



## **AML Compliance: The Italian Landscape – Claudio Mauro**

***26 Apr 2011***

This article examines the Third EU Money Laundering Directive and its implementation in Italy, with special emphasis on anomalous indicators and the advantages of a risk-based approach.

Money laundering is regarded as a major risk to society because it provides criminals with the financial strength to fund and expand their illicit activities. To help prevent this, various nations have established anti-money laundering (AML) laws that regulate how certain types of businesses interact with their clients. For example, in the UK, a body of legislation known as the Proceeds of Crime Act outlines a number of AML measures.

In Europe, according with the Third EU Money Laundering Directive, in order to be AML compliant businesses must implement AML programmes. Although a business is allowed to develop its own programme, it must meet certain minimum standards, such as outlining procedures for requiring identification to verify customers, filing reports and maintaining certain records. It is also necessary for the business to develop methods and procedures to detect suspicious activity.

The first EU Money Laundering Directive was originally transposed by a union of 12 member states, in an environment where the main concern was to prevent the internal market from being usurped to mask the proceeds of crime and to combat drug trafficking. It soon became clear that the scope of the EU AML provisions of Directive 91/308/EEC and its amending directive, Directive 2001/97/EC, needed to be widened to prevent using the financial system for 'terrorist financing'. The new Directive 2005/60/EC does exactly this, as well as consolidating and bolstering the provisions of its predecessors.

Structurally, Directive 2005/60/EC offers no surprises. However, some interesting new terms appear throughout that will require parties involved in financial transactions to be mindful of who they are dealing with, where funds come from and what the purpose of spending those funds are. Additions to the list of entities which must apply customer due diligence are provided under Article 2. Article 4 also provides for member states to extend the Directive to

other professions as they see fit. For the first time, Article 3 defines 'serious crimes', which clears up some ambiguity from previous years. Furthermore, the term 'beneficial owner' has also been defined to prevent the legal owner from acting as a façade for a beneficial entity.

Directive 2005/60/EC would appear to represent the minimum threshold of AML and anti-terrorist financing regulations, as Article 5 provides for flexibility, expressly empowering member states to enforce tighter, more stringent regulations on their home state.

As such, AML and the combating of terrorist financing (CFT) can only be treated as pressing objectives of global concern.

## **The Italian Landscape**

In Italy, the Third EU Money Laundering Directive was implemented by Legislative Decree No 231 on 21 November 2007: "Implementation of the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing as well as of the Directive 2006/70/EC providing for the executive measures".

During 2010, several notices have been amended by Unità di Informazione Finanziaria (UIF), the financial intelligence unit of the Bank of Italy, and the Ministry of Treasury concerning examples of anomalous behaviours related to fraud in the value added tax (VAT) regime in inter-community transactions (within the EEC), individualisation of 'anomaly indicators' in order to facilitate the reporting of suspicious transactions by certain categories of operators, examples of anomalous behaviours related to abuses in public financing, guidelines intended to clarify the framework of the obligation to report suspicious transactions, as recently amended by Article 36, DL No 78 on 31 May 2010.

According to Article 16 of the Legislative Decree No 231, 21 November 2007, financial operators shall apply customer due diligence measures - listed under Article 19 of the Legislative Decree No 231, 21 November 2007 - in the following cases:

- When carrying out transactions involving means of payment, assets or values amounting to €15,000 or more.
- When carrying out occasional transactions amounting to €15,000 or more, whether the transaction is carried out in a single operation or in several operations that appear to be linked.
- When the value of the transaction is undetermined or undeterminable.

- When there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold.
- When there are doubts about the veracity or adequacy of previously obtained customer identification data.

According with Article 19 of the Legislative Decree No 231, 21 November 2007, customer due diligence measures shall comprise:

- Identifying the customer and the beneficial owner, verifying their identity on the basis of documents, data or information obtained from a reliable and independent source.
- Identifying the beneficial owner - including, as regards to legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer - at the same when identifying the customer.
- Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

According to Article 41 of the Legislative Decree No 231, 21 November 2007, where the institutions know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted. Such suspect shall be inferred by the characteristics, the entity, the nature or any other circumstance acquired due to the professional role exercised by the Institution, also considering the economic background and the activities carried out by the client.

According to the same Article 41 (as recently amended by Article 36, DL No 78, 31 May 2010), it shall be deemed as suspicious also the frequent and unjustified cash settlement of any operation, and, in particular, the withdrawal and the deposit of cash for amounts equal or higher than €15,000.

### **Anomalous Indicators**

As stated above, such Ministerial Decrees provide institutions with a list of 'anomalous indicators', i.e. suspicious behaviours of the client, which may give rise to the obligation for the institutions to report the transaction. Such indicators refer to:

- The client's profile (e.g. the client provides false information).
- The professional activity the institution is requested to carry out (e.g. the institution is requested to give advice on deals which are not coherent with the client's core business).
- The terms of payment of the transaction (e.g. the terms of payment proposed by the client are not coherent with the praxis concerning the transaction involved).
- The incorporation of companies, trusts and similar organisations (e.g. the client is willing, without any reasonable cause, to dissimulate or to prevent people from identifying the real owner of the firm).
- Transactions concerning properties and other registered goods (e.g. the client purchases goods at an anomalous price).
- Financial and accounting operations (e.g. the client is willing to carry out accounting operations aimed at concealing financial funds).

These events highlighted the fact that money laundering had taken on epic proportions over time, and that the proliferation of new technologies and communication platforms had created countless opportunities for fraud, money laundering and other illicit financial activities. They also accentuated the need to 'know your customers' (KYC), and led to the creation and implementation of a range of KYC and AML laws aimed at preventing financial criminals from accessing and abusing financial systems.

Given the fact that the greatest majority of criminal activities generating profits only start generating a traceable paper trail once funds are introduced into the financial system, it was deemed necessary to approach AML compliance and law enforcement in a way that clamped down on abuses of the world's official banking and financial systems. To this end, regulatory, legislative and law enforcement agencies set out to create an AML compliance framework and cross-border law enforcement regime aimed at holding financial institutions accountable for their clients' transactional activities.

### **Risk-based Approach**

Generally, Article 9 of the Third EU Money Laundering Directive requires that standard KYC requirements be met prior to the establishment of a business relationship or the carrying out of the transaction. The derogations of Article 9 adopt a risk-based approach and verification of identity can occur during the establishment of the business relationship where there is little risk of terrorist financing and money laundering occurring.

The risk-based approach is apparent in Article 11, which provides for a simplified customer due diligence process, under which some customer due

diligence requirements do not have to be applied in certain circumstances. In contrast, Section 3, Article 13 provides for enhanced customer due diligence requirements, which triggers further KYC requirements in cases of high-risk customers. This 'high risk' category includes customers not physically present for identification purposes and non-domestic politically exposed persons, as mentioned above.

So, the basis for setting up an adequate security system to combat money laundering, terrorism financing and fraudulent activities at the expense of the institution is to conduct a threat analysis. This is designed to prevent damaging events that occurred in the past from happening again, and to uncover and monitor potential areas of risk. The aim of an appropriate threat analysis is to record, identify, categorise and weight the institution-specific risks. But this alone does not protect a financial services provider against money laundering offences or fraud. Every identified risk must be stored with institution-specific measures appropriate to the risk. These measures eliminate the risk or reduce it to an acceptable residual risk. The risk-based approach obliges financial services providers to continually adjust the threat analysis so that they can counteract new developments in white-collar crime.

## **Conclusion**

The AML compliance landscape is a complex one, and despite the fact that most banks and regulated service providers have willingly invested in compliance infrastructure and procedures, many institutions are struggling to surmount the operational challenges of remaining compliant - and hence still face a significant reputational risk.