Financial Conduct Authority

Thematic Review TR14/16

How small banks manage money laundering and sanctions risk

Update

November 2014

Contents

Abbreviations used in this report

AML	Anti-money Laundering
CTF	Counter-terrorist Financing
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FSA	Financial Services Authority
JMLSG	Joint Money Laundering Steering Group
PEP	Politically Exposed Person
MI	Management Information
MLRs	Money Laundering Regulations 2007
MLRO	Money Laundering Reporting Officer
RM	Relationship Manager

1. Overview

Introduction

In 2010/11, the Financial Services Authority (FSA) reviewed 27 banks to assess their anti-money laundering (AML) systems and controls in high-risk situations (the 2011 AML review). This included their dealings with politically exposed persons (PEPs), correspondent banks, and wire transfers. The FSA found significant weaknesses in banks' AML systems and controls, and in particular, how they were managing high-risk and PEP customer relationships. The FSA published its findings in June 2011.[1]

Following the 2011 AML review, we took enforcement action against five banks[2] for failing to manage money laundering risk adequately. We have also published regulatory guidance, Financial Crime: a guide for firms[3], which sets out how firms can manage the money laundering risk in their business.

This thematic review is a follow-up to the 2011 AML review.[4] The objective was to assess the extent to which our actions have affected the quality of AML systems and controls in smaller banks.[5] Given the 2011 AML review findings, we focused on high-risk customers, PEPs, and correspondent banking. We also considered the adequacy of financial sanctions (sanctions) systems and controls[6], as previous FSA thematic work published in 2009 found weaknesses here, particularly among small firms. We did not review banks' wire transfer controls as no major weaknesses were found in this area during the 2011 AML review.

Legal and regulatory obligations

Banks' legal and regulatory AML obligations are set out in the Money Laundering Regulations 2007 (MLRs), the EC Wire Transfer Regulation[7], the Proceeds of Crime Act 2002, and the FCA's Handbook. Banks are also subject to the various pieces of legislation that implement the UK's financial sanctions regime.

1 http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf.

2 Coutts & Company (2012), Turkish Bank (UK) Ltd (2012), EFG Private Bank (2013), Guaranty Trust Bank (2013), Standard Bank Plc (2014).

3 http://fshandbook.info/FS/html/handbook/FC/link/PDF.

4 We also conducted a follow up to our previous report on anti-bribery and corruption controls in commercial insurance broking and have published a report here.

5 Our Systematic AML Programme assesses AML controls in major retail and investment banks separately. We have also begun a programme of regular visits to firms of all sizes (subject to the MLRs) which may be exposed to higher levels of money laundering risk.

6 http://www.fca.org.uk/static/fca/documents/fsa-sanctions-final-report.pdf.

7 Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.

Throughout this review, we have also had regard to our regulatory guidance, Financial crime: a guide for firms, and relevant provisions in the Joint Money Laundering Steering Group's guidance (the JMLSG Guidance).

What we did

We visited 21 smaller banks between October 2013 and June 2014 to assess their AML and sanctions systems and controls. We considered how they had used our regulatory guidance, the 2011 AML review, and enforcement action to inform their approach. Five of the banks visited were part of the 2011 AML review and the others were selected from the remaining population of smaller banks. In total, we visited eight wealth management/private banks, seven wholesale banks, and six retail banks.

Key messages

We found that some retail, wholesale, and private banks had implemented effective AML/sanctions controls, with private banks generally operating to higher standards. For example, some banks demonstrated good senior management engagement on AML, a good understanding of financial crime risk among key staff, close oversight of high risk customer relationships, and an effective use of enhanced due diligence (EDD) as a basis for identifying potentially suspicious activity. This shows it is possible and achievable for small banks to manage their business in line with legal and regulatory AML requirements.

However, given the amount of work we have carried out on AML in recent years, we were disappointed to find continuing weaknesses in most small banks' AML systems and controls. In particular:

- We continued to find significant and widespread weaknesses in key AML controls, including AML risk assessments at both a business and customer level, and EDD and ongoing-monitoring of high risk, PEP, and correspondent relationships.

- A third of banks had inadequate AML resources, and staff knowledge and awareness of AML and sanctions risks were often weak. This included – in a quarter of banks – Money Laundering Reporting Officers (MLROs). Following our visits, several banks have decided to replace their MLROs.

- Overseas banks faced particular AML challenges when they relied on other parts of the Group to carry out customer due diligence (CDD) on their behalf. This was because Group policies and procedures were not always consistent with UK legal and regulatory requirements. In addition, the UK Chief Executive position was sometimes a short-term posting from the home country, with little incentive to ensure AML controls met UK standards.

