

## **Credito Valtellinese Banking Group Anti-Money Laundering Policy**

### **1. GENERAL FRAMEWORK OF THE ISSUE**

#### **1.1. Preliminary Considerations**

The Credito Valtellinese Banking Group (hereinafter also referred to as CV Group or simply Group) actively supports the international efforts to combat money laundering, terrorist financing and in general any type of criminal activity.

The Group is made up of banks and financial and special purpose companies, all operating on Italian territory and hence subject to the supervision of Bank of Italy. Italy is a member of the European Union and of the F.A.T.F. (Financial Action Task Force) and has adopted provisions directed at assimilating both the principles established by community directives (91/308/CEE, 2001/97/CE, 2005/60/CE) and F.A.T.F. recommendations (40 Recommendations June 2003 and 9 Special Recommendations (SR) on Terrorist Financing (TF)).

Specifically in November 2007 the legislator issued Legislative Decree 231/2007 which assimilates Directive 2005/60/CE, coordinating in a single document all the prevailing laws to combat money laundering and terrorist financing (laws that are also referred to hereinafter as AML), while Bank of Italy in its capacity as Supervisory Authority for the banking sectors issued a so-called "Decalogue", which, assimilating the F.A.T.F. recommendations, provides useful elements for detecting transactions that may involve money laundering or terrorist financing.

With a view to prevention Italian legislation has established, with regard to the use of cash and monetary instruments payable to bearer, stricter limits than those established by the community legislator. Specifically Italian legislation establishes a threshold of 5000 euro for each transaction and requests that:

1. the transfer of sums equal to or exceeding this threshold occurs through qualified intermediaries (identified as Banks, Post Offices and EMI);
2. the balance of savings deposits to bearer cannot be equal to or exceed said threshold;
3. bank cheques or banker's drafts issued for amounts equal to or exceeding said threshold must be crossed as non-transferable.

#### **1.2. Group Policies on Anti-Money Laundering and Counter Terrorism Financing**

In order to comply with the provisions and the spirit of sector regulations, the CV Group has defined an anti-money laundering and counter terrorism financing programme, entrusting oversight of the matter to the Compliance Function. The Group model includes: the drawing up of a policy

and of operating regulations; constant surveillance of applicable laws on the matters and analysis of their impact on the corporate structure; maintenance and update of activity monitoring software, for the purpose of detection of any suspicious transactions; constant and continuous control of the programme by the Internal Audit and Compliance Functions.

The model's functionality specifically relies on:

- appropriate diligence on the part of the operator in establishing a continuous relationship and equal diligence in monitoring transactions for the full duration of the relationship;
- a well-defined system for assigning the degree of risk associated with a customer or a transaction, so as to be able to focus attention on those customers and transactions that potentially present a greater risk of money laundering.

The CV Group has drawn up a manual entitled "Consolidated Anti-Money Laundering Rules" which is kept constantly updated. The manual consists of a section concerning the regulatory framework, outlining the obligations arising from national and international legislation on anti-money laundering and counter terrorism financing, and an operative section outlining the conduct that must be followed by operators when performing transactions in order to ensure compliance with legal obligations.

This Policy, which is part of the aforesaid anti-money laundering and counter terrorism financing programme, applies to all the Group's banking and financial companies and features the following key elements:

- customer identification and verification;
- identification of the actual principal of the transaction or holder of the funds;
- particular attention for high risk subjects;
- no type of relations with "shell banks";
- reporting to the Authorities of any suspicious transactions;
- continuous training programme;
- conservation of records for 10 years;
- periodic control of the AML process by competent functions.

In all cases in which the Group may operate with countries that request higher standards, said standards will be analysed and may be taken into consideration when establishing and performing transactions with said countries.

## **2. PROCEDURES AND RULES OF THE CREDITO VALTELLINESE BANKING GROUP**

The Credito Valtellinese Banking Group has introduced special procedures and issued specific internal regulations to ensure compliance with the law, as detailed in the following paragraphs.

### **2.1 Banking Services**

The main aim of the anti-money laundering and counter terrorism financing policy is to avoid the use of banking and financial services for criminal purposes, with the primary objective being that of accepting only customers whose sources of income can be recognised as legitimate.

Each time a relationship is opened with a customer, documents proving the customer's identity must be acquired. For natural persons identity documents that are valid pursuant to national legislation are sufficient, while for companies it is necessary to establish the ownership structure

through official documentation. Identity documents must obviously not be out of date at the time they are checked.

