



SUSTAINABILITY

AML

Policy for the Prevention of Money Laundering and Terrorist Funding

FILK SPA

Via dell'Industria 8
36065 Mussolente
(VI) Italy

T +39 0424 579411
E filk@filk.it
Pec: filkspa@pec.filk.it

CS € 9.000.000 i.v.
Registro delle
Imprese di Vicenza

CF PI / VAT:
IT00325890242
Export M/VI 003835



1

Introduction

Laundering of the proceeds of crime is one of the most serious aspects of criminal behaviour and does much to pollute the entire economic system the reinvestment of ill-gotten gains in legal businesses radically perverts markets and muddies finance, eroding the efficiency and propriety of the economic system in general.

Filk SpA (“the Company”) and the other companies within its Companying group make strenuous efforts to prevent the products and services they provide being used for criminal money-laundering or the funding of terrorism.



The AML/Terrorism Policy developed by the Company (“Policy Against Money-Laundering and the Funding of Terrorism”) takes its place within a broader system of internal controls whereby the Company aims to ensure compliance faces a guarantee compliance with current applicable laws and regulations. It underpins the Companying Group’s entire system of AML safeguards. The Policy also includes an introductory explanation of the general rules, circulars and communications issued by the Company.

The AML/Terrorism Policy's fundamental elements are as follows:

- Identification of all customers, and (if different) the real beneficiaries of accounts and other dealings with the Company;
- Verification of every customer's risk profile;
- Stronger obligations to carry out due diligence when relations are set up with Companies or other financial companies located outside the EU, even when those Companies' home jurisdiction does NOT impose equivalent obligations to those prescribed by the relevant EU Directives;
- Analysis of all the transactions which may be connected with money-laundering or terrorist funding operations;
- An embargo on transactions and accounts where the Company learns that any person on the "terrorist lists" is involved;
- A ban on the opening of any kind of account or the execution of any transaction in the absence of the prescribed documentation or the presence of forged paperwork; the ban also covers cases where the potential customer is suspected of taking part in terrorist activities;
- A ban on dealings with so-called "shell" Companies;
- Immediate notification of the UIF (the Italian Financial Intelligence Unit) whenever legally required;
- Regular training of the Company's staff and contractors so that they are constantly updated concerning relevant AML/terrorism provisions.

The above elements, based on the highest AML/terrorism standards, are mandatory; no exceptions are permitted; managers, employees and contractors must all observe them in order to avoid involving the Company in any kind of money-laundering and or funding of international terrorism which could harm its reputation or its stability.

**Structure
of this
document**

→ This Policy consists of four chapters in all, the first being the Introduction.

The main subjects dealt with in the other chapters are summarized below.

Chapter 2

gives a brief definition of the terms “money-laundering” and of the “terrorist funding”.

Chapter 3

describes the main relevant statutory and regulatory provisions both Italian and international.

Chapter 4

explains the way in which the risks of money-laundering and terrorist funding are handled within the holding company Filk; the aim of the chapter is to describe the methods adopted for managing and monitoring the cited risks.

**Persons to
whom
the Policy
is addressed**

→ This Policy is distributed to all appropriate Organizational Units within the holding company and to all Companying Group subsidiaries.

**Responsibility
for the Policy**

→ The holding company’s Board of Directors, acting on the recommendation of the AML Function, has ultimate responsibility for taking appropriate measures to update the Policy, review it as required for extraordinary reasons, and circulate any changes to Group subsidiaries.

2

Definition of “money-laundering” and “terrorist funding”

Italian legislation¹ has, following EU practice, defined the term “money-laundering” in accordance with the 1988 UN Convention against Illicit Traffic in Narcotic Drugs, as any of the following activities:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his actions;

(b) the concealment or disguising of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

Money-laundering is usually described as a three-stage process:

Placement —————> the proceeds of unlawful activity (intentional or not) are collected and deposited with a Company and/or other financial company;

Layering —————> this is done by carrying out a complex series of financial transactions (which may appear unrelated), so as to hamper the reconstruction of the money movements involved;

Integration —————> the proceeds of crime are used in legitimate business so as to appear formally to have a legitimate origin.