- Despite weaknesses in governance at some banks, we generally saw an improvement in senior management engagement on AML issues compared with the 2011 AML review. However, they had generally been slow to assess their AML systems and controls against our guidance. Three quarters of the banks visited had only taken action to improve their systems and controls since late 2012, often in response to enforcement action against other banks with similar business models.

- Although most banks had an adequate understanding of their obligations under the UK sanctions regime, some had weaknesses in relevant controls. In particular, some banks had decided to exclude certain transaction types from payment screening without first assessing the risk this posed.

Action taken and next steps

We provided individual feedback to each of the banks in our sample. We found particularly serious issues at six banks and, as a result, we have taken the following action:

- Four banks voluntarily agreed to limit their business activities with certain types of high risk customers until they have corrected control weaknesses.

- We required three of these banks to appoint a skilled person under s.166 of the Financial Services and Markets Act 2000 to conduct a more detailed review of the banks' AML and sanctions systems and controls and to make recommendations for improvement. We used this tool mainly where we had previously told banks about weaknesses in their AML controls and they had failed to make adequate improvements.

- The other three banks are conducting remedial work under the guidance of external consultants.

- We have started enforcement investigations into two of the six banks.

We also intend to update our regulatory guidance, Financial crime: a guide for firms, with further examples of good practice in Chapter 3 of this report. As a result of the continued weaknesses in banks' AML controls, we have sought to provide more detailed guidance to help firms implement more effective AML systems and controls. We are consulting on these changes to our guidance here.

2. Findings

Here we set out our collective findings from all the visits conducted. We have illustrated specific examples of the good (highlighted in red) and poor (highlighted in grey) practice we saw at individual firms in the boxes contained in this chapter. We have set out the examples of good practice more fully in Chapter 3.

Governance, culture and management information

We expect senior management to take responsibility for money laundering and sanctions risk management. This includes being aware of the money laundering and sanctions risks to which the firm is exposed and ensuring that these are managed effectively. This is likely to include establishing a strong AML culture, ensuring they receive good quality management information, ensuring control weaknesses are identified and corrected, and allocating adequate resources to manage the risks.

The 2011 AML review found nearly half of banks had a poor AML culture, inadequate management information, and a lack of senior management oversight and involvement in PEP and high-risk customer processes. Although the majority of banks visited during this review showed some improvement in overall governance, we found serious AML governance and oversight weaknesses in six banks, including two that were part of the 2011 AML review.

Governance structures

We expect banks to have a governance structure that is appropriate to the nature, scale, and complexity of their business. We therefore expected to find some variation in the governance structures at smaller banks. Some banks operated management committees that discussed money laundering and sanctions risks, others had a more informal approach to escalating and managing issues. We generally found that senior management at banks with a formal management committee, or other such formal structures, engaged better on AML issues.

Two banks had recently reintroduced a Financial Crime Committee to approve and manage high-risk and PEP customer relationships, improving senior management oversight.

Another bank did not have a dedicated committee to discuss AML issues, but key conversations and decisions between relationship managers (RMs), compliance and senior management were clearly documented and the annual MLRO report was reviewed at a board meeting. Interviews with staff confirmed they had a good understanding of the money laundering risks inherent in their business as well as those posed by individual customers.

We found a third of banks had inadequate AML resources. MLROs were usually approved by the FCA to carry out the compliance function as well as their MLRO role and supporting compliance staff often had additional responsibilities too. This is not a problem in principle, but it was where inadequate AML resources led to inadequate oversight, failure to keep up to date with industry standards, and poorer standards of enhanced due diligence and monitoring. In addition, some banks had failed to consider potential conflicts of interest between the different roles their MLROs carried out. Senior management must ensure that the compliance and AML functions are adequately resourced.

The MLRO and Deputy MLRO at two different banks also acted as the internal auditor. One bank ensured the MLRO did not audit her own function and is now planning to assign the functions to separate individuals. However, the other bank failed to manage this conflict of interest. The Deputy MLRO was responsible for both approving the CDD carried out at on-boarding and auditing customer files to ensure they met legal and regulatory requirements.

Culture and risk appetite

An effective AML and sanctions control framework depends on senior management setting a clear risk appetite and embedding a culture where financial crime – and a failure to control it - is not acceptable. It should also be aligned with their business model and based on a good understanding of the money laundering and sanctions risks to which their bank is exposed. We found the failure to establish a good AML culture correlated strongly to poor overall AML and sanctions systems and controls.

