Jersey Financial Services Commission

BANKING BUSINESS

THEMED EXAMINATION PROGRAMME 2014: AML/CFT AND FINANCIAL SANCTIONS SUMMARY FINDINGS

Issued: August 2014

GLOSSARY OF TERMS

The following table sets out a glossary of terms used in this report.

AML/CFT	Anti-money laundering and countering the financing of terrorism
the AML Handbook	Codes of Practice issued under Article 22 of the Proceeds of Crime (Supervisory Bodies)(Jersey) Law 2008
BRA	AML/CFT Business Risk Assessment
the Commission	Jersey Financial Services Commission
the Banking Codes	Codes of Practice issued under Article 19A of the Banking Business (Jersey) Law 1991
Fuzzy matching	Techniques used to identify names that do not precisely match a target name but may still warrant further enquiry
PEP	Politically exposed person
Screening filter	Software used by banks to screen customer records and transactions against target names
Target name	A name appearing on financial sanctions, PEP or other screening lists

CONTENTS

1 Executive summary

1.1 Introduction

1.1.1 This report provides an overview of the findings from a programme of themed on-site examinations conducted by the Banking division of the Commission during 2013-14.

1.1.2 The findings in this report are drawn from 17 on-site examinations of banks conducted by Commission staff as well as responses to a self-assessment questionnaire that was sent to each of the banking groups represented in Jersey.

1.2 Findings

1.2.1 Overall, the Commission found that banks in Jersey were well advanced in implementing their AML/CFT and financial sanctions systems and controls. These topics have been the subject of considerable focus by international banking groups as a result of regulatory action taken in the US and elsewhere and several of the banks examined were found to have benefited from improvements being carried out by their parent group.

1.2.2 That said, the examination programme highlighted a number of areas in which improvements could be made, particularly where local management had placed undue reliance on the screening arrangements provided by their parent group without having first satisfied themselves that they provided adequate mitigation to the AML/CFT risks applicable to the Jersey business.

1.2.3 The examination programme included a practical screening exercise whereby banks were asked to pass a list of names provided by the Commission through their screening filters and present the results for analysis. This exercise proved valuable in benchmarking the banks' screening arrangements and in two cases led directly to the identification of serious, and previously undetected, flaws in their screening filters.

1.2.4 Areas in which banks tended to be better advanced as a whole included:

- Quality and coverage of the BRA.
- Staff awareness and training.
- Screening at the point of customer take-on.
- Screening of transactions.

1.2.5 Those areas requiring further focus were as follows:

- Automated re-screening of customers.
- Senior management understanding of screening arrangements.
- Coverage of financial sanctions risks in the BRA.
- Screening system user access controls and IT change governance.
- Staff procedures for discounting potential target matches.
- Compliance monitoring.

1.3 Conclusion

1.3.1 The Commission would encourage all banks to consider the findings in this report in the context of their own business.

1.3.2 The Commission has issued individual reports with relevant recommendations to those banks that received an on-site examination. Those banks that did not receive an on-site examination have submitted a self-assessment questionnaire to the Commission which, in some cases, may form the basis for further discussion of this topic.

2 Introduction

2.1 Objectives and limitations

2.1.1 The Commission regularly undertakes on-site examinations on specific themes to assess the extent to which regulated entities are operating in accordance with their obligations under the respective Laws, Orders, Codes of Practice and Guidance Notes. These examinations focus on identifying instances where depositors, customers or the registered entity itself may be at risk or where standards and practices required by the regulatory regime are not being observed.

2.1.2 The Commission's on-site examination programme is designed to:

2.1.2.1 assess the risks faced by the entity and review the controls, procedures, policies and processes in place to mitigate those risks;

2.1.2.2 obtain a greater understanding of the entity's activities, thereby enabling the Commission to focus attention on higher risk areas; and

2.1.2.3 take into account existing relevant information, review the resolution of any previous examination issues and to obtain assurance on any deficiencies highlighted through off-site supervision.

2.1.3 This review did not cover all aspects of AML/CFT and financial sanctions risk and the findings set out in this report should be treated as examples of good practice rather than formal regulatory guidance.

2.1.4 AML/CFT and financial sanctions risk are considered highly pertinent topics owing to the cross-border and, often, non-face-to-face nature of business undertaken by deposit-takers in Jersey. Banks in Jersey are potentially exposed to AML/CFT and financial sanctions risks which, in the most serious cases, have the potential to damage not only their own reputation but also that of Jersey as an international finance centre.

2.2 Methodology

2.2.1 This examination programme was undertaken by way of a self-assessment questionnaire and a series of on-site examinations.

2.2.2 A self-assessment questionnaire was provided to all banks and comprised of 28 questions covering the following topic areas:

- Governance and business risk assessment;
- Policies and procedures;
- Staff awareness and training;
- Customer screening;
- Outsourcing;
- Transaction monitoring and periodic reviews;
- Dealing with potential financial sanctions target name matches;
- Compliance and internal audit; and
- Applying identification measures to existing customers

2.2.3 Following an initial analysis of the questionnaire responses, 17 banks were selected for a three-day on-site examination covering the same subject areas.

2.2.4 The on-site examinations also included a practical test of customer screening arrangements. In advance of the on-site examination, each bank was provided with a list of 25 names to test against its screening filters used in the following situations:

2.2.4.1 A new customer take on;

2.2.4.2 A periodic re-screening of the customer base; and

2.2.4.3 An inward/outward payment.

2.2.5 The results of the screening were then presented for analysis during the on-site examination.

2.2.6 The names appearing on the screening list were drawn from publicly available sources and fell into the following categories:

Category	**Sub category**	**Number**
Sanctions	UK Consolidated list	6
	OFAC SDN List	4
PEPs		6
Crime	Financial	4
	Terrorism	1
	Other	1
Control		3
Total		**25**

2.2.7 An effort was made to introduce as much variety as possible into the screening list by including both legal entities and natural persons and selecting from a variety of financial sanctions lists, PEPs and other higher risk categories. The list of names also included variations known aliases and anomalies intended to test the screening filters' capacity for fuzzy matching.

2.2.8 A detailed analysis of the results of this exercise was provided to each bank as part of its examination report, together with recommendations for remedial action, where relevant.

