Annex B
Report on the system of procedures to combat money laundering and terrorism financing

1. Persons responsible and employee training

The Group's central compliance function fulfills several roles with respect to the anti-money-laundering and terrorism financing system within the Group, including coordination, management, training, administration and control. The Group's head of compliance (Stéphane Cador, cadorst@cic.fr) reports directly to a member of the Group's Executive Management; he is supported by a national manager of the anti-money laundering and terrorism financing system of procedures (Raoul d'Estaintot, raoul.destaintot@creditmutuel.fr).

To execute its assigned missions, the central compliance function has correspondents within the permanent control and compliance departments of the various regional divisions, business line entities and foreign-based entities. These correspondents, in particular the Tracfin correspondents and declarers, report on a functional basis to the central compliance function.

The integration of the five federations in early 2011 involved:

– the creation of an Ile-de-France (IDF) division pooling the resources of CMIDF and CIC Paris,

– the creation of a "Grand Sud-Est" division combining the CMM, CMDV, CMSMB and CMSE regional federations,

– CMC's assumption of responsibility for second-level controls on behalf of CMN beginning April 1, 2011.

In 2011, a second-level control portal dedicated to the fight against money-laundering was rolled out. This portal is itself the control program in which the Tracfin correspondent records the results of his controls at the scheduled reporting intervals. At this time, he must determine whether the money-laundering and terrorism financing risk is covered.

Since October 2011, the self-training manual has integrated a new Tracfin Version 2011 course that replaces the Tracfin Third Directive course and complements the 16 training modules as well as the summary module that enables training initiatives in the branches; employee are required to have completed this new course by end-2013. New features include a regulatory update, new questions and updated cases and situations; in order to pass, persons taking the course must correctly answer at least 75% of the 25 questions asked on the final quiz.

2. Classification of risks, description of procedures

Classification and duty of vigilance

The classification of money-laundering and terrorism financing risks was continued in 2011 using the methodology and principles described in the 2010 report.

The following money-laundering and terrorism financing risk classifications are now available:

– Network,

– Life insurance, property and casualty insurance,

– Fund management, wealth management,

– Equipment leasing, real estate leasing,

– International business,

– Employee savings,

– Point-of-sale financing,

– Real estate function,

– Large accounts function.

As of end-December 2011, the breakdown of the clientele presenting money-laundering or terrorism financing risk (*i.e. with an attached money-laundering risk code*) was as follows, and showed that heightened vigilance was needed for 0.13% of the clients:

Compared to 2010, the main change was the establishment of a new risk coding "RIE 046 -Vigilance LAB". This risk code can be adapted to all types of situations that require the implementation of complementary or strengthened vigilance measures with respect to client relations. It may be positioned by a function or business line based on its own specificities, notably for the initiation of a new client relationship (*for example without a face-to-face meeting with the client*) or based on the account operating method (*for example an account always operated through a proxy*).

Transactions involving embargoed countries (*1,633 outgoing and incoming transfers totaling €51.6 million*) are executed as part of imports or exports of goods and services whose business purpose is fully justifiable, which are subjected to more stringent control, notably through special questionnaires that take into account regulatory changes and documentary controls.

In order to address measures related to political changes in the countries of the Maghreb region as well as the Tracfin warning messages requesting monitoring of Politically Exposed Persons (*PEP*) from these countries prior to the publication of official lists, an emergency operational procedure "Crisis situation in certain countries" was published on March 3, 2011. It notes the persons within the Group to be contacted, the configuration of files to collect, the relevant scope and the content of the messages to create and disseminate the lists.

In order to improve the updating of knowledge on risky clients, a dedicated section was created in the Tracfin application to ask the branch managers to update the Know Your Customer (KYC) questionnaire once a year for this client group. Links make it possible to review the account operations, examine the client's equipment, track his sales history and check the status of any anti-money-laundering warnings. A second-level control task was implemented in order to ensure that these updates have actually been carried out properly.

Similarly, a new control task is planned in 2012 that focuses on questionnaires for new client relations and clients that are not included in the "RIE LAB" risk-coded category.

Monitoring and special analysis in the event of a freezing of assets

The European Union's list of terrorists is updated automatically. New client relations and the items in the third party database are screened regularly. Similarly, transfers are monitored ex ante in order to block the transaction, where necessary, if it turns out that one of the parties is on the terrorist list or could be subject to an embargo (*OVF application*).

For the financing of activities of French companies doing business in countries subject to embargo measures, the International Activities department implements specific procedures based on customized questionnaires and documentary controls, notably invoices, shipping and customs documents.