At one overseas bank, insufficient oversight and ownership of money laundering and sanctions risks resulted in senior management and the MLRO being unable to discuss the level of risk the firm was exposed to. This lack of senior management engagement was reflected in significant failings in customer risk assessment, customer due diligence and ongoing monitoring.

We found that banks that were UK branches or subsidiaries of overseas banks tended to adopt the culture and policies and procedures of their Head Office or parent bank. In some cases, this strengthened the banks' AML control framework, but in others the parents' culture and approach were not aligned with UK law and regulation. Consequently, the UK operations risked falling short of their legal and regulatory obligations. We found this risk was exacerbated where the UK Chief Executive position was a short-term posting from the home country, with little incentive to ensure AML controls met UK standards.

One overseas bank maintained a good AML culture, despite the frequent rotation of its UK branch manager. This was due to the commitment of supporting management and the parent bank, which made it clear that AML compliance was a key priority.

In a quarter of banks, senior management failed to articulate the bank's money laundering risk appetite clearly. We found these banks had established relationships with very high-risk customers or high-risk customers who did not fit their normal customer profile, and they were not well placed to manage these risks.

At one private bank, senior management had set a clear risk appetite and took steps to implement it and ensure a good AML culture through everyday decision making and staff communications. RMs could articulate how they applied the bank's risk appetite in practice. They provided examples of customers they would not accept, as well as situations where they had accepted individual customers but a relationship with the customer's business was outside the bank's risk appetite.

Management Information (MI)

Good quality MI provides senior management with oversight of the money laundering and sanctions risks in their business and enables them to manage those risks effectively.

We found that most banks produced MI on AML and sanctions issues on a regular basis. However, at a small number of banks, the only MI produced was the annual MLRO report. In general, we found MLRO reports at smaller banks were of poorer quality than those of larger banks in the 2011 AML review. In this review, many of the reports summarised the bank's legal obligations but did not cover key risks, emerging trends, or the effectiveness of the control framework. This meant that senior management in those banks did not have the information necessary to manage money laundering risk adequately.

The UK branch manager of a foreign bank stated he did not see any AML or sanctions related MI or the MLRO report, despite the MLRO confirming that he always submitted his report to him.

For proposed guidance on governance, culture, and management information please see the relevant heading in Chapter 3.

Risk assessment

Business-wide money laundering risk assessments

Firms must identify and assess money laundering risk. This risk assessment must be comprehensive and proportionate to the nature, scale, and complexity of the firm's activities and it is an important prerequisite for the implementation of risk-sensitive controls. In particular, it should identify high risk parts of the business and help the firm prioritise its resources to combat financial crime.

Over half the banks visited had not assessed the money laundering risk inherent in their business models and appeared to rely solely on individual customer risk assessments. We found these banks often had a very limited understanding of the risk associated with their products, services, and customer base, did not have appropriately risk-based AML controls, and were unable to discuss emerging risks.

At one bank, both senior management and the MLRO were unable to discuss the money laundering and sanctions risks in their business. We were concerned that they intended to open another office with an extended product range but could not accurately assess the extent to which their existing AML controls would mitigate the increased risk.

The banks that did carry out a business-wide risk assessment did so to varying standards. Some adopted an informal approach, allocating risk ratings according to the general perception of money laundering risk. Others conducted a more formal exercise considering a wide range of factors and risks specific to their bank. These banks tended to use the results to inform their wider controls and customer risk assessments more proactively.

One bank conducted an informal business-wide risk assessment, but did not use it to inform the implementation of appropriate controls. It also did not reflect senior management's view of money laundering risk. For example, the risk assessment stated that trade finance was rated medium risk, but senior management told us the risk associated with their trade finance business was high.

Customer money laundering risk assessments

The 2011 AML review found serious weaknesses in banks' risk assessments of individual business relationships. We were disappointed to find that the quality of customer risk assessments is still weak, with over three quarters of banks failing to implement an adequate customer risk assessment[8] process. In fact, only three banks carried out adequate customer risk assessments. This is a particular concern because the risk assessment process should determine the appropriate level of due diligence and ongoing monitoring for each relationship.

One bank had designed a sophisticated risk assessment toolkit, which considered multiple money laundering risk factors. However, the identification of a higher-risk customer did not consistently lead to adequate enhanced due diligence or ongoing risk management.

Many firms considered only country risk and whether a customer was a PEP when identifying high-risk customers. They did not consider other risk factors, such as the products or services sought, the business the customer was involved in, the source of funds used in the business relationship, expected activity, or the impact of any relevant adverse information. Some banks had calibrated their AML risk assessment in such a way that it was virtually impossible for a customer to be classified as high risk unless they were a PEP – an issue we highlighted in the 2011 AML review. This adversely impacted these banks' ability to manage money laundering risk.