These three stages are not static, and may overlap. Any of them may involve the use of Companies for criminal purposes.

“Funding of terrorism” is defined as “any activity whatsoever aimed by any means whatsoever at the collection, provision, brokerage, deposit, custody or supply of funds or other economic resources however generated with a view to their use, even in part, for the carrying out or at all events the furtherance of one or more criminal acts for purposes of terrorism as defined in the Penal Code, regardless of the use actually made of those funds and/or economic resources in or for the commission of such criminal acts.”²

3

Relevant statutory and regulatory provisions



The laundering of unlawful revenues (ie the recycling of the proceeds of unlawful activities into legitimate assets) knows no national borders or limitations. The opening of markets has made the practice easier, as indeed has the expansion of “legal” financial and commercial dealings. As wider markets become available, the criminal economy is likewise facilitated. Globalized markets, faster financial transactions and the integration of the single European market all work to speed up business for criminal as well as legitimate undertakings. The globalization of the economy and the globalization of criminal activity go hand in hand, and this calls for internationally standardized regulation.

Strategies to prevent and defeat money-laundering, and the statutory rules which give those strategies expression, are therefore becoming more international³. Their aim is to prevent those who move ill-gotten funds around today’s increasingly open and competitive markets exploiting holes in the nets set up by the various individual countries to prevent such movements. It should be pointed out that there are still geographical areas and jurisdictions whose rules are not yet

in line with international best practice; stricter AML controls, calibrated to match the greater risk, need to be applied to those areas.

Companies and other financial intermediaries therefore find themselves having to cope with growing compliance and reputational risks arising from their potential involvement in unlawful transactions.

So far as European Community rules on the prevention of money-laundering are concerned, the main provisions are contained in Directives 91/308/EEC and 2001/97/EC and, most recently, in the so-called Third AML Directive 2005/60/EC (“on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing”) which abrogates those two earlier ones and introduces significant changes to the AML system, bringing the European rules into line with those enshrined in the 2003 GAFI Recommendations. So far as the prevention of terrorist funding is concerned, on the other hand, the relevant Directive is 2006/70/EC implementing Directive 2005/60/EC.

Italian law has incorporated the Third AML Directive and its implementing Directive 2006/70/EC by means of the following measures

- **The AML Act 2007** (Legislative Order 231/07) “*Incorporation of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and its implementing Directive 2006/70 EC*”: This Act reorganized Italian law on money-laundering.

→ **The Funding of Terrorism Act** (Legislative Order No. 109 of 22 June 2007): *“measures to prevent, counter and defeat the financing of terrorism and the activity of countries which threaten international peace and security, in implementation of European Directive 2005/60/EC”*. The Act contains provisions designed to prevent and defeat terrorist funding by giving Companies and other financial intermediaries more systematic obligations to fulfil whenever they are in contact with persons suspected of involvement in terrorist activities.

Under these Acts the Banca d'Italia has issued two regulations: *“Operational instructions for strengthened controls to prevent the funding of programmes tending to the proliferation of weapons of mass destruction”*

(May 2009) and *“Provisions concerning irregularity Indicators for Companies and financial Intermediaries”* (August 2010).

Other regulatory provisions include the models and typical patterns of irregular commercial and financial behaviour which may indicate money-laundering or terrorist funding activity, issued by the Financial Information Unit, and the Economic and Finance Ministry's Order dated 18/08/2008 including a list of those countries outside the EU which impose obligations equivalent to those provided for in Directive 2005/60.



→ Lastly there are the “*arrangements, procedures and internal controls designed to prevent the use of Companies and other financial companies for the purposes of money-laundering or terrorist financing as defined in Art. 7(ii) of the AML Act 2007*” issued by the Banca d’Italia in agreement with [the markets and insurance regulators] CONSOB and ISVAP on 10 March 2011, which Banca Filk promptly implemented.

The threshold of watchfulness is designed to be reached sooner than in the past: there are more detailed and stronger KYC rules under which operators are obliged to ensure that they are fully and “duly” informed about their customers, and which even provide that if there has not been complete disclosure between the parties then the relationship must not be initiated, or must be broken off.

