Money Laundering Theme – International Banking Cluster

Executive summary

This note summarises the results of the International Banking Cluster. This is one of the projects recommended by our July 2001 report entitled ‘Money Laundering – Tackling our New Responsibilities’.

That report identified a number of "clusters of activities" which are particularly vulnerable to money laundering. It highlighted International Banking as one such cluster.

We found that while some firms met legal and regulatory requirements and good practice standards, a number fell short. In some cases the deficiencies were sufficiently material for us to refer the matter to our Enforcement Division in line with normal practices, while others were addressed through remedial action agreed between banks and the FSA.

The most common shortcomings related to identity verification, including inadequate documentation, and a failure to identify the ultimate beneficial owners and controllers of corporate clients. In addition, anti-money laundering systems and controls for correspondent banking activities were widely found to be inadequate.

Introduction

Reducing the extent to which regulated firms may be used in connection with financial crime, including money laundering, is one of our statutory objectives. Our report of July 2001 entitled 'Money Laundering – Tackling our New Responsibilities' identified a number of clusters which were particularly vulnerable to money laundering. One of the clusters identified was International Banking, which was highlighted by our investigation into banks that handled money linked to General Abacha and includes banks with direct involvement in non-Financial Action Task Force (FATF) markets.

The International Banking project's focus was a programme of visits by our Deposit Takers, Major Financial Groups and Investment Firms Divisions between December 2001 and October 2002. These Divisions visited a sample of approximately twenty international banks that we identified as being at risk of money laundering.

Our findings are grouped under three headings:
- Know Your Customer (KYC);
- transaction monitoring & know your business; and
- other anti-money laundering controls.

Comments on good practice or compliance with our Money Laundering Rules are made where appropriate. Our next steps are set out at the end of the report.

Detailed findings:

(I) Know Your Customer

Account opening

The nature of identity verification documentation obtained for clients varied significantly between banks. Relevant factors appear to include the size of the UK operation and the diversity of banks' client bases.

Some banks are adopting the good practice of following a risk-based approach to client identification and KYC. This means the degree of due diligence performed on prospective clients is aligned to the level of money laundering risk. For example, banks may carry out additional checks on clients from high-risk jurisdictions or on those engaging in activities that are perceived to be vulnerable to money laundering. Our review also identified that some banks update KYC information regularly, for example through monitoring for ownership and directorship changes or to ensure clients continue to be regulated or publicly listed.

Most small banks and some larger ones exhibited weaknesses in account opening procedures. Common failings included:

- personal customer identity or address documentation held on file fall below Joint Money Laundering Steering Committee (JMLSG) Guidance Notes' standards;

- identity and address documentation obtained for the directors and signatories of corporate accounts held on file fall below JMLSG Guidance Notes' standards;
- beneficial owners of high-risk corporate accounts are not always identified;
- the document (e.g. utility bill or bank statement) used to verify an address is not recent;
- faxed copies of documents are accepted as original; and
- photocopied documents are not always certified to confirm that the originals have been seen.

Identifying current customers

Some international banks have already conducted comprehensive reviews of customer accounts. They have also sought to obtain identity verification documentation for all customers, including those that opened their accounts before the introduction of the Money Laundering Regulations in 1994. Others have examined the KYC documentation they have on file and have begun preparations for a risk-based exercise to update it.

We are reviewing the information, provided by and for banks and other firms, about the implications of a proposed amendment to our Handbook in this area. In particular, we are analysing the potential costs of any rule change and the implications of using various key 'filters' to minimise the number of customers for whom action to identify might be required.

Correspondent banking

The JMLSG Guidance Notes recommend that transactions conducted through correspondent relationships need to be managed taking a risk-based approach. However, many banks visited did little to investigate the background and controls of their correspondent banks. Common weakness included:

- no procedures in place to identify the beneficial ownership of correspondent banks, including those domiciled in NCCT or weak regulatory environments;
- international remittances made from the bank's parent to beneficiaries around the world are executed without identifying the underlying clients; and
- although some banks investigate the money laundering regulatory environment of their correspondent banks' country of domicile, others only confirm that there are controls and legislation in place. They do not obtain any assurance as to the substance of the controls or whether they are equivalent to UK requirements.

We have previously highlighted the need for adequate controls in relation to correspondent banking business and expect banks to review their procedures in this area as a matter of urgency.

Cross-border bookings

Some banks who conduct business relationships with clients in the UK but book transactions relating to these relationships to overseas legal entities, for example for settlement or accounting purposes, do not perform money laundering verification checks on these clients. These business relationships may cover cross-border advisory services, the operation of a global trading book by teams located in different jurisdictions, or reflect the centralisation of settlement processes for clients whose relationship is managed from more than one location.

Regardless of where a transaction is to be booked, if a client proposes to carry out 'relevant regulated activities' as defined by our Money Laundering sourcebook, the bank should perform checks on the client in line with UK requirements.

Group introductions

For identity verification purposes, some banks rely on introductions from other group companies located in non-EU jurisdictions without gaining adequate assurance that the records available are consistent with UK requirements.