We expect banks to take a holistic view of the money laundering risks associated with a business relationship and to ensure there are appropriate and adequate controls to mitigate them; for example, through more frequent monitoring. Banks should record their customer risk assessment and, where the risks are high, the reasons why the bank is content to accept the risk and how it intends to mitigate it.

8 A customer risk assessment includes the consideration of money laundering risk posed by individuals associated with the customer.

A branch of an overseas bank accepted a customer whose ultimate beneficial owner had been charged overseas with 107 counts of money laundering. The board signed off the relationship on the condition that EDD was carried out. However, the file lacked an adequate risk assessment and explanation of how senior management were satisfied that the customer funds were not the proceeds of crime.

Many banks still assessed country risk solely on the basis of Financial Action Task Force (FATF) membership, or FATF's list of countries with strategic deficiencies, and did not consider other useful sources of information.[9] In addition, some banks were not classifying countries as high risk if their Group had a presence there. We highlighted these poor practices in the 2011 AML review.

One bank downgraded a country from high risk to medium risk solely because it moved onto the FATF Grey list from the Dark Grey List. This was despite the fact that inclusion on the Grey list means FATF has identified strategic AML deficiencies in that country.

For proposed guidance on risk assessment please see the relevant heading in Chapter 3.

Customer Due Diligence

In general, we found most banks were adequately identifying and verifying their customers in accordance with their obligations under the MLRs. This is an improvement from the 2011 AML review, where we found deficiencies in identification and verification documentation at a number of banks.

The MLRO at one bank refused to waive UK CDD and EDD requirements despite considerable pressure from its overseas parent bank to speed up the on-boarding process.

We also found that all banks were using commercially-available PEP databases to screen new customers, but some did not conduct risk-sensitive PEP screening of their existing customer base.

Over a quarter of banks failed to capture adequate information on the nature and intended purpose of the customer relationship. This is an important part of the due diligence process and enables effective on-going monitoring of the relationship.

9 Additional public sources of information could include HM Treasury sanctions lists, MoneyVal evaluations, Transparency International Corruption Perception Index, and public information about the quality of regulation.

Enhanced Due Diligence

The central objective of EDD is to enable a bank to better understand the risks associated with a high-risk customer and make a balanced decision of whether to accept or continue the relationship. This information also helps the bank to mitigate identified risks through enhanced on-going monitoring of the business relationship.

In 2011, the FSA found serious weaknesses in the level of EDD carried out on high risk customers and PEPs. It set out its expectations clearly in both the 2011 AML review and subsequent guidance. However, the quality of EDD remained the weakest area for most banks visited in this review, with over three quarters failing to conduct adequate EDD consistently on their high risk relationships.

Many banks struggled to understand what, and how much, EDD information they should collect and how they should use it. Most were not conducting EDD commensurate to the level of money laundering risk posed by the customer. Some banks were not willing to ask for information from prominent PEP customers and were therefore unable to carry out adequate EDD.

Establishing the source of wealth and source of funds was a particular issue despite this being a legal requirement (imposed by the MLRs) when the customer is a PEP and good practice for other high-risk customers. The aim of source of wealth/funds checks is to be reasonably satisfied that the funds used in the relationship are not the proceeds of crime. However, many banks thought that establishing the source of funds meant simply collecting evidence of a bank transfer.

A small private bank had a customer who was publically alleged to have laundered approximately $700m with a known corrupt foreign official. Despite classifying the customer as high risk, the bank only identified this allegation a year into the relationship and still failed to conduct adequate EDD to determine whether the customer's wealth and the funds used in the relationship were legitimate.

Many banks were still failing to identify relevant adverse information through open source media and, where adverse information had been identified, it was often assessed in terms of reputational risk rather than money laundering risk – another issue we highlighted in the 2011 AML review. However, a small number of banks produced detailed and meaningful EDD reports on their higher risk customers – all through publicly available information.

An RM at one bank noted on the file of a high-risk customer that to the best of his knowledge 'there has never been any negative comment about his activities'. We conducted a simple Google search which revealed a report by an African government committee alleging that the customer had been involved in corrupt activity surrounding the privatisation of state-owned companies.

EDD on correspondent banks

The MLRs include specific EDD provisions for non-EEA respondent banks. Half the banks visited had correspondent banking relationships and all but two had correctly identified that EDD

was required for their non-EEA correspondent banking relationships. However, we found the quality of EDD and risk assessment on respondent banks was generally poor. In particular, most banks failed to adequately determine the reputation of the respondent and the quality of its supervision, to fully understand the nature of its business, and to assess their AML and counter-terrorist financing (CTF) controls.