2.3 Regulatory Requirements

2.3.1 The Proceeds of Crime (Supervisory Bodies)(Jersey) Law 2008 appoints the Commission as the supervisory body responsible for overseeing compliance of persons conducting financial services business with the Money Laundering (Jersey) Order 2008 and the AML Handbook.

2.3.2 Jersey registered deposit-takers are also obliged to adhere to the Banking Codes, which set out the requirements for, *inter alia*, the risk management framework that must be maintained by banks. The Banking Codes include the following provisions relevant to AML/CFT and financial sanctions:

"A registered person must organise and control its affairs effectively for the proper performance of its business activities and be able to demonstrate the existence of adequate risk management systems.

A registered person's systems must ensure that:

> *Management is able to properly guard against involvement in financial crime and ensure that the registered person is complying with all relevant legislation and guidance to counter money laundering and the financing of terrorism. Anti-money laundering legislation includes the Proceeds of Crime (Jersey) Law 1999, the Money Laundering (Jersey) Order 2008, the Terrorism (Jersey) Law 2002 and the Drug Trafficking Offences (Jersey) Law 1988, as well as any other applicable Laws and United Nations or European Union Sanctions Orders applied within Jersey, all as amended from time to time. The legislation must be observed in conjunction with the standards set out in the relevant Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism (the "relevant AML/CFT Handbook") issued by the Commission. In addition to legal action, failure to follow legislation to counter money laundering and the financing of terrorism or the relevant AML/CFT Handbook may form the basis for regulatory action by the Commission;*
>
> *Management is able to perform sufficient due diligence on the registered person's customers and prospective customers to adequately assess all relevant risks, including that of money laundering;"*

3 Findings

3.1 Governance of AML/CFT and financial sanctions risks

3.1.1 Senior management involvement and oversight are essential if a bank is to successfully identify and mitigate its AML/CFT and financial sanctions risks. In approaching this series of examinations, the Commission was mindful that all Jersey registered deposit-takers are either branches or subsidiaries of a wider banking group and may therefore be reliant upon group screening and monitoring arrangements delivered outside of the Island.

3.1.2 Whilst acknowledging the potential benefits of such an approach, the Commission was keen to establish whether local management were sufficiently informed of the workings of group screening and monitoring arrangements to allow them to assess whether they adequately addressed the AML/CFT and financial sanctions risks faced by the Jersey operation.

Senior management awareness and oversight

3.1.3 In general, the Commission found that bank senior management's awareness of customer screening and monitoring arrangements was well developed, perhaps reflecting the increased focus that has been applied to this topic in the wake of recent regulatory enforcement actions in the US and elsewhere.

3.1.4 However, in a number of cases, the screening exercise conducted as part of the on-site examination highlighted some limitations in the screening arrangements that had not been fully appreciated by local management. Some illustrative examples of this are provided below:

(Fig. 1)

The Mayor

One bank was surprised when a PEP featuring on the screening list was not identified by one of its screening filters. The PEP in question was the mayor of a major overseas city. Upon investigation, it was established that the bank's parent group had excluded mayors from the categories of PEPs included in its screening filter on the basis that its onshore business only banked UK residents and therefore considered the role of a mayor as relatively low risk in that context.

Punctuation

One of the names on the screening list had been manipulated by the Commission by removing an apostrophe and a hyphen from the original target name which, in some cases, resulted in the name not being identified by screening filters. Local management tended to be surprised by this result, highlighting the importance of ensuring that staff procedures for inputting customer names are properly aligned with the bank's screening filters.

Which screening lists?

Some of the senior management of banks were not aware which screening lists were used in the screening filters deployed by the bank and were therefore surprised when some of the names in the screening list provided by the Commission failed to produce a match. Examples of such exclusions included disqualified directors and some categories of crime. It is critical that banks understand the extent of their subscription to commercially available screening solutions (such as World-check) and not simply assume that all risk categories are included.

3.1.5 The Commission also examined to what extent the screening and monitoring arrangements were being overseen by local management. Whilst there tended to be sufficient escalation of potential target name matches identified by the screening filters, a number of banks were recommended to improve their ongoing monitoring of the effectiveness of screening and monitoring arrangements. Such monitoring should include not only information on whether alerts are being responded to within agreed timescales but also analysis of the quality and quantity of alerts being raised in order to determine whether the systems continue to perform as intended.

Good Practice:

- Senior management have sufficient awareness of the workings of group screening and monitoring systems to determine whether they adequately address the risks faced by the local business.
- There is a mechanism by which local management are made aware of material changes to group systems so as to be able to raise objections or, where necessary, adopt alternative mitigating controls.
- Local management receive ongoing information on the performance of screening and monitoring tools.

Poor practice:

- Senior management place blind reliance on group systems.
- Senior management are not in a position to oversee the performance of screening and monitoring arrangements.

AML/CFT Business Risk Assessment

3.1.6 It is a requirement under the AML Handbook that all financial services businesses assess their AML/CFT risks and, based on that assessment, adopt an AML/CFT strategy. The Commission has previously examined deposit-takers against these requirements and has largely found the requirements to be well understood and BRAs to be of a good standard.

3.1.7 Consequently, findings in this area tended to be relatively minor and included the need to ensure that the BRA provided adequate coverage of financial sanctions as well as AML/CFT risks. In particular, a number of banks were recommended to revisit their BRA in order to provide specific coverage of financial sanctions issues in the following areas:

3.1.7.1 Geographic factors;

3.1.7.2 Customer screening arrangements;

3.1.7.3 Management information;

3.1.7.4 Policies and procedures;

3.1.7.5 Staff training; and

3.1.7.6 Reliance on third parties.

3.1.8 In some cases, banks were recommended to provide a more detailed description of their screening and monitoring arrangements so as to ensure that senior management had been provided with sufficient information to determine whether the arrangements provided sufficient mitigation against the risks identified in the BRA.

3.1.9 Finally, the Commission recommended that some banks amend their BRA to include details of any areas in which the bank had decided not to apply screening measures (e.g. a number of banks had determined that they would not apply screening to BACS payments or cheques, on the basis that risk levels were acceptable).