The JMLSG Guidance Notes state that copies of the identification evidence, certified by a senior manager of the firm, should accompany the introduction certificate if:

- the group introducer is not subject to anti-money laundering legislation and regulations that are at least equivalent to that required by the European Directive, and
- no group procedures exist that require identification and record keeping to UK standards.

Identification of complex offshore entities

Some banks do not go far enough to identify the ultimate beneficial owners and controllers of offshore corporate clients that are part of complex or relatively opaque organisation structures.

Banks' money laundering verification work relating to these types of client often results in intermediate but not ultimate owners being identified. In some cases, this reflects misunderstandings over the level at which identity verification checks should be performed within clients' organisational structures, rather than an inability to obtain the required documentation.

(II) Transaction monitoring & know your business

Transaction monitoring

For banks in the cluster exercise, reliance upon staff vigilance, supported by effective training and awareness programmes, remains the most important and effective tool for monitoring transactions and detecting suspicious activity on client accounts. There is, however, considerable divergence in the use and standard of monitoring procedures.

Transaction monitoring is an area of interest to us and we are considering issuing a Discussion Paper on this subject. However, firms are reminded that our Senior management arrangements, Systems and Controls sourcebook currently requires a firm to "take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime".

Our work established that some firms found monitoring of some business activities, such as the provision of cross-border payment services for small corporate clients, was enhanced by introducing straightforward monitoring systems. This was done, for example, by applying basic filters to standard reports that allow staff to review transactions.

Some large international banks are investigating whether to introduce more sophisticated transaction monitoring systems with dedicated support teams, and some have firm plans to introduce these, but it is too early to assess their effectiveness.

Many firms now have procedures in place for checking international payments against Office of Foreign Assets Control and Bank of England sanctions lists.

Know your business

We identified differing practices on maintaining information on customer files to document the nature of clients' business. Such documentation could cover the purpose of the account, the expected pattern of transactions across the account, the origin of funds to be deposited and the wealth and employment of customers.

We are considering whether firms, even if they have adequate information on the identity of their clients, may not be able to identify suspicious transactions in their accounts because they lack information about their customers' business. The issue of whether current requirements are sufficient to allow firms to understand the source of some, or all, of their customers' wealth and their account behaviour also arose in the Retail Banking Cluster. The Discussion Paper noted above would also cover this area.

(III) Other anti-money laundering controls

Training

Although many of the banks have well-developed programmes, we found that training of staff on anti-money laundering policies, procedures and controls in some banks was not compliant with our Money Laundering rules. Some smaller banks did not have a formal training programme at all.

Banks should have procedures to ensure that all relevant staff have appropriate money laundering training at least every two years, in line with our Money Laundering sourcebook.

Some banks have not introduced training programmes to raise staff knowledge and awareness of the UK's Proceeds of Crime Act (POCA). This deficiency needs to be dealt with as a priority in view of the requirements of POCA.

Internal audit

We identified shortcomings in the internal audit function at many smaller banks. Group internal auditors often did not have a full grasp of UK anti-money laundering issues, nor did they demonstrate an adequate understanding of the Money Laundering sourcebook. At some small banks, the compliance officers' duties incorporate not only that of the Money Laundering Reporting Officer (MLRO) but also internal audit responsibilities.

Firms are reminded that the Approved Persons chapter of our Supervision Manual states that, depending on the scale, nature and complexity of its business, it may be appropriate for a firm to have a separate audit function. Our Senior management arrangements, Systems and Controls sourcebook also requires an internal audit function to be independent of the day-to-day activities of the firm.

Where it is not appropriate to separate the function of MLRO from that of the internal auditor, some banks put in place head office oversight to maintain an effective internal audit regime and ensure that auditors from head office are familiar with UK requirements. In addition, some banks develop risk-based audit programmes which review anti-money laundering systems and controls across support functions and product or business lines.

Money Laundering Reporting Officer

We found that MLROs are able to conduct their duties most effectively when they have sufficient access to and support from senior management to implement adequate anti-money laundering systems and controls.

It is common practice for staff to discuss potential suspicious transaction referrals with their line management before providing the details to the MLRO. However firms should ensure that this consultative process does not hinder or prevent staff from discharging their obligations to report suspicions to the MLRO under our Money Laundering sourcebook. There should be no 'barriers' preventing staff from reporting suspicion referrals to MLROs.

At some banks, departments which do not report directly to the MLRO are responsible for the day-to-day operation of account opening and other anti-money laundering processes. While this may be appropriate for the nature of the business, firms are reminded that our Money Laundering sourcebook includes Guidance that the MLRO should act as the focal point for the oversight of all activity relating to anti-money laundering within a firm.

Next steps

In the light of this report, we shall now write to the CEOs of international banks with UK operations asking them to assess their systems and controls in the areas discussed in this paper and confirm, if applicable, where remedial action is being taken to address any weaknesses. Over the next year, we will follow this up with further visits, focussing on the weaknesses identified in this project. We will target these towards those firms seen as high risk or those whom we believe have failed to take remedial action.