The main change relative to 2010 involves the upgrade to the screening application (TIESUS is now SUSPECTS) to automate as much as possible the process for controlling the client database and new client relations.

Control methods with respect to the duty of vigilance in respect of foreign subsidiaries and branches

Special guidelines for these entities were disseminated in 2006 and subsequently updated in 2010 following the transposition of the EU's Third Directive into French law. Under these guidelines, the host country's regulations are applied if they are more stringent than those applicable in France. The guidelines also include points on the duty to establish an anti-money-laundering program adapted to the entity's specific risk classification, to inform the National Compliance department when drafting a report on a suspect transaction or activity or the annual report on internal control, which must include a section on the fight against money laundering. The Compliance Committee's reports must also be submitted.

Contacts were established with the correspondents of the subsidiaries and branches located abroad. Meetings and conferences were held with TARGOBANK in Germany and Spain, Banque de Luxembourg and CIC Switzerland.

Work has begun in order to establish a procedure for intra-Group information sharing.

Conditions for reliance on a third party to identify customers

(Articles L561-7 and R561-13-I)

BFCM has established a customer relations and agreements management application (PRESC) with "financial institution" third parties (i.e. those qualifying as "Intermediaries for Banking and Payment Services Transactions") for the purpose of issuing mortgage loans and business loans. This application was rolled out in the CM10-CIC Group on January 1, 2011. All those firms that qualify as Intermediaries for Banking and Payment Services Transactions are therefore listed in the PRESC application. All agreements drafted in PRESC include a Banking Transaction Intermediary mandate.

The supporting documents related to the identity of the customer as well as, where applicable, the actual beneficiary and the purpose and nature of the customer relationship are provided to the bank before any new customer relationship is opened, since the complete file must be sent to the bank. Only the bank is authorized to determine whether to grant a credit or not based on the submitted documents (*with the exception of cases where the future borrower is already a Bank customer, in which case the due diligence will already have been performed by the Bank*).

With respect to the home country of the service provider, the agreement does not contain any restrictions, although controls may be easily implemented through the application.

The current agreement between the bank and third parties defining the methods for submitting the collected materials and controlling the due diligence implemented is in the process of being updated with respect to the collection of supporting documents and their certification.

Conditions for the use of service providers to identify customers

(Articles R561-13-II)

These provisions apply only in some business lines, in particular Sofemo, CM-CIC Bail, Cofidis, C2C and Banque Casino.

In 2010, efforts were focused on updating the agreements with these third parties in accordance with Article 11-10 of CRBF Regulation 97-02.

The point of sale financing procedure (consumer credit) is currently being updated for the purpose of harmonizing the methods of anti-money-laundering controls among institutions.

Methods for implementing obligations in the area of wire transfers

These methods remained unchanged from those described in the 2010 report.

As a payments service provider for the order giver

The anti-money-laundering procedure for the network indicates that for outgoing wire transfers, there should be no doubt regarding the fact that our "order-giving" customer is behind the transaction. Similarly, the identity of the beneficiary as well as his or her bank account information must be indicated on the wire transfer order:

- the beneficiary must be clearly identified on the wire transfer order, along with his or her bank account information,
- this information must be broken down based on the destination (inside or outside the European Union) of the funds.

As an intermediary payments service provider:

This section applies only to BFCM and CIC Paris. The methods are as follows:

- control that identification information is present for the order giver,
- transmission of information received to the beneficiary's payments services provider for individual transactions and reposting for each individual transaction of information received in the file "Header" for bulk transactions,
- transmission within three working days of complete information on the order giver,
- storage of information for five years and the current year.

As the beneficiary's payments service provider

The anti-money-laundering procedure for the network indicates that for "incoming" wire transfers, there should be no doubt regarding the fact that our "beneficiary" customer is in fact the actual beneficiary of the transaction.

In order to identify the order giver, the following minimum information is required:

- In the case of transfers from a bank established in a European Union member country: at a minimum, a reference to its unique bank code.
- In the case of transfers from outside the European Union, the identity of the order giver must be provided: Name + account number or unique bank code + address or date and place of birth or national identity number.
- In the absence of this information, a clarification must be requested. Any discrepancy must be notified to the Tracfin correspondent to determine whether a report needs to be submitted.

Finally, a warning (EVT 656) notifies the network of any incomplete transaction from abroad with respect to the identification of the order giver, it being noted that all these transactions are detected and monitored by CM-CIC Services, which prompts the deficient institutions if necessary.

Methods for circulating information within the Group

Information needed by the unit responsible for helping to combat money laundering and terrorism financing

The single Tracfin manual has been replaced by two manuals, one for the networks, the other for the business lines. A third manual dedicated to Tracfin notification correspondents and persons working in the anti-money-laundering departments was distributed.