The Company’s own rules include, in particular

→ the Code of Ethics;

→ the Rules for the AML/terrorism risk management process, specifying the processes and activities to

→ be carried out by the Company in the discharge of its AML/terrorism obligations;

→ the Procedure for AML/terrorism control safeguards, describing the Company’s integrated system of internal controls guarding against the risks of money-laundering and terrorist funding, and detailing the safeguards in place and the procedures established by the AML Office.

This set of operational and procedural rules is designed not only to ensure compliance with the law’s mandatory provisions but also to prevent the Company becoming involved, even unwittingly, in acts of moneylaundering or terrorism.

4

Guidelines

The Filk Group's policy for the prevention of money-laundering and terrorist funding is based on the following:

- Institutional support from and involvement of all levels of the organization;
- Corporate rules even stricter than the official provisions require;
- Transactions analysed by staff who really know the customers;
- Rigour and depth in analysing suspicious transactions;
- Systematic and permanent auditing of Group subsidiaries and non-Italian counterparts;
- Continuous support to the Internal Audit and Training functions;
- Priority to AML prevention over the Group's commercial interests.



The prevention of money-laundering is of strategic importance in fighting crime; it is based on the following principles:

- Customer Due Diligence;
- recording and keeping of data on business relationships and transactions;
- adequate organizational procedures and internal controls;
- reporting of suspicious transactions.

Guidelines for the discharge of these obligations to legal standards are set out below.

Customer Due Diligence (CDD)

There are three levels of obligation in terms of “Customer Due Diligence” (in the wording of the Third Directive): general, enhanced and simplified. These are explained in the following paragraphs. The due diligence obligation does not apply only to new customers (in whose case it must be discharged before opening a business relationship or executing a one-off transaction), but also to existing customers (in whose case the due diligence must be carried out at the next appropriate contact and in any case by the deadline determined in relation to the relevant risk band).

This obligation requires the Company to identify its customers and their beneficial owners, and to verify their identity, to understand the nature of the business relationship and to carry out ongoing monitoring throughout the relationship. In the case of the “enhanced” due diligence obligation, the Company must take further steps, whose scope is to be judged in accordance with the degree of risk posed by the customer or the business relationship. The “simplified” due diligence obligation allows the Company to apply simplified measures to certain types of customers or business relationships.



Customer Due Diligence, then, does not consist of an one-off action at a single moment in time but is rather a process made up of a sequence of many actions. Some of these (identification and verification of identity, for instance) are done only once; others (above all, the monitoring of transactions carried out and the customer's commercial, financial and occupational profile) are to be repeated continuously throughout the business relationship.

If unable to comply with its Customer Due Diligence obligations, the Company will not establish a business relationship nor execute any transaction, and will terminate any existing business relationship.

GENERAL DUE DILIGENCE OBLIGATIONS

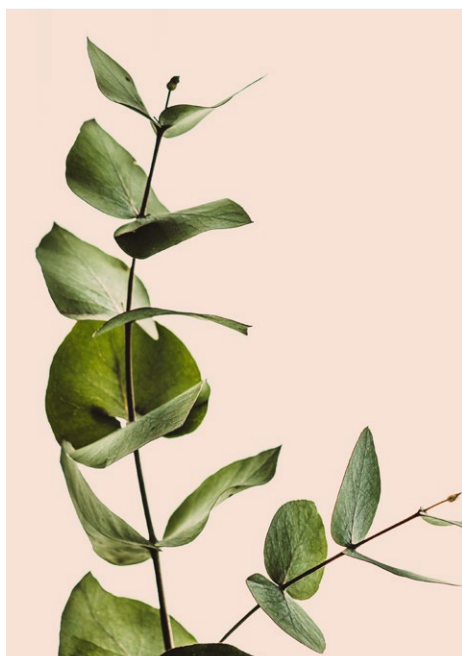
The general obligations consist of the following activities:

- a)** identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- b)** identify, where applicable, the "beneficial owner"⁴ and verify his identity;
- c)** obtain information on the purpose and on the intended nature of the business relationship or professional services;
- d)** conduct ongoing monitoring throughout the course of the business relationship or professional services.