Some banks used an extract, or their own version, of the Wolfsberg Group's Correspondent Banking AML Questionnaire[10] but failed to adequately assess the responses. Nearly all of these questionnaires had been completed with 'yes' or 'no' answers and did not provide adequate qualitative information for banks to be able to assess their AML and CTF controls – an issue we highlighted in the 2011 AML review.

> One bank accepted at face value as statement that a correspondent bank had controls to manage higher-risk customers despite the fact it was also clear in the same questionnaire that the correspondent bank was based in a country with no legislation for EDD and did not have any policies for EDD.

Some banks informed us they visited all of their correspondent banks. However, the visit reports provided did not show that the quality of the respondent's AML control framework had been assessed and instead appeared to show the focus had been on furthering the commercial relationship.

For proposed guidance on enhanced due diligence please see the relevant heading in Chapter 3.

Reliance

Reliance can be a useful and cost-effective way for banks to meet CDD requirements. The MLRs allow banks to rely on another person to carry out any CDD measures, subject to certain conditions. However, the relying bank remains responsible for meeting its obligations under the MLRs. It should therefore be satisfied that the extent of CDD measures applied by the bank being relied upon are commensurate with the money laundering risk and meets the standards the MLRs require. These requirements apply to all banks, whether or not they form part of the same group as the relied-upon bank. The JMLSG has issued detailed guidance on this.[11]

We found that a number of banks relied on other banks to carry out CDD and EDD on their behalf but did not take steps to ascertain whether the due diligence on which they were relying was commensurate with their customer risk assessment. This was a particular concern where the customer was high risk and relying banks were not undertaking any of their own EDD. These banks often did not have enough information to carry out adequate enhanced ongoing monitoring of high-risk relationships and appeared to fall short of the MLRs' requirements.

10 http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Anti-Money-Laundering-Questionnaire-2014.pdf.

11 http://www.jmlsg.org.uk See in particular Part I Chapter 5 Section 5.6.

One bank relied on its overseas parent to conduct CDD and EDD of high-risk relationships without making any of its own enquiries and was unable to produce relevant information during our visit. It was not clear how the bank was able to conduct meaningful monitoring of these business relationships.

Enhanced ongoing monitoring

Firms are required to conduct risk-sensitive ongoing monitoring of their customers, and high-risk customers must be subject to enhanced ongoing monitoring. The 2011 AML review found the majority of firms had ongoing monitoring procedures, but they were not always effective.

Transaction monitoring

Banks must monitor transactions to ensure these are consistent with their knowledge of their customer. Transaction monitoring is integral to the identification of suspicious transactions.

We found smaller banks used a mixture of automated and manual transaction monitoring systems, but we identified weaknesses in the standard of transaction monitoring being undertaken. Some banks failed to establish expected account activity when accounts were opened. This subsequently made it difficult for staff to identify whether transactions were unusual or suspicious. Half the banks in our sample focused solely on identifying large transactions and did not consider any other 'red flags' when assessing the customer's activity. In particular, they did not seek to identify trends or unusual patterns, such as a customer making frequent low-value deposits that collectively exceeded their stated income.

Two banks were incorporating more sophisticated transaction monitoring rules and scenarios into their automated systems. This was to reduce reliance on RMs identifying suspicious transactions.

Some banks set an individual threshold limit for each customer and a transaction was only investigated if it exceeded the threshold. However, this is reliant on thresholds being set at the right level and reviewed on a regular basis to ensure they remain appropriate. We did not see this method working effectively where it was the only form of transaction monitoring carried out.

RMs at the majority of wholesale banks were unable to describe how they conducted manual transaction monitoring of their customer accounts. The MLROs at these banks had not provided them with training on 'red flags' specific to their business.

Periodic reviews

Nearly half the banks visited either did not carry out periodic reviews of their high-risk relationships or had only recently introduced a periodic review process. It was not clear how these firms had been able to manage their money laundering risk effectively and in many cases, firms risked falling short of their obligations under the MLRs.

One bank classified all of its 2,800 customers as high risk and relied on three staff members to carry out all annual reviews. As a result, the reviews were inadequate, focusing solely on account activity.

Another bank, which only decided to introduce annual reviews after our visit, intended for two employees to conduct 1,200 reviews every year in addition to their existing full-time responsibilities.

One private bank carried out annual reviews for all their PEP and high-risk customers. They reassessed the money laundering risk posed by the customer and refreshed existing CDD and EDD information as appropriate.

Another private bank undertook short reviews of its higher-risk customers, as and when the RM spoke to the customer, as well as a more formal annual review.