These manuals include:

– the general principles,

– the code of ethics,

– the risk classification procedures by business line as well as by function (checks and wire transfers),

– procedure, compliance, regulatory and jurisprudence fact sheets as well as methodologies (suspicious activity report and anti-money-laundering questionnaire)

– documentation on the applications (Tracfin, second-level control and Anti-money-laundering Compliance portal applications),

– documentation issued by the public authorities (mainly the French ACP's basic guidelines and Tracfin activity reports).

Information related to the existence and content of suspicious activity reports

In addition to the intra-Group coding (RIF), an initiative was launched to define an information-sharing procedure for the clientele's personal identification data in cases involving the implementation of third-party introductions, discussions on the existence or content of a suspicious activity report or the coding of the client's money-laundering risk. This procedure would apply to the various Group entities in France and abroad (Luxembourg, Switzerland, Germany, United States, United Kingdom, Singapore, Monaco, Belgium, Spain) and take into account legal constraints involving confidentiality, money-laundering prevention and personal data protection.

Methods for defining the criteria and thresholds for material discrepancies

The overhaul of the Tracfin application made it possible to establish a data center that serves as a source for monitoring information and statistical data. Statistics were therefore compiled by banks, federations and regional delegations, for Tracfin correspondents and the Compliance Control Committee (CCC).

These statistics include:

– client breakdown by money-laundering risk (RIE LAB) in absolute and relative terms,

– breakdown of outgoing and incoming transfers to and from countries on the black list or subject to an embargo

– monitoring of processing of warnings, review files, proposed and actual suspicious activity reports,

– training,

– monitoring of anti-money-laundering control tasks by the branches (first-level control),

– monitoring of second-level control tasks.

3. Permanent controls

The first-level control plan is included in the dedicated control application (*CINT*), branch-by-branch or Caisse-by-Caisse at Crédit Mutuel. It is supervised by the permanent control teams which are split into regions.

With respect to the second-level permanent control, the results are replicated through the portals for the networks (CINT) and business lines (CINTMT).

However, the second-level controls still have room for improvement with respect to the quality of the comments accompanying the reviews. The degree of completion for new customer files continued to improve, but further work is needed in order to digitize customer identification supporting documents.

The main deficiencies observed include the following areas:

– the degree of completion of files on existing clients still needs to be refined, notably with respect to the existence of a digital ID, it being noted that these documents exist but are usually stored in the accounts;

– files occasionally remain suspended in the Tracfin application, although clear improvements have been made since the introduction of EVT 730, which provides a daily reminder to the appropriate agents of the cases in the application;

– internal training is still insufficiently supported by the heads of the entities;

– justification of transactions formally entered in the Tracfin application could be improved;

– use of the Tracfin application could be optimized at the branch level.

The following corrective measures have been implemented to remedy the deficiencies observed:

– each quarter, permanent control verifies that the network entities have correctly processed the controls and formalized the observations through an analysis of the quality level of each control point for a random sampling of branches;

– in the Tracfin application, a section for clients coded as high risk for money-laundering combined with an icon placed next to the client's name that signals the absence of digitized ID supporting documents, makes it possible to prioritize actions to be taken;

– recommendations have been made to the branches regarding the use of the training cited in the Tracfin manual for the network and the requirement to follow the self-training manual updated in October 2011;

– branches receiving a low rating are included among the priority controls for the following year.

In conclusion, this first year with a second-level control plan dedicated to preventing money-laundering demonstrates good use of applications by the controllers. Their controls demonstrate adequate understanding of the risks, without any significant discrepancies. The main area of focus for 2012 will be on reducing the time required to fill out the files.

A monthly "*Validation Webcheques*" control aims to verify the network's proper application of the control procedure for checks issued. The controls and statistics demonstrate the proper use of this procedure by the branch networks. The number of branches showing discrepancies is limited, and they are contacted systematically.

4. Main deficiencies highlighted by the domestic and foreign control authorities and corrective measures

CF de CM (10278) was audited by the French ACP specifically with respect to anti-money-laundering and terrorism financing. The report had not been received as of the publication date of this registration document.

Last year, the ACP also audited the Marseille airport's foreign exchange counter, which is part of the Crédit Mutuel Méditerranéen regional federation.

Siccfin audited the Monegasque branches of the CMM and CIC LB regional federations. With respect to CIC LB, Siccfin concluded that the recommendations made during the previous audit in late 2008 had been properly followed and did not find any material discrepancies. As for CMM, client record-keeping (paper and electronic) is in need of substantial improvement, notably through the implementation of a summary data sheet.