These activities must be carried out for all new customers and, after an assessment of the risk, existing customers and, in particular, this applies in the following cases:

- a)** whenever an ongoing relationship is established;
- b)** whenever a one-off transaction ordered by a customer is executed involving the transmission or other movement of funds of or exceeding the statutory threshold, regardless of whether this is done in a single transaction or an apparently split transaction or linked series of transactions;
- c)** whenever there is a suspicion of money-laundering or terrorist financing, regardless of any derogation, exemption or threshold whatsoever that might otherwise be applicable;
- d)** whenever there are doubts as to the accuracy or adequacy of the data obtained beforehand for the purposes of identifying a customer.



The obligations are performed as follows:

- a)** the customer's identity is ascertained and checked, and data on the beneficial owner procured, in the customer's presence, by inspecting an unexpired identity document (any of the prescribed forms) before an ongoing relationship is set up. In the case of a corporate customer the individual's authority to represent that customer must be verified, and the details needed to ascertain and check the identity of the representative(s) authorized to sign for the intended transaction;
- b)** the beneficial owner's identity is ascertained and checked at the same time as the customer's; in the case of corporations, trusts and similar juristic persons this requires the taking of adequate steps (commensurate with the risk) to understand the customer's ownership and control structure. The enhanced CDD obligation applies in the case of trusts and corporations in which trusts hold interests.

c) continuous monitoring throughout the course of the ongoing relationship is done by checking that the transactions carried out by the customer are compatible with facts known to the Company or about the customer, his trading activities and risk profile, by having regard where necessary to the origin of funds, and by keeping all the Company's documents, data and information properly up to date;

The identification particulars relating to account holders must be procured for the following persons:

→ for accounts in the name of individuals (including joint accounts):

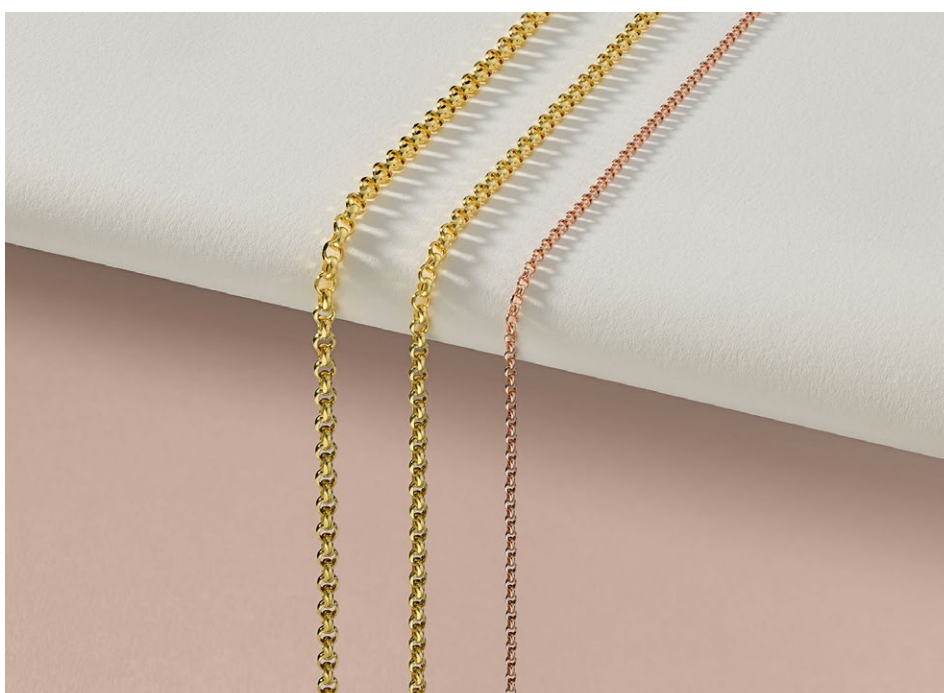
- all the account holders;
- any powers of attorney;
- any appointed representatives specifically authorized to carry out particular counter transactions;

→ for accounts in the name of juristic persons and "sole trader" firms:

- the juristic person itself and the authorized individual who is setting up the relationship
- a "sole trader" firm, and its proprietor,
- any persons with authority to carry out transactions on the account, or any appointed
- representatives specifically authorized to carry out particular counter transactions.