Where banks carried out periodic reviews, we found standards varied. Some banks failed to update existing EDD (including adverse media searches) or to consider whether the customer risk assessment remained appropriate.

For proposed guidance on enhanced ongoing monitoring please see the relevant heading in Chapter 3.

Sanctions

Most banks had an adequate understanding of their obligations under the UK sanctions regime. However, the adequacy and effectiveness of sanctions controls varied significantly.

We found that responsibility for screening customers and payments against applicable sanctions lists sat with a range of different teams, including compliance, operations, and IT. Where compliance was not responsible, we found a lack of oversight of whether sanctions lists were being kept up to date and quality assurance was weak.

Many banks did not understand how the systems they used had been calibrated and at what thresholds 'fuzzy matching'[12] had been set. We expect banks to understand the systems they use to ensure they mitigate risk as intended.

12 JMLSG suggests 'fuzzy matching' describes any process that identifies non-exact matches. www.jmlsg.org.uk see in particular Part III Chapter 4 Section 4.42.

One bank did not carry out quality assurance work on the effectiveness of its sanctions systems and controls. Compliance was unclear about whether all corporate customers and associated persons were screened by the automated system and the MLRO and Deputy MLRO did not have a consistent view of the scope of the bank's sanctions screening.

Some banks conducted daily automated screening of their customers and associated individuals using fuzzy matching. Others conducted sanctions screening using a system with fuzzy matching at on-boarding but, when sanctions lists were updated, they only conducted a manual search of their customer database without the benefits of fuzzy matching. Banks that carry out this kind of manual customer sanctions screening should consider running their whole customer base through a system with fuzzy matching capabilities periodically so that potential matches are not missed.

Nearly all the banks visited used an automated system to screen payments against sanctions lists. However, some banks were not performing sanctions screening on certain types of transactions, such as direct debits, cheque and debit card payments. It is important for banks to consider the risk of sanctions breaches and decide on an appropriate level of sanctions screening to manage the risk for their bank. Where a bank places reliance on automated sanctions screening undertaken by the receiving bank, it should take steps to ensure it is appropriate to rely. We have already issued guidance in this area, which can be found in Chapter 7 of Financial crime: a guide for firms.

A UK branch of an overseas bank, with a high-risk customer base, performed manual payment screening retrospectively and relied on the time difference between the UK and the payee's country to recall any payments involving sanctioned individuals or entities within a three to four hour window. There are clear deficiencies with this approach.

For proposed guidance on sanctions please see the relevant heading in Chapter 3.

Training and awareness

Banks must ensure they employ staff with the skills, knowledge and expertise to carry out their functions effectively. To help ensure this, banks should provide tailored, practical AML and sanctions training for staff in key roles. The 2011 AML review identified a lack of bespoke training for staff dealing with high-risk customers. This led to staff making poor judgements and failing to manage the money laundering risks to which their bank was exposed.

In this review, we found that, despite most banks providing staff with annual AML and sanctions computer-based training, staff in smaller banks tended to have weaker AML and sanctions knowledge than staff in larger banks. Although there were notable exceptions to this finding, particularly in private banks, we found training at nearly half of banks was ineffective. Staff in important AML roles were often unable to discuss money laundering risk or potential money laundering 'red flags'.

An RM at a branch of an overseas bank failed to identify multiple 'red flags' on the account of a high-risk customer. These included regular loan overpayments with the extra funds subsequently being paid away to a different bank account, changes to the nature and use of the account, and bribery and corruption allegations about the customer, which were published during the course of the relationship.

The level of AML and sanctions knowledge among MLROs in a quarter of banks visited was inadequate. In particular, they did not understand their legal and regulatory responsibilities, money laundering risks, or 'red flags' relevant to their bank. The MLRO is an essential function and a weak MLRO cannot meet their obligation to oversee their bank's AML compliance. We found that MLROs in a quarter of banks had a detrimental effect on the overall standard of AML and sanctions systems and controls in their bank. Following our visits, several banks have decided to replace their MLROs.

At a UK subsidiary of an overseas bank, the MLRO stated he did not see the value in establishing the source of wealth or source of funds for PEP customers, thereby demonstrating a clear lack of understanding of his legal and regulatory obligations.

Action taken by banks in response to the 2011 AML review

Of 21 banks visited in this project, five had been visited during the 2011 AML review. In general, we found there had been slow progress in ensuring AML and sanctions controls were fit for purpose and compliant with legal and regulatory requirements.