The Group provides specific procedures for transactions with occasional customers and for customers that have been identified by other financial intermediaries (so-called Distance Identification).

As provided by Legislative Decree 231 dated 21 November 2007 (assimilation of Directive 2005/60/CE), when opening a relationship information must be gathered on:

- grounds for opening the relationship;
- financial position of the holder;
- source of funds.

Accounts or relationships cannot be opened anonymously or under false name.

With reference to subjects with registered office in off-shore jurisdictions, the documents presented when establishing the relationship must be carefully examined and the opening must be authorised by the competent corporate functions.

Customer identification is managed by an electronic procedure named “Electronic Relations Procedure”, which allows the check to be completed only when all the necessary data has been gathered, that is, the data prescribed by national and community legislation (surname, name – corporate name, address, province, municipality, tax code, place of birth, date of birth, gender, details of an identity document and address for correspondence).

This data is stored in a single computerised database (*Archivio Unico Informatico*), set up pursuant to law, for ten years from termination of relations with the customer.

The customer data is constantly monitored and updated by operators, especially when significant changes occur.

The CV Group demands particular diligence from branch operators when maintaining relations with categories of subjects which by their nature feature high risk of money laundering or terrorist financing. This category specifically includes:

- subjects resident in or possessing funds which originate from countries that do not adhere to international standards to combat money laundering, terrorism financing and criminal activity in general (usually included in the F.A.T.F. “black list”);
- subjects that perform activities that by their nature are more exposed to the risk of money laundering and terrorist financing (money transfer, gold trading, etc.);
- subjects that are included among the “Politically Exposed Persons”, i.e., subjects who hold or have held public offices, as well as their relatives and consultants.

The opening of relationships with said subjects is submitted to a specific authorisation process as provided by the Group’s internal procedures.

The Group is provided with internal regulations that provide clear instructions on the matter of identification and possible reporting of potentially suspicious transactions. In addition to the identification procedures implemented by the operators having direct contact with the public, the Group uses an algorithm-based procedure which each month, by assessing the type of transaction executed, the type of customer and the risk associated with the subject, extracts potentially suspicious transactions which are punctually analysed by the branch managers and by the competent inspection service.

Any anomalous or potentially suspicious activity is submitted to the attention of the Head of Anti-Money Laundering (person appointed for each of the Group's banking and financial companies). If plausible motivation for the transaction cannot be found, the Head of Anti-Money Laundering reports it to the competent Authorities and assesses whether to suspend business relations or to continue the relationship constantly monitoring the customer's activity.

Half-yearly reports are drawn up on performance of the monitoring activity and update of anti-money laundering obligations; the Board of Statutory Auditors of the Group financial company or bank involved periodically examines the content of the aforesaid reports.

## **2.2. Fight against International Terrorism**

Like all financial intermediaries the Companies of the Credito Valtellinese Banking Group play a specific role in the prevention and fight against terrorism.

International terrorism does not always originate from criminal activities which are instead the basis for money-laundering activity. It is precisely for this reason that national and international legislation calls upon intermediaries to assist governments in the fight against terrorist financing, through prevention, analysis and disclosure of information in their possession. Specifically, they must collaborate to ensure that terrorist organisations do not gain access to financial services, to support the security forces in identifying potential suspects and to provide full and effective replies to any requests for information from the Authorities.

Naturally all these control activities are carried in a non-discriminating manner and with full respect for the individual's rights.

Greater focus is placed on analysing transactions of subjects that perform activities deemed by the Authorities to be exposed to greater risk of terrorist financing. As soon as the Authorities issue the lists of the activities that can potentially be linked to the phenomenon, appropriate internal regulations and implementation procedures will be drawn up so as to allow accurate monitoring of activities performed by subjects operating in sectors considered to be at risk.

As stated above, the action to combat international terrorism is therefore subject to increasing attention from both national and international legislators.

This commitment has led to the introduction of various types of financial sanctions, such as the freezing of assets, the restriction of credits, financial or commercial sanctions, importation and exportation bans.

The embargo measures can essentially be divided into three types:

1. lists contained in the European Union Regulations;
2. lists of American issue and contained in the O.F.A.C. (Office of Foreign Assets Control) provisions;
3. individual sanctions introduced by the Italian order with reference to any lists of national issue.

### **2.2.1 European Lists**

The European Union has often used sanctions or restrictive measures in implementation of resolutions of the United Nations Security Council, or in an autonomous manner.

These measures are directed against governments of third party countries, as well as natural persons or corporate entities and include specific embargoes on arms, commercial or financial restrictions, restriction on the granting of entry visas or specific measures required by the case in question.

Violation of restrictive measures established by community regulations causes the transactions performed to be null and void and leads to an administrative sanction of no less than half the value of the transaction.

The CV Group has established with regard to the European lists:

- a ban on opening relationships with subjects included in the lists;
- a ban on operating with subjects included in the lists and the freezing of any assets or funds possessed by these subjects and deposited at one of the Group's Banks;
- an obligation to report any operating activity of these subjects to the competent Authorities;
- a ban on executing transactions between the Group's customers and subjects included in the lists, with freezing of the assets involved in the transaction;
- a ban on performing transactions related to the export of firearms or the financing of such transactions.

### **2.2.2 US Lists**

The restrictive measures enforced by the US government are enforced through the O.F.A.C., and essentially consist of two types: freezing of goods and funds associated with names included in the lists and total or partial embargo measures on individual countries.

This legislation applies to financial intermediaries incorporated under US law and directly or indirectly to non-US intermediaries only with regard to activity that passes through the United States.

The CV Group has signed the USA Patriot Act; hence, Group banks abstain from carrying on business with subjects included in the US lists through US correspondent banks or those of US origin.

Furthermore, as a rule, even if not expressly provided in the USA Patriot Act, Group banks avoid executing transactions in US dollars or in other currencies destined to subjects included in the lists even if performed without the intervention of US correspondent banks; this rule may only be derogated in exceptional cases, provided that the danger of terrorist financing is patently inexistent and subject to the obtaining of specific authorisation from the General Management of the Group bank involved.

Specific authorisation from General Management, to be granted after appropriate preliminary investigation, is also requested in the event that transactions involving letter of credit or similar document originating from intermediaries included in the OFAC lists are payable at Group banks.

In relation to the above and with regard to both the European and US lists, the Group uses an IT application to check the names subject to embargo; the related lists are interfaced with company procedures, highlighting transactions to be frozen and reported or the impossibility of opening an ongoing relationship.

## **2.3 Relations with Correspondent Banks**

“Relations with correspondent banks” means the supply of current liability accounts or other type of accounts and all the related services in favour of another institute used for cash transactions, for managing available funds and for short term loans or investment requirements.

The CV Group provides for specific precautions to be taken in establishing and maintaining relations with non-EU correspondent banks, in compliance with national anti-money laundering provisions in force; specifically, the opening of the relationships in question is subordinate to authorisation from the General Management of the competent Group bank.

With regard to the request for the opening of correspondent relationships from EU banks, the Group policy provides for the acquisition of special documentation that certifies precise compliance with international anti-money laundering and counter terrorism financing legislation, in accordance with international best practices (Wolfsberg).

The Group is not party and does not intend to be party to any type of relationship with so-called “Shell Banks”, i.e. banks that:

- do not handle business with a fixed address;
- do not employ one or more full-time employees with a fixed head office;
- do not conserve operating reports at this address;
- are not subject to inspections on the part of the banking authorities that issued their authorisation to operate.

Internal regulations do not allow our customers to make direct use of correspondent accounts.

#### **2.4. SWIFT and Telegraphic Keys**

In the case of request for exchange of SWIFT or telegraphic keys the Group banks will proceed to identify the requesting foreign financial institution and to verify its position with regard to AML through the data that can be found in the Bankers Almanac.

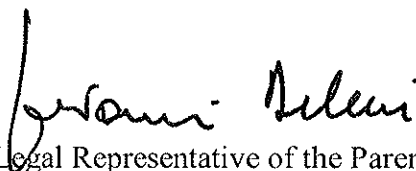
#### **2.5 Training**

The Group has set up a training programme that includes an on-web self-learning course available to all employees, which is obligatory for employees who have relations with customers and who perform analysis and control activities on the matter.

Classroom courses have been set up for branch managers during which instructions are provided on how to identify potentially suspicious transactions and manage anomalous activities.

Information on anti-money laundering and the fight against terrorism is also provided as part of the course for new recruits, with illustration of the key principles and of the Consolidated Anti-Money Laundering Rules.

Sondrio, 05.06.2009

  
The Legal Representative of the Parent Bank