In particular:

- Full details must be held both on all the account holders (including minors) and on all persons authorized to operate the account. In the case of joint accounts, therefore, the failure to procure full particulars of one such person will make the account unavailable to the other(s) as well, regardless of their standing instructions (concerning joint or several signatures) for withdrawal of funds; likewise in the case of accounts in the name of juristic persons, &c., incompleteness of the data on just one of the authorized signatories will prevent all the others operating the account even though they may have provided the details required by law;
- In the case of non-bearer accounts in the name of a minor it is necessary to get the Tax Registration Number (which can be issued to any person, even a minor) and an identity document.
- In the case of accounts in the name of institutions, associations or companies, the data must be collected not only on the institution, &c. itself but also on its legally-authorized representative who sets up the account, and on all persons authorized to act on its behalf.



**SIMPLIFIED
DUE DILIGENCE**

Simplified Due Diligence may only be applied if the customer is:

1. one of the persons designated in Art. 11(i) and (ii) (b and c) of the AML Act;
2. a EC credit or financial institution covered by Directive 2005/60/EC;
3. a credit or financial institution situated in a non-EC jurisdiction which imposes requirements equivalent to those laid down in this Directive and provides for supervision of compliance with those requirements; or
4. a government department or an institution or an organism which performs “public functions” as defined in the Treaty on European Union, the treaties on the European Communities or derived EC law.

Where the simplified obligation is applied, the Company must still check that the customer in fact qualifies for this simplification. If there are grounds for thinking that the identification that has been made is unreliable, or insufficient for gathering the necessary information, then the simplified CDD may not be applied.



The simplified obligation may also be applied with reference to the following products

1. life insurance policies with an annual premium of no more than €1,000 or a single premium of no more than €2,500;
2. supplementary pension schemes governed by the Pensions Code, Legislative Order No. 252/2005, provided that there is no surrender clause other than as provided for in Art. 14 of that Code and the policy cannot be used as collateral for a loan other than as prescribed by current laws and regulations;
3. compulsory pension, superannuation or similar schemes that provide retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme except upon death;
4. electronic money as defined in Art. 1(2)(h-ter), of the Companying Code where, if the device cannot be recharged, the maximum amount stored in the device is no more than €150, or where, if the device can be recharged, a limit of €2,500 is imposed on the total amount transacted in a calendar year, except when an amount of €1,000 or more is redeemed in that same calendar year by the bearer as referred to in Article 3(iii) of EC Regulation No. 1781/2006;
5. any other product or transaction representing a low AML/terrorism risk which meets the technical criteria established in accordance with Art. 40(i)(b) of the European Directive, if authorized by the Economy and Finance Minister as prescribed in Art. 26.

ENHANCED
CDD OBLIGATIONS

Enhanced due diligence must be applied to all customers with a greater risk of money-laundering or terrorist funding and, at all events, in the following cases:

- when the customer is not present in person,
- in the case of accounts with correspondent Companys in non-EU jurisdictions
- in the case of relationships with and/or transactions by politically exposed persons;
- whenever the Company's risk-based approach (see 4.1.6 below) requires it.

OBLIGATION TO
DECLINE BUSINESS

Whenever the Company is unable to comply with the CDD obligations it must put a block on the setting up of the business relationship and prevent any transaction being executed; any existing business relationship or professional services already being provided must be terminated.



The obligation not to engage in a business relationship also extends to relationships with:

- Companys or other financial companies located in any jurisdiction outside the EU which does NOT
- impose equivalent obligations to those prescribed by the relevant EU Directives;
- “shell” Companys, wherever located.

In all these cases it will be necessary to consider submitting a report to the UIF. Before reporting a suspicious transaction to the UIF and in order to make it possible to exercise the power of suspension provided for in Article 6(vii)(c) of the Act, the Company should refrain from executing transactions where there is a suspected connection with money-laundering or terrorist funding.