Most banks had considered the 2011 AML report and regulatory guidance and some had conducted gap analyses against the Enforcement Notices issued to Coutts & Co, EFG Private Bank, and Guaranty Trust Bank. Three of the five banks visited during the 2011 AML review had considered the issues highlighted in their individual feedback letters and conducted a gap analysis against our guidance. However, one of these banks was still in the process of correcting the issues that had been highlighted. The remaining two banks had not considered our guidance and had not adequately addressed the individual feedback points. We have followed up on these issues with those two banks.

Of the 16 banks the FSA did not visit during the 2011 AML review, nine had carried out, or were in the process of carrying out, remedial work in response to the 2011 AML report and Enforcement Notices. The other six had taken little or no action.

3. Examples of good practice

This chapter summarises examples of good practice we identified during this review. It builds on our regulatory guidance in Financial crime: a guide for firms. We are consulting on amendments and additions to this guidance.

Management Information (MI)

Useful MI provides senior management with the information they need to ensure that the firm effectively manages the money laundering and sanctions risks to which it is exposed. MI should be provided regularly, including as part of the MLRO report, and ad-hoc as risk dictates.

Examples of useful MI include:

- An overview of the money laundering and sanctions risks to which the bank is exposed, including information about emerging risks and any changes to the bank's risk assessment.
- An overview of the systems and controls to mitigate those risks, including information about the effectiveness of these systems and controls and any changes to the bank's control environment.
- Legal and regulatory developments and the impact these have on the bank's approach.
- Relevant information about individual business relationships, for example:
  - The number and nature of new accounts opened, in particular where these are high risk.
  - The number and nature of accounts closed, in particular where these have been closed for financial crime reasons.
  - The number of dormant accounts and re-activated dormant accounts.
  - The number of transaction monitoring alerts and suspicious activity reports, including where the processing of these has fallen outside of agreed Service level agreements.

Governance structures

Banks should put in place a governance structure that is appropriate to the size and nature of their business. To be effective, a governance structure should enable the firm to:

- Clearly allocate responsibilities for financial crime issues.
- Establish clear reporting lines and escalation paths.
- Identify and manage conflicts of interest, in particular where staff hold several functions cumulatively.
- Record and retain key decisions relating to the management of money laundering and sanctions risks; including, where appropriate, decisions resulting from informal conversations.

Culture and tone from the top

An effective AML and sanctions control framework depends on senior management setting and enforcing a clear risk appetite and embedding a culture of compliance where financial crime is not acceptable.

Examples of good practice include:

- Senior management taking leadership on AML and sanctions issues, for example through everyday decision-making and staff communications.
- Clearly articulating and enforcing the bank's risk appetite. This includes rejecting individual business relationships where the bank is not satisfied that it can manage the risk effectively.
- Allocating sufficient resource to the bank's compliance function.
- Ensuring that the bank's culture enables it to comply with the UK's legal and regulatory AML framework.
- Considering whether incentives reward unacceptable risk taking or compliance breaches, and if they do, removing them.

Risk assessment

Banks must identify and assess the money laundering risk to which they are exposed. This will help banks understand which parts of their business are most vulnerable to money laundering and which parts they should prioritise in their fight against financial crime. It will also help banks decide on the appropriate level of CDD and monitoring for individual business relationships.

A business-wide risk assessment:

- Must be comprehensive. It should consider a wide range of factors, including the risk associated with the bank's customers, products, and services. It is not normally enough to consider just one factor.
- Should draw on a wide range of relevant information. It is not normally enough to consider just one source.
- Must be proportionate to the nature, scale and complexity of the bank's activities.

Banks should build on their business-wide risk assessment to determine the level of CDD they should apply to individual business relationships or occasional transactions. CDD will help banks refine their assessment of risk associated with individual business relationships or occasional transactions and will determine whether additional CDD measures should be applied and the extent of monitoring that is required to mitigate that risk. An individual assessment of risk associated with a business relationship or occasional transaction can inform, but is no substitute for, a business-wide risk assessment.

A customer risk assessment:

- Should enable banks to take a holistic view of the risk associated with a business relationship or occasional transaction by considering all relevant risk factors.

- Should be recorded – where the risk is high, banks should include the reason why they are content to accept the risk associated with the business relationship or occasional transaction and details of any steps the bank is to take to mitigate the risks, such as restrictions on the account or enhanced monitoring.

Enhanced Due Diligence (EDD)

The central objective of EDD is to enable a bank to better understand the risks associated with a higher-risk customer and make an informed decision of whether to on-board or continue the business relationship or carry out the occasional transaction. It also helps the bank to manage the increased risk by deepening their understanding of the customer, the beneficial owner, and the nature and purpose of the relationship.