Good Practice:

- The BRA should include coverage of financial sanctions risks.
- Screening and monitoring arrangements should be properly documented in the BRA so as to allow management to assess whether they provide an acceptable level of risk mitigation.
- Accepted risks should be documented in the BRA together with the accompanying rationale.

Poor practice:

- Failing to consider financial sanctions risks.
- Lack of detail on the workings of screening and monitoring arrangements.

3.2 Staff training and awareness

3.2.1 The effectiveness of AML/CFT and financial sanctions controls can be undermined if relevant staff lack sufficient training and awareness. All financial services business have an obligation under the Money Laundering (Jersey) Order 2008 to provide training to their staff and to have procedures in place to monitor the effectiveness of such training.

3.2.2 The Commission's previous experience has been that these requirements are generally well understood by both deposit-takers and their staff and this was borne out again, with relatively few findings raised on this topic. Without exception, those banks examined were providing staff with regular anti-money laundering training and were monitoring the delivery of such to ensure that all relevant staff were being trained at an appropriate frequency.

3.2.3 The Commission's focus on this series of examinations was to consider to what extent financial sanctions issues were addressed in staff training. Whilst the majority of the training delivered focussed on anti-money laundering, most deposit-takers included some element of financial sanctions training, whether as part of their general AML training or, in some cases, on a standalone basis.

3.2.4 Clearly the nature and frequency of financial sanctions training should be proportionate to the staff member's role and therefore the Commission would tend to

expect more specialised training to have been made available to those staff that have cause to investigate potential financial sanctions target name matches as part of their duties.

Good Practice:

- Regular financial sanctions training and awareness programmes that are relevant for the staff member's role.
- Testing to monitor the effectiveness of training.
- Ongoing monitoring of staff to identify where there may be a training need.
- Proper communication of changes to relevant policies and procedures.

Poor practice:

- Training does not address financial sanctions risks.
- Lack of specialist training for relevant staff.

3.3 Customer screening

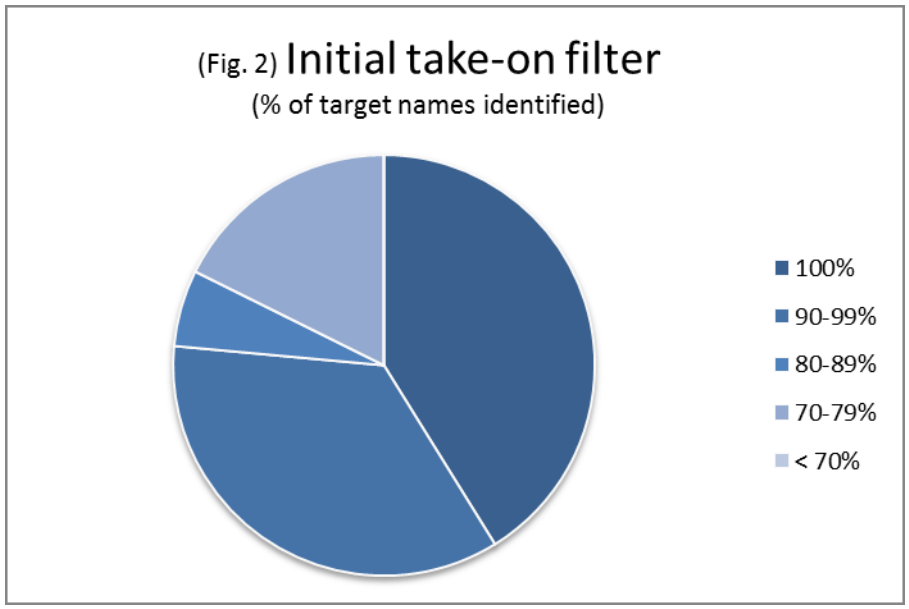
3.3.1 Customer screening is the process by which a business identifies whether a counterparty or transaction may be subject to financial sanctions or exhibits other higher risk characteristics. The Commission's focus throughout this examination programme was to consider the arrangements relied upon by deposit-takers for screening new customers, existing customers and customer transactions.

3.3.2 As outlined at section 2.2 of this report, the examinations included a practical test of deposit-takers' screening arrangements using a screening list of 25 names selected by the Commission. This exercise proved very useful in benchmarking screening arrangements and led to some material findings.

Screening at customer take-on

3.3.3 Screening of customers at the point of take-on is a bank's first line of defence and it is therefore critical that the screening systems provide adequate coverage of risks and generate good quality results.

3.3.4 Without exception, all of the banks examined performed some form of screening at the point of customer acceptance through one, or a combination of, commercially available screening filters, in house screening systems and internet searches. The scope of such screening was typically wide at the point of customer take-on and included searches against relevant financial sanctions lists, PEP lists, internal watch-lists and other higher risk categories such as crime and terrorism.



3.3.5 As shown at Fig. 2 above, the screening filters used by banks at the point of customer take-on performed relatively well, albeit not perfectly, with all banks achieving a match rate of 70% or above against the screening list and three-quarters of the banks achieving a match rate exceeding 90%.

3.3.6 Where the results tended to diverge was in relation to the four names on the screening list that had been altered to test fuzzy matching arrangements. Banks tended to perform best where either:

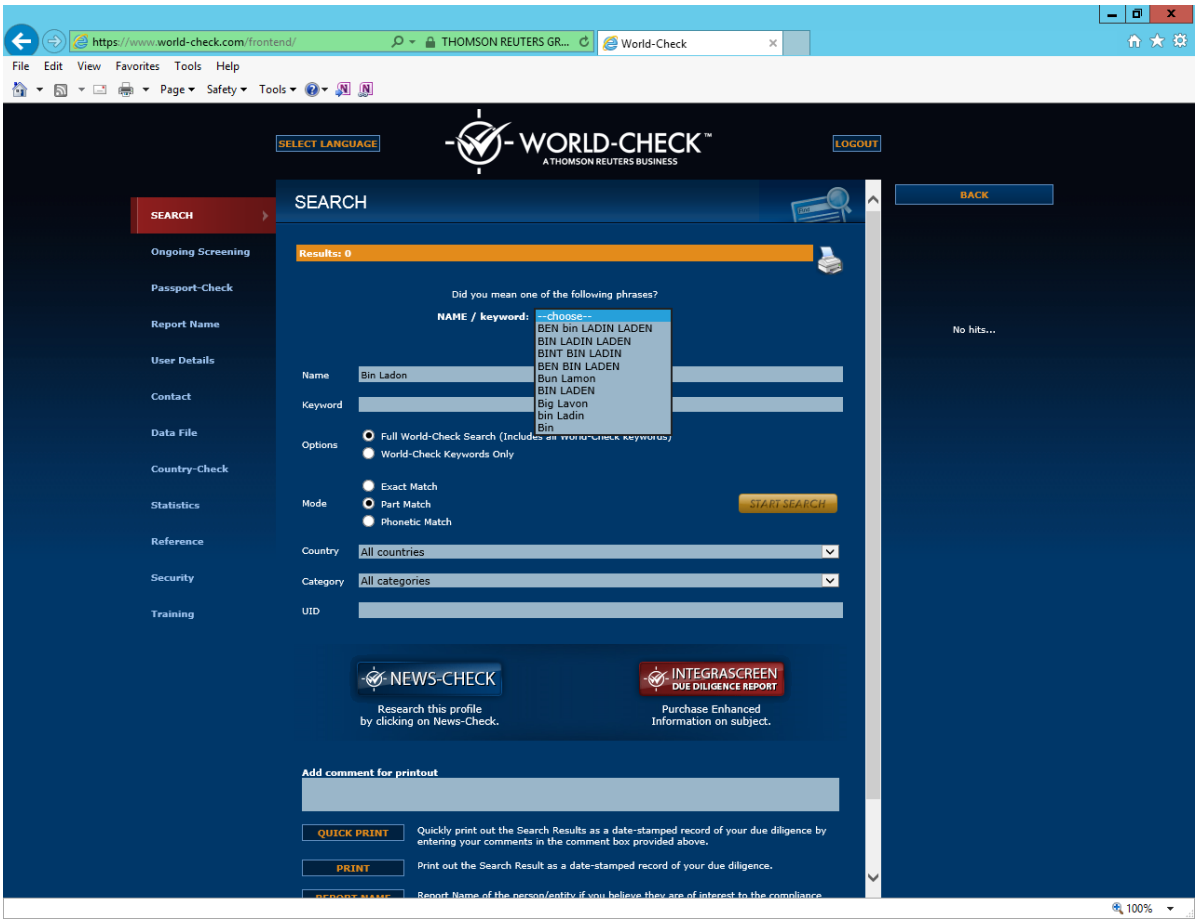
3.3.6.1 the settings within the screening filter were preconfigured and could not be altered by the staff member; or

3.3.6.2 clear guidance had been issued to staff on how a name should be input and which variable settings (e.g. part match, exact match and phonetic match settings) should be used.

3.3.7 The importance of staff procedures was illustrated by the fact that a number of banks produced different results despite using the same commercially available screening filter and that, in some cases, (as illustrated below) staff had failed to recognise that the screening filter was alerting them to a potential match.

(Fig. 3) World-check close matches

A number of the banks examined used World-check at the point of customer take-on. All of the target names on the Commission's screening list were available within World-check; however, some staff were not aware that, in certain circumstances, World-check displays potential target matches in a drop down box at the centre of the screen rather than in the results field on the right hand side of the screen.



Good Practice:

- Customers are screened prior to take-on.
- Screening is undertaken against a comprehensive set of screening lists.
- Associated parties (e.g. directors, beneficial owners) are also screened.
- Staff screening procedures are tailored to the screening filter being used.

Poor practice:

- Only screening the account holder and not associated parties.
- Reliance on a commercially available screening product without a proper understanding of its coverage.
- Inadequate screening guidance given to staff.

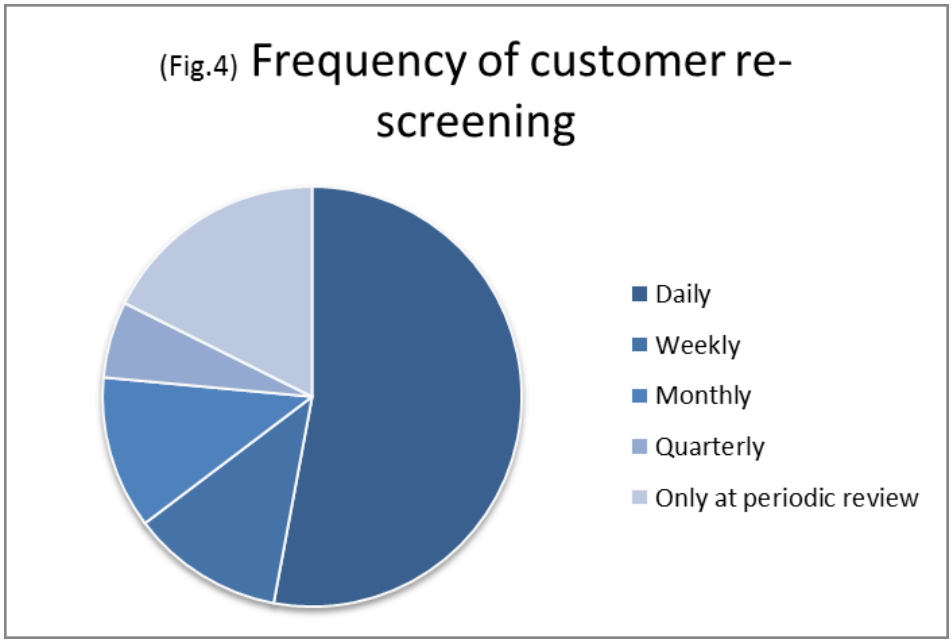
Periodic re-screening of customers

3.3.8 The scope and frequency of periodic re-screening of customers was the most significant point of difference between those banks examined.