If it is impossible to refuse because the Company is obliged by law to accept a deed or execute a transaction which by its nature cannot be postponed, or if to decline might hinder investigation, the Company is nonetheless obliged to report the suspicious transaction immediately as prescribed by Article 41 of the AML Act.

ANTI-TERRORISM MEASURES

To ensure that it duly discharges its obligations and observes all prohibitions provided for under current applicable laws and regulations concerning terrorism, the Companying Group must:

- decline to carry out transactions in any way involving (submitted or ordered by or on behalf of) any person listed in the EC regulations or in any order issued by the Italian authorities;
- report suspected terrorist funding transactions to the UIF;
- apply automated controls on personal details, and compare these with the names on the lists provided by the UN and in EC regulations;
- constantly monitor those lists and their revisions, and check that they match the lists published by the authorities;
- freeze any account in which any person on the “terrorist lists” plays a part.

In all these cases it will be necessary to consider submitting a report to the UIF. Before reporting a suspicious transaction to the UIF and in order to make it possible to exercise the power of suspension provided for in Article 6(vii)(c) of the Act, the Company should refrain from executing transactions where there is a suspected connection with money-laundering or terrorist funding.

If it is impossible to refuse because the Company is obliged by law to accept a deed or execute a transaction which by its nature cannot be postponed, or if to decline might hinder investigation, the Company is nonetheless obliged to report the suspicious transaction immediately as prescribed by Article 41 of the AML Act.

Obligation to make and keep records

Record making

All details acquired by the Company in performance of its CDD obligations are recorded for use in any subsequent investigation concerning money-laundering or terrorist funding activities, or in analyses conducted by the regulators or any other competent authority.

For this purpose the Company has set up a Centralized Computer Archive (AUI) to store the following information:

- details of business relationships: (i) the commencement date, (ii) the customer's ID data, together with details of all persons authorized to transact business on behalf of the account holder, and the account number, if any;
- details of all transactions [of €15,000 or more, whether in single transactions or apparently linked or subdivided sets of transactions]: (i) the date, (ii) the reason for the transaction, (iii) the amount, (iv) the transaction type, (v) the means of payment used and the ID data of the person making the transaction and of any other person on whose behalf it is being made.

The above information must be recorded promptly and in any case no later than thirty days after the transaction has been executed or the account opened, changed or closed.

Record keeping

In connection with its CDD obligations the Company must keep a copy of or references to the documents required for ten years after the end of the business relationship.

So far as transactions and business relationships are concerned, accounting entries and records (the original documents or copies of equivalent evidential validity in law) must be kept for ten years after execution of the transaction or the end of the business relationship.



Organizational procedures and internal control measures

In order to comply with the law as it stands from time to time, the Companying Group has created an organizational model designed to guard against risks connected with taking in, recycling or lending out any money or other assets derived from unlawful sources.

Filk has set up a powerful safeguard against money laundering in the form of its AML Office, which is tasked and resourced both to plan and develop responses to systemic change and to deal with the issue in operational terms with a high standard of professional competence.

Responsibility for the AML Function and for submitting reports of suspicious transactions under Art. 41 of the AML Act has also been formally defined.

Lastly, the wider internal control system involves the interaction and involvement of many corporate units and functions⁵ which work together, each in its role and with its specific functions, to ensure that the model for guarding against AML/terrorism risks is effective and adequate. This interaction between the various functions is realized by means of a rapid system of information sharing adequate to the Group's complexity, the type of services and products offered and the scale of the risk associated with the characteristics of its customer base.

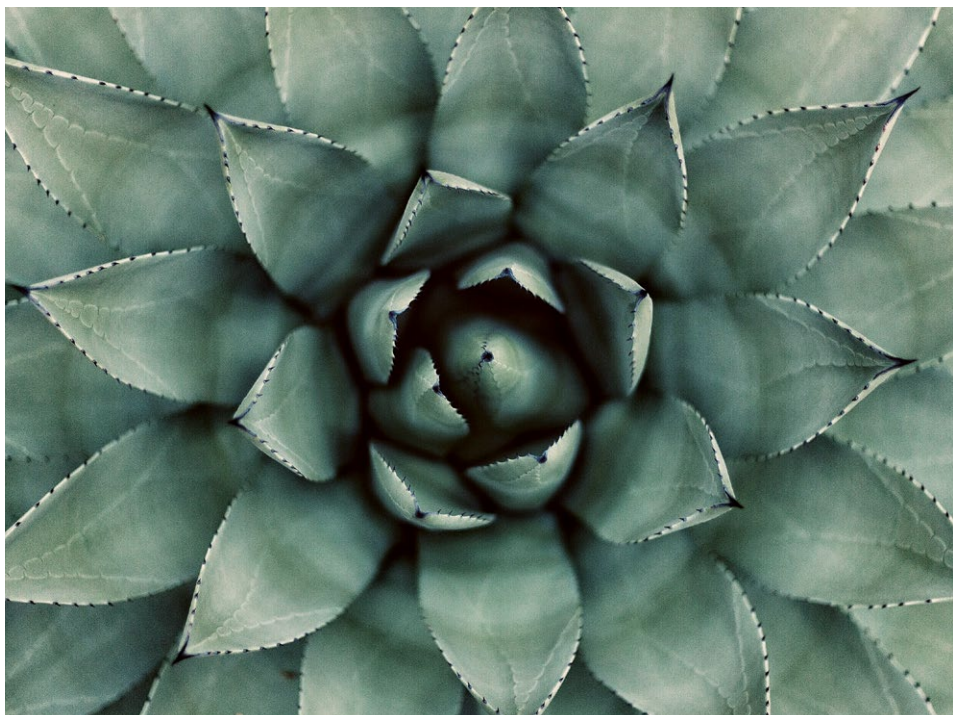
Checking the adequacy of the safeguards adopted by the Group is one of the duties which the Banca d'Italia is expected to perform on all those Companies and other financial intermediaries which it supervises under the "prudential review and assessment process", so as to ensure that they are as fully informed as possible of the potential implications of any non-compliance in their corporate dealings.

Reporting suspicious transactions

Whenever the Company suspects or has reasonable grounds for suspecting that a money-laundering or terrorist funding operation has been or is being conducted or attempted, it submits a suspicious transaction report to the Financial Information Unit (UIF) as required under Art. 41 of the AML Act. Such reports are made without delay.

Until the report has been submitted the Company refrains from executing the transaction, unless that is impossible due to the normal conduct of business or might hinder investigation, in which case the report is sent immediately after the transaction has been executed.

Grounds for suspicion include the characteristics, scale and nature of the transaction and any other circumstance whatsoever which comes to such persons' knowledge as a result of their functions, also taking into account the financial scope and nature of the business carried on by the subject of the report, as understood from information available to the reporting organization either as a result of its own business or as a result of a commission. To facilitate the identification of suspicious operations the Company refers particularly to the "operating instructions for identifying suspicious operations" issued and periodically revised by the UIF.



Training of employees, contractors and sales agents

In accordance with statutory and regulatory provisions the Companying Group organizes in-house AML training programmes for all its staff (employees, contractors and sales agents) so as to spread a culture of compliance with the AML regulations throughout the organization and raise awareness of the issues among the staff.

The Group sets up its own education and training courses taking account of changes in laws and regulations, the procedures laid down for meeting the Company's obligations to gather information needed for identifying and verifying its customers, making and keeping records, and detecting irregularities for the purpose of assessing transactions as suspicious with a view to reporting them if necessary.

The aim of the training programme is to ensure that the staff understand the organization's obligations and responsibilities and the overall thinking behind the Group's rules, and that they both recognize which activities might be connected with money-laundering or terrorist funding and know what to do as a result. Special training programmes are provided for the staff of the AML Function.

Particular attention is also paid to training those staff (sales agents in particular) who come into direct contact with customers, and to newly-hired staff.

Raising the calibre of the Company's staff is an ongoing and systematic process which forms part of the overall programme of taking due account of changes in laws and regulations and in the Company's procedures.

FILK S.P.A.

CEO

Andrea Cremasco