

CYPRUS – EFFECTIVE IMPLEMENTATION OF CUSTOMER DUE DILIGENCE MEASURES

LEVEL OF IMPLEMENTATION OF PREVENTIVE MEASURES BY FINANCIAL INSTITUTIONS

SUMMARY REPORT OF MAIN FINDINGS BY MONEYVAL AND THE INDEPENDENT AUDITOR

Pursuant to the tasks listed in the terms of reference for the third party Anti-Money Laundering (“AML”) audit of the effective implementation of customer due diligence (CDD) measures with particular reference to deposits and loans (see attached – Annex 1), Moneyval and Deloitte provided final reports on the credit sector’s overall level of compliance with the Cypriot AML legal framework on 24 April 2013. In addition, Deloitte also provided data and analysis related to individual institutions’ level of compliance.¹

The data included in Deloitte’s analysis exposes systemic deficiencies in the implementation of preventive measures by the audited institutions. While Moneyval was not able to access actual customer files, its findings significantly revise its previous, more favorable assessment of Cyprus’ AML system. In particular, Moneyval’s assessors express their concern that the combination of a number of features associated with international banking business (e.g. introduced business, plus complex structures, plus use of nominees) may, in higher-risk cases, bring the cumulative level of inherent risk beyond a level that is capable of being effectively mitigated by the CDD measures currently being applied.

The main shortcomings are summarised below.

1. Customer Due Diligence

1.1. Business profile

Accurate customer information is at the root of AML preventative measures as it forms the basis for effectively knowing the customer, understanding the business relationship, and establishing a proper risk profile. However, the reports found that customer business profiles are generally not properly established by Cypriot banks. The institutions included in the sample did not appear to uphold a suitable degree of accuracy in gathering and documenting relevant information from customers, and therefore were not consistently in a position to understand the purpose of the account, define the customer’s business economic profile and evaluate the expected pattern and level of transactions.² A few examples can be taken from the data provided by Deloitte:

- 70% of the most complex ownership structures have nominee shareholders and an average of three layers between the customer and the beneficial owner(s), and the identity of the beneficial owners is identified through independent source (whether

¹ The sample included 390 customers (the top 180 depositors and 90 borrowers and the remainder randomly selected) in the six credit institutions with more than EUR 2 billion in deposits. The top borrowers account for more than EUR 16 billion or more than 15% of the total loans, and the top depositors account for more than EUR 8 billion or approximately 10% of the total banking system deposits.

² Examples of required information observed to be missing from or insufficiently detailed in customers files include: overly generic descriptions of customer’s business activity and purpose of opening the account, of the documentation regarding the expected origin of incoming funds and the expected destination of outgoing transfers and payments, and of the customer’s source and size of wealth and annual income.

- by the bank or an introducer) in only 9% of these cases.
- Around 27% of deposit client files reviewed showed inaccurate information on the customer and beneficial owner. The figure for loan files was 11%.

1.2. Customer risk profile

Efficient use of resources and effective customer due diligence measures require assessing risks associated with different types of customers. Although both reports found that banks in Cyprus did business with customers which could be considered to present higher risk (but not necessarily definitively “high” risk) profiles, the banks’ awareness of the measures to be taken at client take-on and on an ongoing basis was found to be insufficient, especially in relation to politically exposed persons. In addition, the overall awareness regarding clients presenting higher risk profiles was not demonstrated to be robust. In particular, the low awareness within banks of the combination of risk factors posed by their customers (e.g. use of nominees, non-resident clients, use of introducers without direct access to beneficial ownership information) was seen as a potential vulnerability. In particular, Deloitte’s analysis of customer files indicates that:

- In relation to the 390 customers included in the sample, the audit reveals that simple commercial database checks showed that approximately 10% of these customers are “politically exposed persons” (PEPs) that had not been detected or flagged by the banks.
- Although the samples analysed by Deloitte are quite similar from one bank to another, the risk profile assignments differ significantly, with high risk customers representing 8% of the sample in one bank and 58% in another.

1.3. Ongoing customer due diligence

The risk profile of a customer may and does change during the course of a business relationship. Accordingly, it is important that information on the customer and its beneficial owners be regularly updated. The requirements to perform ongoing due diligence on the customer and the business relationship did not appear to be properly implemented. Weaknesses in customer identification measures, and in building of the economic profile and risk-profiling over time, undermine the effectiveness of the monitoring carried out in the course of the relationship. In addition, the auditor observed a general lack of traceability of controls performed within customers’ files (with specific reference to high risk customers).³ In particular, Deloitte’s analysis confirms that:

- Only four internal investigations for possible ML were recorded on the customers in the sample during the period from 2008 through 2012.
- Ongoing monitoring of high risk customers and beneficial owners data appears at best to be performed only once a year.

2. Reliance/Introduced business

While banks may rely on introducers (e.g. other financial institutions, lawyers, accountants in or outside the country) to perform parts of the CDD process, this practice presents risks which require proper safeguards. In Cyprus, the use of business introducers is widespread but inadequately managed, hampering appropriate knowledge of the customers. It is estimated that

³ For example, specific customer review forms and/or documentation/proof of information obtained by an independent and reliable source are missing.

75 percent of international business is brought in by Cypriot introducers (sometimes involving chains of introducers outside Cyprus) rather than directly sourced. Accordingly, banks place significant reliance on business introducers in Cyprus or other countries to provide information for CDD purposes. In those cases where the customer is introduced, the identity of the beneficial owner is typically presented to the bank as part of an overall package of CDD documentation provided by the introducer. However, banks remain in many cases at least one step removed from direct contact with the beneficial owner, and are even further removed where chains of introducers are used.⁴ The institutions included in the sample appear to have been overly reliant on third parties in providing CDD information in the absence of a risk-based verification of the underlying information provided. This is particularly evident with regard to multi-layered and less transparent ownership and control structures involving foreign jurisdictions generally considered to be of higher money laundering risk.

3. Company registry

An efficient company registry is essential to ensure the ability of banks to fully apply CDD measures with respect to registered legal persons. This is especially critical in Cyprus given the speed with which company structures can be changed and the widespread use of nominees, which may go unnoticed by financial institutions. While around 90 percent of the top depositors and borrowers included in the sample are legal persons and around 40 percent of the total are Cypriot legal entities, the current poor functioning of the Company Registry makes identity verification challenging. There is a large backlog of amendments to registration documents at the Company Registry and a lack of follow up for a significant number of unsubmitted annual returns and financial statements. At the end of February 2013, 270,741 companies were included in the register, 56,815 of them having been registered since the start of 2010.

4. Suspicious transaction reports (STRs)

STRs must be made to the financial intelligence unit when banks have suspicions that funds are the proceeds of a criminal activity or are related to terrorist financing. Banks' ability to report STRs is highly dependent on the quality of CDD and ongoing monitoring, which informs their knowledge of the customer. The reports reveal that the banks failed to report a significant number of suspicious transactions to the authorities, including in very compelling cases. Moneyval notes that only a few STRs appear to have been made as a result of ongoing monitoring or in relation to tax-related suspicions of ML. These weaknesses are confirmed by Deloitte's review of customers' files.

- No suspicious transactions were reported to the Financial Intelligence Unit between 2008 and 2010 with regard to the customers included in the sample (mostly the top depositors and borrowers of the six main institutions), and only one was filed in 2011, and a few in 2012.
- Deloitte's forensic analysis of customers' transactions revealed 29 potentially suspicious transactions during the past 12 months; none of these was identified by the banks as deserving further scrutiny or potential reporting.
- In a number of other cases, the absence of information on the beneficial owner or publicly available information pointing to the criminal environment of customers and/or beneficial owners may have warranted reporting to the authorities.

⁴ E.g., the beneficial owner is identified through a noncertified declaration, the control chain between the customer and the beneficial owner is not always easily traceable.

In conclusion, while identifying no regulatory weaknesses, both reports suggest that there are substantial shortcomings in the implementation, by banks, of AML preventive measures. First, shortcomings have been detected in the implementation by banks of customer due diligence, including with regard to the proper identification of and follow-up on beneficial ownership and the classification of risk profiles. These shortcomings are particularly worrisome in a context of overreliance on third-party “introducers”, and of a poorly functioning company registry. Second, the reports’ findings indicate that banks have reported almost no suspicious transactions to the Financial Intelligence Unit, although in a number of cases publicly available information pointed to the customers’ criminal background. These findings also highlight the AML supervisory authority's failure to adequately monitor the implementation by banks of the AML framework. Corrective measures to address the shortcomings identified in the reports will need to be articulated by the program partners and included in an action plan-to be agreed with Cyprus by the time of the-first review of the program.