The extent of EDD must be commensurate to the risk associated with the business relationship or occasional transaction but banks can decide, in most cases, which aspects of CDD they should enhance.

Senior management should be provided with all relevant information (e.g. source of wealth, source of funds, potential risks, adverse information and red flags) before approving PEP relationships to ensure they understand the nature of, and the risks posed by, the relationship they are approving.

Examples of effective enhanced due diligence measures we observed included:

- Obtaining more information about the customer's or beneficial owner's business.

- Obtaining more robust verification of the beneficial owner's identity on the basis of information obtained from a reliable and independent source.

- Carrying out searches on a corporate customer's directors (or individuals exercising control) to understand whether their business or integrity affects the level of risk associated with the business relationship, for example because they also hold a public function.

- Using open source websites to gain a better understanding of the customer or beneficial owner, their reputation and their role in public life. Where banks find information containing allegations of wrongdoing or court judgments, they should assess how this affects the level of risk associated with the business relationship.

- Establishing the source of wealth to be satisfied that this is legitimate. Banks can establish the source of wealth through a combination of customer provided information and documents such as: evidence of title, copies of trust deeds, audited accounts (detailing dividends), letters from employers confirming salary, tax returns, or bank statements. It is important for banks to establish how the customer or beneficial owner acquired their wealth, especially where they are a prominent PEP. This is distinct from identifying the assets they now own.

- Establishing the source of funds used in the business relationship to be satisfied that they do not constitute the proceeds of crime. The source of funds refers to the activity that generated the funds; it does not refer to the means through which a customer's funds were transferred to the bank.

- Commissioning external third party intelligence reports where it is not possible for the bank to easily obtain information through open source searches or there are doubts about the reliability of open source information.

- Where the bank considers whether to rely on another firm for EDD purposes, it ensures that the extent of EDD measures is commensurate to the risk it has identified and that it holds enough information about the customer to carry out meaningful enhanced ongoing monitoring of the business relationship. The bank must also be satisfied that the quality of EDD is sufficient to satisfy the UK's legal and regulatory requirements.

Enhanced ongoing monitoring

In addition to guidance contained in Part 1 Box 3.8 of *Financial crime: a guide for firms:*

- Compliance have adequate oversight over the quality and effectiveness of periodic and event driven reviews.

- The firm does not place reliance only on identifying large transactions and makes use of other 'red flags'.

Transaction monitoring

Examples of red flags in transaction monitoring can include (this list is not exhaustive):

- Third parties making repayments on behalf of the customer, particularly when this is unexpected.

- Repayments are made from multiple bank accounts held by the customer.

- Transactions are inconsistent with the business activities of the customer.

- The purpose of the customer account changes without adequate explanation or oversight.

- Transactions unexpectedly involve high risk jurisdictions, sectors, or individuals.

- Early repayment of loans or increased frequency/size of repayments.

- Accounts with low balances but a high volume of large debits and credits.

- Cumulative turnover significantly exceeds the customer's income/expected activity.

- Debits are made shortly after credits for the same value are received.
- The customer makes frequent transactions just below transaction monitoring alert thresholds.
- Debits to and credits from third parties where there is no obvious explanation for the transaction.
- The customer provides insufficient or misleading information when asked about a transaction, or is otherwise evasive.

Customer reviews

Banks must keep the documents, data or information obtained as part of the CDD process up to date. This will help banks ascertain that the level of risk associated with the business relationship has not changed, or enable them to take appropriate steps where it has changed.

Examples of factors banks may consider when conducting periodic reviews:

- Has the nature of the business relationship changed?
- Does the risk rating remain appropriate in light of any changes to the business relationship since the last review?
- Does the business relationship remain within the firm's risk appetite?
- Does the actual account activity match the expected activity indicated at the start of the relationship? If it does not, what does this mean?

Examples of measures banks may take when reviewing business relationships:

- Assessing the transactions flowing through the customer's accounts at a business relationship level rather than at an individual transaction level to identify any trends.
- Repeating screening for sanctions, PEPs, and adverse media.
- Refreshing customer due diligence documentation, in particular where this is not in line with legal and regulatory standards.

Sanctions

In addition to guidance contained in Part 1 Chapter 7 of *Financial crime: a guide for firms,* example of good practice include:

- Firms carry out 'four-eye' checks on sanctions alerts before closing an alert or conducting quality assurance on sanctions alert closure on a sample basis.
- Firms regularly screen their customer database (including associated persons) against sanctions lists using systems with fuzzy matching capabilities.
- Alert handlers have access to CDD information held on each of the bank's customers.

Financial Conduct Authority

PUB REF: 4952

25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk