generated by the screening systems, what the timeframe for investigating alerts was, and at which points alerts should be escalated for further consideration by compliance and/or the Board.

Area for improvement: Screening policies and procedures

Whilst policies and procedures included details on resolving alerts, there were firms with policies and procedures that were lacking in basic detail of the screening process. Firms should ask themselves whether the policies and procedures cover the following:



Given that failures in the system will result in a failure to generate alerts, appropriate documentation and governance around this process is critical. Procedures should also include details of contingency plans for systemic failures in the process, including whether there are back-up systems or processes to use until the system is operational again, and what service level agreements there are with external vendors, Group or otherwise to investigate issues.

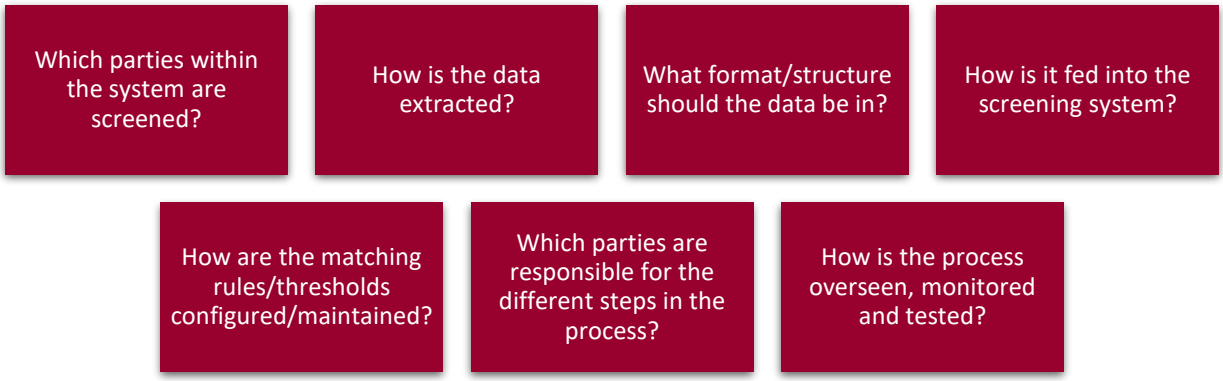
Case Study: Oversight of systems

One firm participating in the thematic review has thousands of business relationships spanning a broad range of jurisdictions, including those deemed to pose a higher risk of ML/TF and those with active sanctions regimes in place. This firm has previously changed the automated screening tool being utilised and has multiple systems (some of which are legacy) storing data on customers and other relevant parties. The firm therefore has multiple sets of

data it must arrange to be screened by the screening system and has, on a number of occasions, identified that groups of names have failed to load into the screening system. In one instance this resulted in over 10,000 names not being screened for over 2 years. Once identified, the firm re-screened the names and no sanctions breaches were found, however it was noted that this firm did not have a control in place to ensure that all required names were successfully loaded into the screening system.

Area for improvement: Understanding systems

Firms should ensure that they understand and have documentation that clearly evidences the interaction between their customer data systems and screening systems. Firms should be able to answer the following:



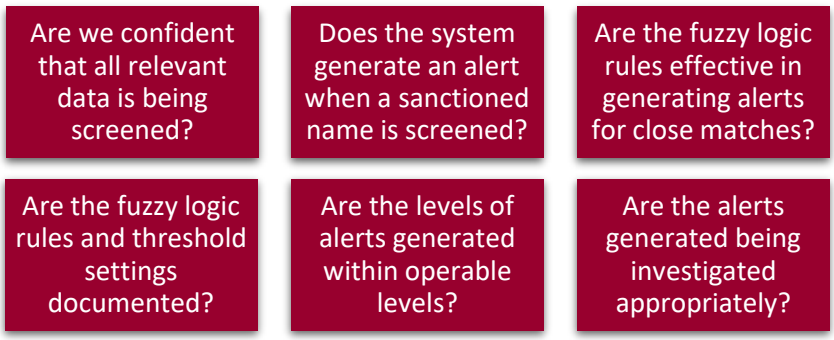
Ongoing monitoring and testing that each sanctions screening system is configured appropriately will mitigate the risk of the firm being unaware its systems are failing to screen relevant parties for an extended period of time.

4.3 Testing of sanctions screening systems

The Handbook requires firms to ensure that their compliance monitoring arrangements include an assessment of the effectiveness of the firm's sanctions controls and their compliance with the Bailiwick's sanctions regime. The consequences of breaching sanctions can be severe and, as such, it is of paramount importance that the Board has confidence that its screening systems and related processes are effective and, as with other financial crime controls, this confidence can be assisted through testing.

It was particularly disappointing to hear some views on testing such as the sanctions screening system generating alerts being proof that the system is working effectively. Systems may be generating alerts but this does not necessarily mean it is generating all alerts that the firm expects nor whether there are any names being omitted from screening in the first place.

The area of sanctions screening systems is specialist and it is not suggested that Boards have intricate knowledge of all aspects of every system involved however, understanding the fundamentals of the systems and processes so that risks can be identified and mitigated *is* expected. Boards could ask the following questions of themselves during an assessment of the sanctions screening process:



Where the response to any of these questions is 'No', Boards should consider developing their understanding, documentation, and testing regarding the sanctions screening systems.

Area for improvement: Outsourced functions

We saw in some instances a heavy reliance on Group or external vendors in that there were assumptions of confidence in the system as it was being maintained by a Group centre of excellence or because the system was provided by a specialist external vendor. Despite these Group/external parties having expertise in this area, where there are Group managed or externally developed systems, or where screening is outsourced, the local firms should still be testing the systems themselves or being provided with sufficient detail to be assured that the system is being tested and is working effectively.

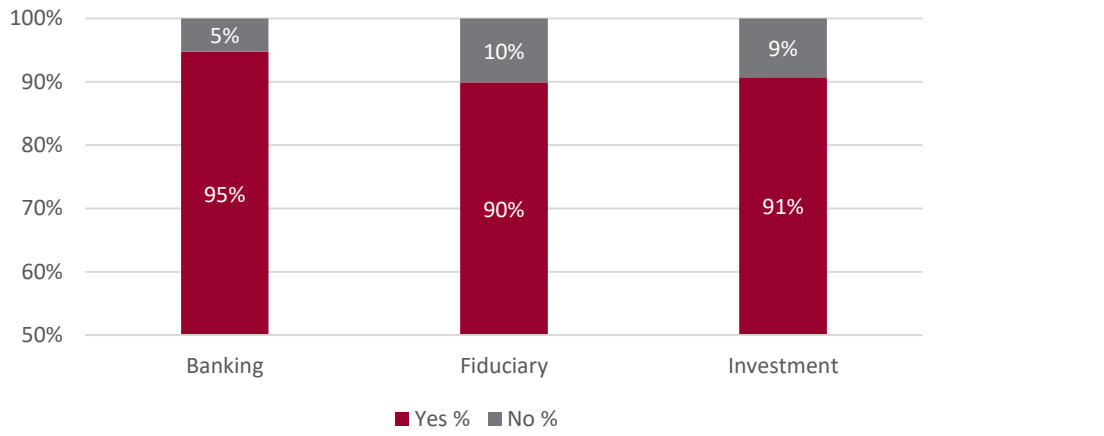
Furthermore, the onboarding process undertaken as part of the effectiveness testing highlighted that for some of the larger firms which are part of a Group, there were varying degrees of local understanding regarding who was responsible within the Group for the different aspects of the end-to-end screening process. Whilst our testing in this format may have been new to some firms, and thus required additional input from Group, some firms were not able to readily access the Group function responsible for the screening process and required deadline extensions in order to perform the effectiveness testing.

Given the legal onus to apply sanctions is on the locally licensed firm, firms should be able to quickly identify those individuals with the Group which are responsible for investigating and resolving issues. Firms should have readily available documentation detailing the various stakeholders and individuals/departments which are involved in the end-to-end sanctions screening process.

Good Practice: Oversight of Group processes

We also saw good practice from a small number of firms in respect of oversight of third parties where these firms' local compliance teams visited the Group office/team to review and discuss the sanctions screening processes – both the technical aspects as well as the processes for reviewing and discounting alerts. This is a good example of how the local firm has ensured it is aware of how the system is working and is comfortable with the processes, despite them being Group driven and owned.

"Has the effectiveness of sanctions screening systems been subject to the firm's compliance monitoring programme since 1 January 2017?"

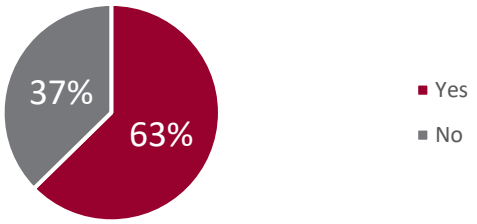


It was encouraging to see a high proportion of firms across all sectors testing the effectiveness of their screening systems through the CMP.

Area for improvement: Compliance monitoring

Whilst testing is undertaken as part of the CMP, the testing we saw commonly focussed on testing the rationales and timeframes for discounting alerts, which is only one element of the whole screening process. To ensure the system is indeed effective and functioning as expected, testing that the system is appropriately generating alerts in the first place is required. The testing should represent a test of the business-as-usual process of automated screening, which will likely include the interfacing of multiple systems and the transmission of data. Furthermore, firms should also be testing the different types of records/entities held within its system (i.e. natural persons, entities, vessels, aircraft, stocks/shares) to ensure each type of record/entity is feeding into the automated screening system.

Has the effectiveness of screening systems been subject to the firm's internal audit processes since 1 January 2017?



63% of firms with an internal audit function have had the effectiveness of their screening systems reviewed and the details given indicated that a wide range of issues have been identified by internal audit across these firms. Given that the automated screening systems are a key control in mitigating sanctions risk, the systems utilised should be part of the AML/CFT internal audit remit and periodically captured as part of internal audits. Those firms with internal audit functions which have not tested the effectiveness of the sanctions screening systems should give consideration to this when agreeing the scope of future internal audits.

Good Practice: Testing by external parties

It was positive to see some firms utilising external third parties to test and assist with ongoing tuning of screening systems. There were instances where performance benchmarking was undertaken to inform the firm of its performance compared with its peers. Unsurprisingly, these firms performed strongly in the thematic review effectiveness testing and these firms could explain in detail why any test entries did not 'hit'.

4.4 Implementation of screening systems

When implementing an automated sanctions screening tool, firms should be performing due diligence on the vendor and undertaking a risk assessment of the tool before implementing it to ensure it will meet expectations. As part of its engagement with a prospective vendor, information should be sought regarding:

- The data content/structure requirements
- How the system works in practice
- The limitations of the system
- Any assurance testing undertaken by the vendor
- The level of ongoing maintenance & support provided
- The level of data and reporting that can be extracted

Good Practice: Implementing new screening systems

Examples of good practice were noted at two firms that had recently implemented new sanctions screening systems. Both firms ran the incumbent system concurrently with the replacement system for a period of time to ensure the replacement system was performing to expectations. Furthermore, one of these firms used the lowest percentage thresholds (most cautious approach) for matching as it was not as familiar with the new system, with these settings to be reviewed as part of ongoing monitoring and tuning.

Case Study: Board involvement in implementation of sanctions screening systems

Conversely, the process taken by one firm to change its sanctions screening system provider was undertaken largely via email sent by the compliance function to the Board. Whilst a brief overview of the new system was included (including any cost savings through switching provider), it did not include sufficient details as to how Compliance was satisfied that the new system was appropriate nor what governance arrangements would be in place for the new system. There was mention that policies and procedures would need to be updated but there was no explanation of the expected differences nor details of the due diligence undertaken on the proposed vendor, which parties were responsible for the implementation of new system, nor what reporting would be provided during implementation and on an ongoing basis. Furthermore, there was limited discussion or challenge seen regarding the change.

4.5 Ongoing monitoring of screening systems

There were many examples of firms reporting appropriate statistics to the Board and relevant committees, including:

- how many hits were generated during the period
- how many hits are outstanding and awaiting resolution
- average time to investigate hits
- how many true matches
- how many false positives
- any records failing to load into screening system

What was also often seen in periodic Board reporting was cut and paste excerpts from the Commission's website detailing that a sanctions list was updated. Reporting of this information should be tailored to be relevant to the firm. If sanctions notices are issued regarding jurisdictions which the firm has customers with connections, some commentary around what this means to the firm would serve better than simply transposing the notification.

Good Practice: Reporting of screening system performance

That said, good practice was seen through one firm comparing its monthly screening volumes and Compliance providing commentary to the Board regarding any spikes or dips. Furthermore, this firm compared its screening volumes to that of other branches within the Group, providing rationale for any major differences.

The above is not to say that Boards should receive every single piece of information regarding the sanctions screening system's performance, but the reports on system performance should be a part of regular upwards reporting with an opportunity for oversight to be exercised and evidenced.

Conclusion

The majority of firms are placing reliance on automated sanctions screening systems to identify sanction targets. Whilst these systems can create efficiencies and be effective in identifying potential sanctions connections, firms should be alive to the risk of placing over reliance on these systems and accept that the process is complex.

The effectiveness testing undertaken as part of this thematic review was extensive, and the results showed that the tested firms' automated sanctions screening systems are effective, with only a minority of firms in need of material improvements to demonstrate that their systems are effective. However, the thematic review has also shown that there are differing levels of maturity within firms in respect of the assessment and consideration of sanctions risk, along with the testing and oversight of the sanctions screening systems employed to mitigate this risk, particularly from some firms utilising Group centres of excellence. The documentation surrounding the sanctions screening processes was noted to be lacking in some areas and, generally, they were not as well developed as those policies and procedures in place for other areas of firms' AML/CFT compliance frameworks.

Effective sanctions screening is only one part of a firm managing TF and PF risks, firms also need to understand what TF and PF threats their business is exposed to and instil adequate controls in respect of: (i) the identification and verification of customers, and their ultimate beneficial owner(s), (ii) understand where their customers' source of funds and wealth originate from and (iii) perform ongoing monitoring of transactions and activity, to mitigate these risks fully.

Firms with material deficiencies identified during the thematic review are subject to risk mitigation programmes. Going forward the Commission will consider how **all** firms have incorporated the findings from this report into their policies and procedures as part of its supervision.