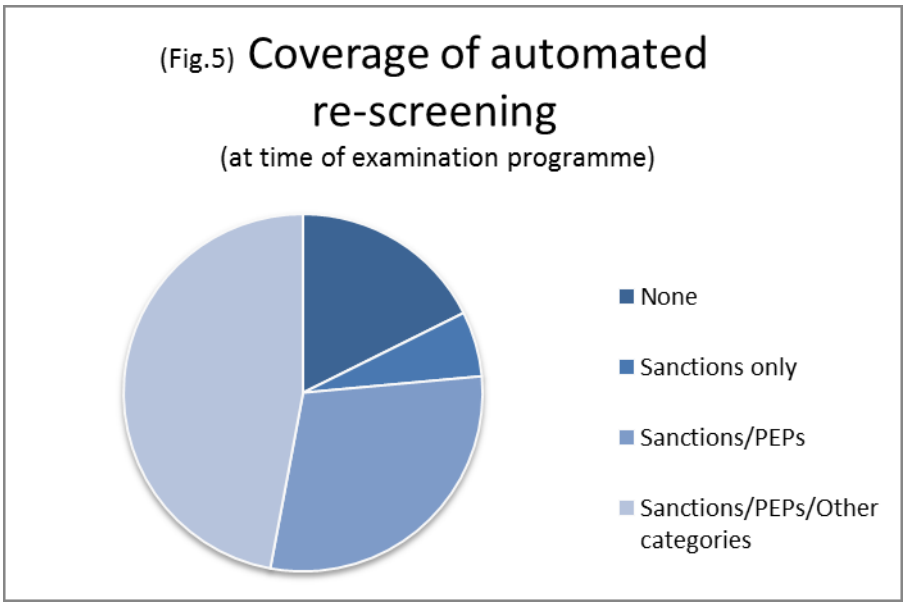
3.3.9 Re-screening of customers is important because banks need to be able to identify when the risks associated with a particular customer have increased. Without a regular programme of re-screening, a bank may find itself in a position of providing facilities

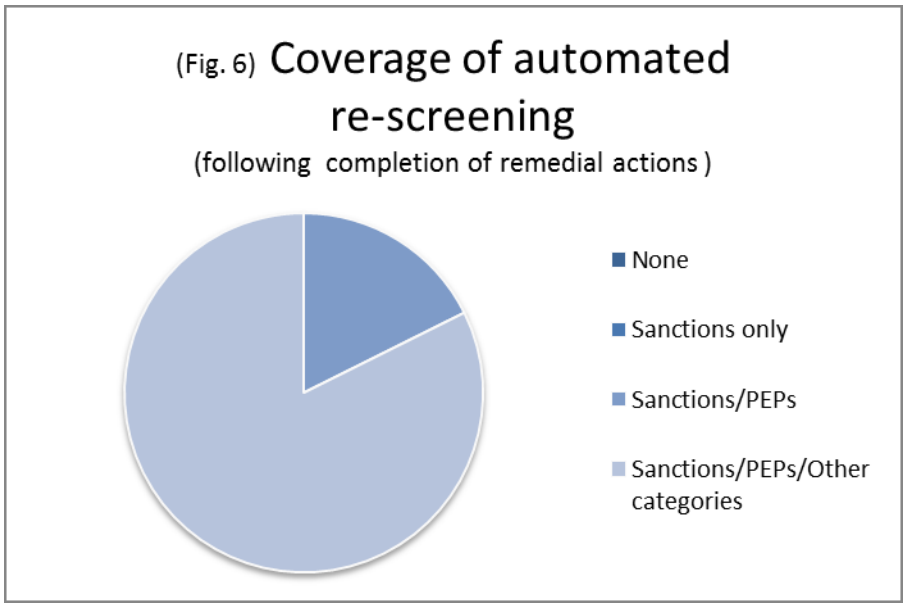
to a customer that is exhibiting higher risk characteristics that warrant enhanced monitoring or, ultimately, represent an unacceptable level of risk to the bank.

3.3.10 In view of the above, the Commission was disappointed to find that three banks had yet to implement any automated re-screening arrangements at the time that they were examined. These banks were reliant on manual re-screening conducted at the time of the customer's periodic review which, in the case of customers assessed to be lower risk, could result in the customer only being re-screened at five-yearly intervals or on a trigger event basis. This approach was regarded as unsatisfactory and all affected banks have now adopted automated re-screening arrangements.



3.3.11 At the other end of the spectrum, best practice involved daily re-screening of all customers and associated parties (e.g. company directors and beneficial owners) against the full range of financial sanctions, PEP and other risk categories used during customer take-on screening. Banks following this approach tended to perform their re-screening on a "delta match" basis whereby the number of false positive matches is reduced by only screening against changes to the relevant screening list and changes to the bank's customer records (e.g. change of customer name).





Good Practice:

- Automated re-screening of the entire customer base and associated parties.
- Re-screening includes some fuzzy matching capacity.
- Re-screening is performed against the same categories that are screened at on-boarding.
- Re-screening is performed daily on a "delta match" basis.

Poor practice:

- No automated re-screening. Reliance on manual re-screening at the periodic review.
- Re-screening is not performed against associated parties.
- Re-screening is performed infrequently against the full customer base resulting in a significant number of false positive matches.

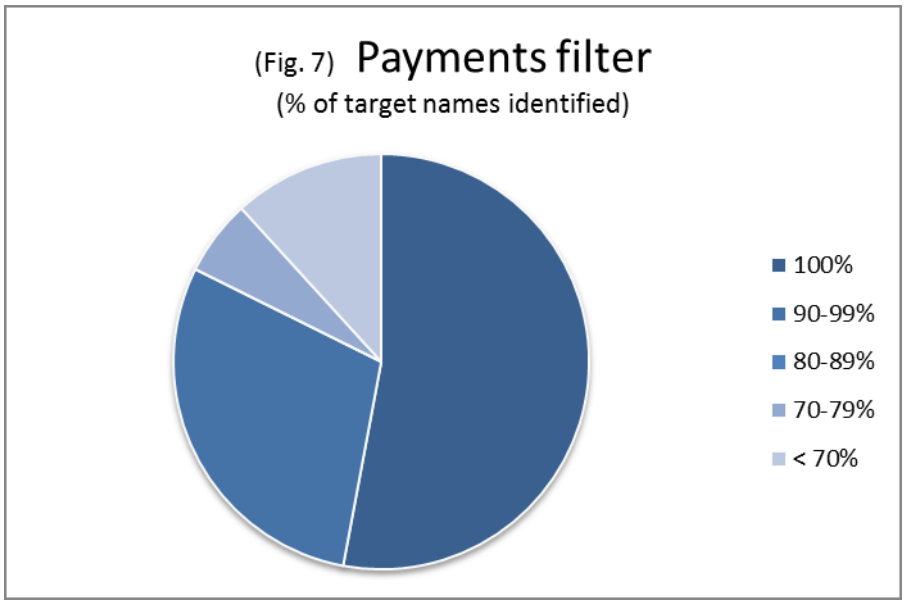
Screening of transactions

3.3.12 Transaction screening is the process by which banks identify whether a payment is being made to, or for the benefit of, a person that may be subject to financial sanctions or have other higher risk characteristics. Those banks examined were asked to pass the screening list provided by the Commission through their inbound and outbound payments screening filters and present the results for analysis.

3.3.13 Transaction screening arrangements were found to be relatively consistent, with banks focussing their efforts on screening SWIFT messages to identify financial sanctions target names. A number of banks had taken a risk based decision to not conduct screening of other transaction types (e.g. BACS and cheques) and in such cases the Commission recommended that the bank document its rationale for doing so in its BRA.

3.3.14 The screening results against payment filters are shown at Fig. 7 and were found to be of good quality overall, with 14 of the 17 banks examined achieving a match rate in excess of 90% against the relevant names on the screening list.

3.3.15 That said, the screening exercise served to highlight two cases where the screening arrangements were found to be materially deficient. In one case, a screening filter used by the bank did not link to one of the key financial sanctions lists. Whilst the gap was partly mitigated by a secondary screening filter used by the bank, some vulnerability remained. The second case involved under-performance of the screening filter as a result of a software update and is discussed in more detail at section 3.6.



Good Practice:

- Transaction screening arrangements are properly understood by local management and documented in the BRA.
- Screening is applied to all relevant SWIFT message fields.
- Screening arrangements and fuzzy matching calibration are subject to regular review.

Poor practice:

- Reliance on group systems without a proper understanding of the coverage provided.
- Excluding certain transaction types from screening without a documented rationale.
- Excluding screening against certain financial sanctions lists without a documented rationale.

3.4 Fuzzy matching arrangements

3.4.1 Fuzzy matching refers to techniques used to identify names that do not precisely match a target name but are still potentially relevant. By way of example, fuzzy matching arrangements can be used to identify the following variations:

Variation	Example
Different spelling of names	"Jon" instead of "John" "Abdul" instead of "Abdel"
Name reversal	"Adam, John Smith" instead of "Smith, John Adam"
Shortened names	"Bill" instead of "William"

Insertion/removal of punctuation and spaces	"Global Industries Inc" instead of "Global-Industries, Inc."
Name variations	"Chang" instead of "Jang"

3.4.2 The screening list provided to banks included four names that had been altered to test fuzzy matching arrangements as follows.

3.4.2.1 Name reversal;

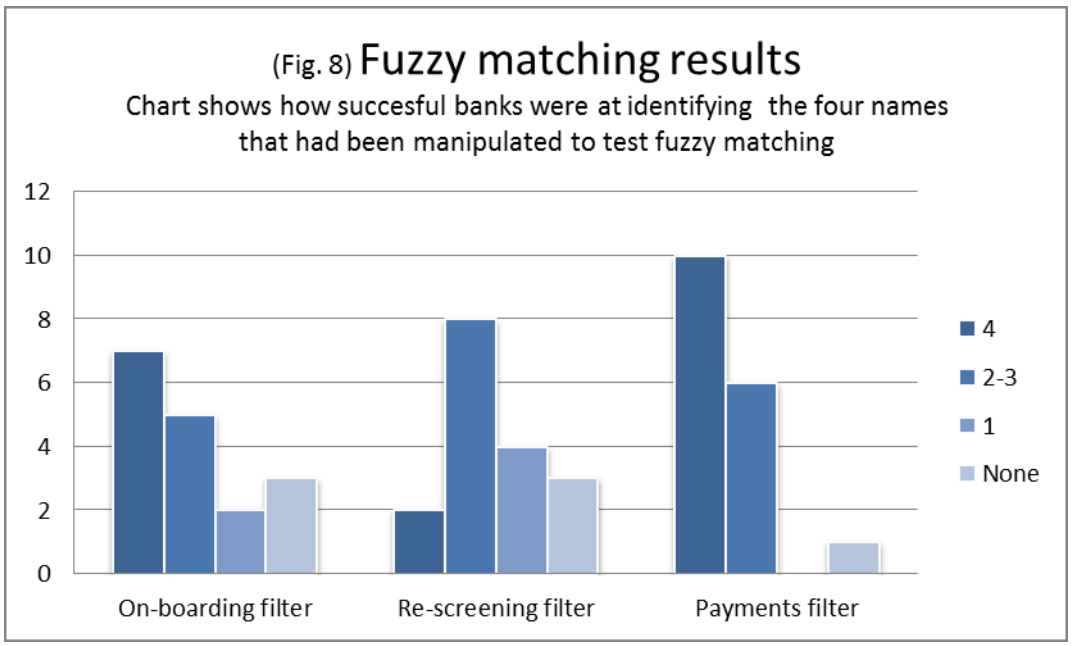
3.4.2.2 Removal of punctuation;

3.4.2.3 Spelling variations; and

3.4.2.4 Abbreviations e.g. "Ltd" instead of "Limited."

3.4.3 The summary results from this test are set out at Fig 8. The results indicated that banks were most successful at identifying name variations when using their payments screening filter, with the on-boarding filter ranking second and the re-screening filter tending to be the least successful. This result was predictable as banks tended to calibrate the fuzzy matching on their payments filters to generate a wider range of potential matches, given that payment details may include names that are not customers of the bank and have therefore not been subject to verification against identification records.

3.4.4 By contrast, re-screening filters tended to be calibrated to produce fewer potential matches given that the bank is searching against existing customers and can therefore have a greater degree of confidence in the accuracy of its customer records. Whilst this logic is understandable, it is important that banks take into account the structure and quality of their customer data as this may vary from one database to another, warranting different fuzzy matching calibration levels.



3.4.5 One of the key learning points from this exercise was for local management to gain an understanding of what fuzzy matching techniques are used by the bank. By having some knowledge of this, local management are better placed to assess the quality of alerts generated by screening systems and contribute to considerations around their optimum calibration.

Good Practice:

- Fuzzy matching arrangements are understood by local management and subject to regular review.
- Fuzzy matching calibration is driven by risk considerations, rather than resources.
- The quality of customer records is taken into account when calibrating fuzzy matching.

Poor practice:

- Reliance on "factory settings", without a proper understanding of the coverage provided.
- Focussing on the quantity, rather than the quality, of fuzzy matching results.

3.5 Dealing with potential target name matches

3.5.1 All screening systems generate alerts which need to be evaluated by the bank and either escalated for further review or discounted as false positives. The evaluation process can be challenging for banks as they will often need to assess a high volume of alerts within a payment processing deadline and it is therefore vital that staff performing this work have appropriate training, guidance and oversight.

3.5.2 As part of its on-site examinations, the Commission was provided with the relevant procedures used by staff and undertook sample testing of recent alerts.

Procedures for discounting alerts

3.5.3 In practice, the vast majority of alerts generated by screening systems are found to be false positives and can therefore be discounted. However, in assessing the validity of an alert, it is important that staff apply a consistent set of criteria and that any marginal alerts are escalated for further review at an appropriate level.

3.5.4 Those banks that performed best in this area had a clearly documented procedure for staff to follow, setting out in what circumstances an alert could be discounted as a false positive. The procedures also required that a rationale be recorded when discounting the alert (sometimes by way of a code selected from a drop down box) in order to provide an audit trail for later review.

3.5.5 Those banks that performed less well tended to provide an inappropriate level of discretion to staff, with only the most obvious matches being subject to secondary review. Where a rationale had been recorded, it tended to be non-specific (e.g. "not

our customer") and would therefore not provide a reliable audit trail or a useful basis for quality assurance testing.

Dealing with customers

3.5.6 Dealing with customers that have had their transactions delayed or their assets blocked represents a challenge for staff and potential risks for the bank. Where there is a suspicion of money laundering, the bank is subject to "tipping off" provisions and must therefore manage its communications very carefully.

3.5.7 Tipping off provisions do not apply to financial sanctions alerts and communication can therefore be more direct but will still need to be handled at an appropriately senior level. In light of this, the Commission recommended that a number of banks establish guidelines for staff to use when communicating with customers that have been subject to alerts.

3.5.8 Most of the banks examined recognised these risks and had made arrangements for any un-discounted target name matches to be escalated to the Compliance department, which would then communicate with the customer, as necessary.

Terms and conditions

3.5.9 Some banks place a standard clause in their terms and conditions, allowing them to delay or defer a payment instruction, pending investigation. Whilst most of the banks examined felt that their existing terms and conditions would allow for such a delay, the Commission recommended that some banks make this more explicit in order to comply with the requirement to be transparent with customers under the Banking Codes.

Good Practice:

- Staff procedures set out the criteria under which target name matches can be discounted.
- Staff are prompted to consider revising the customer's risk rating and filing a suspicious activity report following a target name match.
- Staff are given guidance on how to communicate with customers that are subject to a target name match.
- Customer terms and conditions allow for the delay or deferral of a payment, pending investigation .

Poor practice:

- No rationale is recorded when discounting a target name match.
- The investigation of alerts is not subject to regular sample testing.
- Terms and conditions that fail to adequately protect the bank from consequential loss claims arising from delayed or blocked payments resulting from screening and subsequent investigation processes.

3.6 IT governance

3.6.1 It is a requirement under the Banking Codes that deposit-takers have "adequate procedures in place for controlling changes to systems and records to ensure that only valid changes are made to such systems and records."

3.6.2 Given the degree of reliance on automated screening and monitoring arrangements, it is crucial that banks maintain appropriate IT governance to ensure that any changes made to their systems are properly authorised and have been assessed by staff with relevant expertise. An unauthorised or ill-judged change to these systems could expose the bank (and in turn the Island) to significant reputational risk.

User access and change control

3.6.3 The Commission examined the extent to which banks had restricted the ability of their staff to make modifications to screening and monitoring arrangements and, where such access had been granted, whether appropriate "four eyes" approval processes or detective controls existed.

3.6.4 Whilst the ability to effect such changes was typically restricted to relevant staff, the Commission found that, in a number of cases, banks had not implemented measures to oversee such changes and would not therefore be aware that a change had been made.

3.6.5 These considerations also apply to key elements of static data on which screening and monitoring systems rely. By way of example, a number of banks had implemented a risk based approach to transaction monitoring, whereby the customer's risk rating is used to determine the nature of the transaction monitoring applied to the customer's accounts. In such cases, it is important to consider what four-eyes or detective controls are in place in respect of changes made to the customer's risk rating in the bank's static data, as an accidental, or incorrect, change could result in the bank's transaction monitoring process being subverted.

Post implementation testing

3.6.6 It is quite understandable that banks will wish to calibrate their screening systems so as to improve the quality of the results generated and reduce the amount of staff time spent pursuing false positive matches. When considering such changes, it is crucial that banks conduct a proper assessment of the risks and that adequate testing is undertaken by appropriately qualified staff.

3.6.7 In one case identified as part of this thematic review, a bank had implemented changes to a third-party supplied screening filter at the suggestion of the supplier, in order to reduce the number of false positive matches being produced. The changes were approved by the bank's Compliance department and were not subject to pre and post implementation testing by IT specialists within the bank. It was subsequently identified that the change had been applied in a way that would have potentially resulted in positive matches being ignored by the screening filter. This led to a significant remediation exercise for the bank and subsequent Internal Audit assurance testing.

Good Practice:

- Access to key systems and static data is subject to appropriate user access controls and changes are subject to appropriate four-eyes and/or detective controls.
- Changes to key screening and monitoring systems are subject to proper risk assessment and IT governance arrangements.

Poor practice:

- Lack of controls over key systems.
- Making changes in order to eliminate false positive matches without proper risk assessment and testing.

3.7 Outsourcing

3.7.1 A significant proportion of the banks examined had outsourced elements of their customer screening and monitoring arrangements to specialised centres within their own group. In some cases, these arrangements included the screening of customers at take-on, as well as the initial assessment of alerts generated through the screening of existing customers and transactions.

3.7.2 The Commission found that these arrangements were largely working as intended and that the Commission's Policy and Guidance Note on Outsourcing had been properly observed. Where the Commission did have findings and observations in this area, it tended to be around the lack of sufficient quality assurance testing conducted by, or on behalf of, the Jersey based business. Whilst the outsourced function tended to be subject to quality assurance testing by the parent group, the sampling did not always provide sufficient coverage of work performed on behalf of the Jersey business.

3.7.3 A further point worth emphasising is that any outsourcing agreement should require that any further sub-delegation of responsibility by the outsourcee is subject to prior notification and approval.

Good Practice:

- Outsourcing is undertaken in accordance with the Commission's Policy and Guidance Note on Outsourcing.
- Regular reporting against agreed performance targets.
- Regular quality assurance testing.

Poor practice:

- Local management do not have a clear understanding of what work is being performed on their behalf.
- Over-reliance on group quality assurance testing.

4 AML/CFT and financial sanctions – Consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Governance – Senior Management awareness	
Senior management have sufficient awareness of the workings of group screening and monitoring systems to determine whether they adequately address risks faced by the local business. There is a mechanism by which local management are made aware of material changes to group systems so as to be able to raise objections or, where necessary, adopt alternative mitigating controls. Local management receive ongoing information on the performance of screening and monitoring tools.	Senior management place blind reliance on group systems. Senior management are not in a position to oversee the performance of screening and monitoring arrangements.
Governance – AML/CFT Business Risk Assessment	
The BRA should include coverage of financial sanctions risks. Screening and monitoring arrangements should be properly documented in the BRA so as to allow management to assess whether they provide an acceptable level of risk mitigation. Accepted risks should be documented in the BRA, together with the accompanying rationale.	Failing to consider financial sanctions risks. Lack of detail on the workings of screening and monitoring arrangements.
Staff training and awareness	
Testing to monitor the effectiveness of training. Regular financial sanctions training and awareness programmes that are relevant for the staff member's role. Proper communication of changes to relevant policies and procedures. Ongoing monitoring of staff to identify where there may be a training need.	Training does not address financial sanctions risks. Lack of specialist training for relevant staff.

Examples of good practice	Examples of poor practice
Customer screening – Screening at customer take-on	
Customers are screened prior to take-on. Screening is undertaken against a comprehensive set of screening lists. Associated parties (e.g. directors, beneficial owners) are also screened. Staff screening procedures are tailored to the screening filter being used.	Inadequate screening guidance given to staff. Only screening the account holder and not associated parties. Reliance on a third party screening product without a proper understanding of its coverage.
Customer screening – Periodic re-screening of customers	
Automated re-screening of the entire customer base and associated parties. Re-screening includes some fuzzy matching capacity. Re-screening is performed against the same categories that are screened at on-boarding. Re-screening is performed daily on a "delta match" basis.	No automated re-screening. Reliance on manual re-screening at the periodic review. Re-screening is not performed against associated parties. Re-screening is performed infrequently against the full customer base rather than on a "delta match" basis, resulting in a significant number of false positive matches.
Customer screening – Screening of transactions	
Transaction screening arrangements are properly understood by local management and documented in the BRA. Screening is applied to all relevant SWIFT message fields. Screening arrangements and fuzzy matching calibration are subject to regular review.	Reliance on group systems without a proper understanding of the coverage provided. Excluding certain transaction types from screening without a documented rationale. Excluding screening against certain financial sanctions lists without a documented rationale.
Customer screening – Fuzzy matching arrangements	
Fuzzy matching arrangements are understood by local management and subject to regular review. Fuzzy matching calibration is driven by risk considerations, rather than resources. The quality of customer records is taken into account when calibrating fuzzy matching.	Reliance on "factory settings", without a proper understanding of the coverage provided. Focussing on the quantity, rather than the quality, of fuzzy matching results.

Examples of good practice	Examples of poor practice
Dealing with potential target name matches	
Staff procedures set out the criteria under which target name matches can be discounted. Staff are prompted to consider revising the customer's risk rating and/or filing a suspicious activity report following a target name match. Staff are given guidance on how to communicate with customers that are subject to a target name match. Customer terms and conditions allow for the delay or deferral of a payment, pending investigation.	No rationale is recorded when discounting a target name match. The investigation of alerts is not subject to regular sample testing. Terms and conditions that fail to adequately protect the bank from consequential loss claims arising from delayed or blocked payments resulting from screening and subsequent investigation processes.
IT governance	
Access to key systems and static data is subject to appropriate user access controls and changes are subject to appropriate four-eyes and/or detective controls. Changes to key screening and monitoring systems are subject to proper risk assessment and IT governance arrangements.	Lack of controls over key systems. Making changes in order to eliminate false positive matches without proper risk assessment and testing.
Outsourcing	
Outsourcing is undertaken in accordance with the Commission's Policy and Guidance Note on Outsourcing. Regular reporting against agreed performance targets. Regular quality assurance testing.	Local management do not have a clear understanding of what work is being performed on their behalf. Over-reliance on group quality assurance testing.

ACKNOWLEDGEMENTS AND FURTHER READING

The Commission wishes to thank those banks that participated in this exercise for their co-operation and assistance.

Persons wishing to gain a further insight into this topic may wish to view the following publications:

- Jersey Financial Services Commission, Financial Sanctions – Practical Guidance, Jan 2011, http://www.jerseyfsc.org/pdf/Financial_Sanctions_Practical_Guidance.pdf
- The Financial Services Authority, ***Financial services firms' approach to UK financial sanctions***, April 2009, http://www.fsa.gov.uk/pubs/other/sanctions_final_report.pdf
- The Financial Services Authority, ***Banks' management of high money-laundering risk situations***, January 2011, http://www.fca.org.uk/static/documents/fsa-aml-final-report.pdf

The Commission would welcome comments on any of the contents of this report and would also be happy to address any concerns or questions that the reader may have in this respect. Any such communications should be addressed to the relevant Supervision Manager or, where this does not apply, to:

Darren Boschat
Deputy Director, Banking

Tel: +44 (1534) 822060
E-mail: d.boschat@jerseyfsc.org