AUTORITÉ DES MARCHÉS FINANCIERS

DRAFT

FINANCIAL CRIME RISK MANAGEMENT GUIDELINE

November 2011

TABLE OF CONTENTS

Preamble

The *Autorité des marchés financiers* ("AMF") establishes guidelines setting out its expectations with respect to financial institutions' legal requirement to follow sound and prudent management practices and sound commercial practices. These guidelines therefore cover the execution, interpretation and application of this requirement.

The AMF favours a principles-based approach rather than a specific rules-based approach. As such, the guidelines provide financial institutions with the necessary latitude to determine the requisite strategies, policies and procedures for implementation of such management principles and to apply sound practices based on the nature, size and complexity of their activities.

The AMF considers governance, integrated risk management and compliance (GRC) as the foundation stones for sound and prudent management practices and sound commercial practices and, consequently, as the basis for the prudential framework provided by the AMF.

This guideline is part of this approach and sets out the AMF's expectations regarding sound and prudent financial crime risk management practices, including sound commercial practices.

Introduction

In the ordinary course of their activities, financial institutions may unwittingly or not be used to facilitate or be the target of activities associated with financial crime.

In addition to any losses the institution might sustain, the lack of diligence in its financial crime risk management could damage its reputation. In certain cases, this could lead to the public losing confidence in the institution itself and in the entire financial sector.

Thus, the scope of financial crime, and the growing threat these risks pose for consumers of financial products and services and for financial institutions require that the AMF encourage the implementation by financial institutions of an effective financial crime risk management framework.

In this context and pursuant to the authority[1] conferred upon the AMF under the various sectorial statutes it administers, it is issuing this guideline to inform financial institutions of its expectations with respect to financial institutions' legal requirement to follow sound and prudent financial crime risk management practices, including sound commercial practices.[2] The guideline favours *a priori* the need for financial institutions to have effective governance and to implement risk management practices in order to prevent and detect activities associated with financial crime.

The principles set forth in this guideline favour a proactive approach aimed at reducing the risk that a financial institution will be involved in financial crime activities. The application of these principles and compliance therewith by financial institutions should therefore be combined with the sustained efforts of the AMF and other stakeholders, including the police forces and Financial Transactions and Reports Analysis Centre of Canada *(*"FINTRAC") to fight financial crime so as to better promote the integrity of the markets and provide better protection for the public.

1 *An Act respecting insurance*, R.S.Q., c. A-32, ss. 325.0.1 and 325.0.2;
An Act respecting financial services cooperatives, R.S.Q., c. C-67.3, s. 565;
An Act respecting trust companies and savings companies, R.S.Q., c. S-29.01, s. 314.1.

2 *An Act respecting insurance,* R.S.Q., c. A-32, s. 222.2;
An Act respecting financial services cooperatives, R.S.Q., c. C-67.3, s. 66.1;
An Act respecting trust companies and savings companies, R.S.Q., c. S-29.01, s. 177.3.

Lastly, the AMF's expectations are based on core principles and guidelines issued by international organizations,[3] including the Basel Committee on Banking Supervision ("BCBS"), the Financial Action Task Force ("FATF") and the International Association of Insurance Supervisors ("IAIS").

[3] Basel Committee on Banking Supervision, Customer due diligence for banks, October 2001;

Basel Committee on Banking Supervision, Core Principles Methodology, October 2006;

Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003;

Basel Committee on Banking Supervision, Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers, May 2009;

Financial Action Task Force, Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, June 2007;

Financial Action Task Force, The FATF Forty Recommendations, October 2003. The IX Special Recommendations, October 2004;

International Association of Insurance Supervisors, Countering Fraud in Insurance (Insurance Core Principle 21 and Application Paper), October 2011;

International Association of Insurance Supervisors, Anti-Money Laundering and Combating the Financing of Terrorism (Insurance Core Principle 22), October 2011;

International Association of Insurance Supervisors, Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism, October 2004;

International Association of Insurance Supervisors, Insurance Core Principles, Standards, Guidance and Assessment Methodology, October 2011.

Scope

This financial crime risk management guideline is intended for insurers of persons (life and health), damage insurers, portfolio management companies controlled by an insurer, mutual insurance associations, financial services cooperatives as well as trust and savings companies, which are governed by the following Acts:

- *An Act respecting insurance*, R.S.Q., c. A-32
- *An Act respecting financial services cooperatives,* R.S.Q., c. C-67.3
- *An Act respecting trust companies and savings companies*, R.S.Q., c. S-29.01.

This guideline applies to financial institutions operating independently as well as to financial institutions operating as part of a financial group.[4] In the case of financial services cooperatives and mutual damage-insurance associations that are members of a federation, the standards or policies adopted by the federation should be consistent with—and even converge on—the principles of sound and prudent management practices, including sound commercial practices prescribed by law and detailed in this guideline.

The generic terms “financial institution” and “institution” refer to all financial entities covered by the scope of this guideline.

[4] For purposes of this guideline, “financial group” refers to any group of legal persons composed of a parent company (financial institution or holding company) and legal persons affiliated therewith.

Coming into effect and updating

This financial crime risk management guideline will come into effect on month xx, 201X.

With respect to the legal requirement of institutions to follow sound and prudent management practices, including sound commercial practices, the AMF expects each institution to develop strategies, policies and procedures based on its nature, size, complexity and risk profile, and to ensure the adoption of the principles underlying this guideline by month XX, 201X (two years after coming into effect). Where an institution has already implemented such a framework, the AMF may verify whether it enables the institution to satisfy the requirements prescribed by law.

This guideline will be updated based on developments in financial crime risk management and in light of the AMF's observations in the course of its supervision of financial institutions.

Financial crime risks

In the insurance and deposit sectors, a financial institution may be the target of activities of every type and scope associated with financial crimes and involving a variety of parties, including customers, employees, officers and those with whom it has business dealings, such as suppliers.

For purposes of this guideline, the principal activities associated with financial crime are internal fraud and external fraud,[5] money laundering, embezzlement, the illegal transfer of funds to financial or tax havens,[6] illegal tax avoidance (tax evasion) and terrorist financing. Certain activities are frequently reported in the media, such as fraudulent insurance claims, fraud involving mortgage loans, debit cards and credit cards, and the fraudulent use of confidential customer information.

Financial crime can expose a financial institution to various risks, including operational, legal, regulatory and reputational risks. The extent of these risks, alone or in combination, is particularly wide when the perpetrators take advantage of deficiencies in the institution's management or the complicity of its employees or officers.

A financial institution should have a global perspective on financial crime risks. It should establish measures to prevent financial crime and detect activities that may be associated with it. These measures should also facilitate examinations, inspections and investigations relating to financial crime.

[5] Generally speaking, internal fraud is fraud committed by a senior executive, a director or an employee, whether or not in collusion with an internal or external party (for example, embezzlement by an employee).

Generally speaking, external fraud is fraud committed by a customer or a third party (for example, a forged signature on a cheque, an insurance claim in which the value of an item claimed has intentionally been overestimated).

[6] The Organisation for Economic Co-operation and Development (OECD) defines a tax haven as a country or territory with no or nominal taxation. A financial haven is a country or territory where banking secrecy prevails. Reference: www.oecd.org.

Financial crime risk management governance

Principle 1: Roles and responsibilities of the board of directors and senior management

The AMF expects a financial crime risk management framework to be supported by effective governance.

The AMF considers the board of directors[7] and senior management to be ultimately responsible for establishing sound and prudent financial crime risk governance management practices and sound commercial practices.

In light of the roles and responsibilities incumbent upon them under the Governance Guideline,[8] the board of directors and senior management should, among other things:

- develop, approve and implement strategies, policies and procedures.

  In order for an institution to manage financial crime risks effectively and efficiently, these strategies, policies and procedures should focus primarily on preventing and detecting activities associated with financial crime and address the institution's vigilance with respect to customers, employees, officers and those with whom it has business dealings. To this end, the institution should take into account its vulnerability to these risks, particularly with respect to the following elements:

  - customers and the nature of their transactions;
  - employees, officers and service providers;
  - the financial products and services offered;
  - the institution's information systems and internal controls;
  - the methods of used by the authors of activities associated with financial crime and the possibility of operational events and their potential impact.

[7] A reference to the board of directors can also include a board committee, such as a board committee established to examine specific issues.

[8] *Autorité des marchés financiers*, Governance Guideline, April 2009.

Strategies, policies and procedures should be documented and reviewed on a regular basis, particularly in light of changes in the institution's customers, the marketing of new products and the growing complexity of activities associated with financial crime;

- promote a culture that encourages ethical conduct at every level of the institution;

- ensure that staff and officers have proper training and that the people assigned to manage financial crime risks are experienced.[9]

  Responsibility for developing and implementing the financial crime risk management strategy should be entrusted to the chief risk officer.[10] Depending on the size of the institution and the extent of the financial crime risks, a person could also be appointed to be in charge of financial crime risk management;

- adequately monitor financial crime activities that are suspected or have been identified. They should also ensure that these activities are reported to the appropriate authorities and that any relevant information and results of examinations and investigations are communicated;

- ensure that the institution complies with all statutes, regulations and guidelines.[11] As such, they should ensure, in particular, that reports, documents and declarations are completed and sent to the AMF and to the other appropriate authorities, in the prescribed form and within the stipulated time limits.

Framework for financial crime risk management

Principle 2: Financial crime risk management

The AMF expects financial crime risk management to form an integral part of a financial institution's integrated risk management.

The financial institution should manage financial crime risks within its integrated risk management framework. Accordingly, it should give consideration to the interrelationships and interdependencies between risks. This means that the institution should:

- identify, assess and quantify financial crime risks;

- implement risk mitigation measures in order to reduce the likelihood of events that could affect the institution.

---

9 *Autorité des marchés financiers*, Guideline Governing Integrity and Competency Criteria (draft), October 2011.

10 *Autorité des marchés financiers*, Integrated Risk Management Guideline, April 2009.

11 *Autorité des marchés financiers*, Compliance Guideline, April 2009.

The integrated risk management approach should allow the institution to identify operational risk events associated with financial crime and to implement measures to reduce the occurrence of such events and their potential impact on the institution.

Thus, the institution should take the following, in particular, into account:

- internal factors such as:
  - its organizational structure, the nature of its activities, its strategic orientations and its policies;
  - the quality of its internal controls, including the segregation of duties and the delegation of powers;
  - the nature and characteristics of its products;
  - the risk profile of its customers, their business activities and the volume of their local and cross-border transactions;
  - the information technology used;
  - its business dealings, including any possible outsourcing;
  - employee versatility and turnover, the degree of employee knowledge about financial crime, the quality of its labour relations;
- external factors such as:
  - legal, regulatory and normative requirements relating to the fight against financial crime, including the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (2000, c.17) ("Proceeds of Crime Act"), and changes to the designated persons list established by the United Nations;[12]

    Among other things, the institution should participate in an electronic funds transfer tracing system. The AMF expects the institution to fulfill its obligation to declare certain electronic funds transfers made by its customers to the FINTRAC;[13]

[12] Reference: *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. Additional information is available on the AMF website: http://www.lautorite.qc.ca/en/suppress-terrorism.html.

[13] *Guideline 8B: Submitting SWIFT Electronic Funds Transfer Reports to FINTRAC*, published by FINTRAC in June 2011.

- the economic and social context, new threats and opportunities involving financial crime as well as changes in the techniques and methods used;[14]

- changes in international orientations for fighting financial crime.

Principle 3: Intra-group management

The AMF expects a financial institution to manage its financial crime risks in accordance with the management framework applicable to the group to which it belongs.

Activities associated with financial crime carried out through a financial institution that forms part of a group are likely to have significant repercussions on the other entities in the group and adversely affect their solvency and, ultimately, the reputation of the entire group.

Consequently, it is important to adopt a comprehensive approach to financial crime risk management at the group level, locally, nationally and internationally.

It is essential that coherent standards be adopted within the group and that the entities forming part of the group exchange information, particularly in order to identify and assess areas of vulnerability and reduce financial crime risks.

Principle 4: Customer vigilance

The AMF expects a financial institution to conduct continuous vigilance with respect to customers by having sufficient knowledge about them and applying appropriate procedures so as to detect transactions likely to be associated with financial crime.

In applying customer vigilance measures, the financial institution should consider the extent of financial crime risks, particularly with respect to monetary transactions, insurance products and investment products.

[14] Acting on information gathered by its investigators, including through cyber-surveillance, the AMF regularly issues warnings. The information may also be received from investors and from regulators in other jurisdictions. http://www.lautorite.qc.ca/en/alerts.html

Know your customer

The know your customer rule is an essential component of financial crime risk management. It contributes to reducing the likelihood that operational events will occur through a financial institution.

Knowing customers, including their dealings with the institution's other customers and, if applicable, with the other entities forming part of the institution's group, will also allow an institution to measure its concentration risk. Extra vigilance should be conducted especially in the context of related counterparties and related party lending.

An institution should establish appropriate identification procedures and a risk profile and acceptance criteria for its customers, particularly for categories of customers that are likely to present a greater risk. Accordingly, it should require all appropriate supporting documents based on the type of customer and the particular characteristics of certain accounts, such as corporate, institutional or trust accounts. It should also ensure that the customer is not on the lists of persons and organizations believed to be associated with terrorist activities.[15]

To the extent possible, an institution should conduct increased vigilance with respect to customers:

- whose structure or type of activity makes it difficult to identify the owner or controlling interests;
- who act as financial intermediaries, securities dealers, advisers or representatives, custodians, trustees or professionals;
- where something seems odd, for example, a customer who often changes addresses, who refuses to provide proof of identity or who is more interested in the surrender of an insurance policy than meeting insurance needs;
- who are large depositors or borrowers, groups of related borrowers, or "politically exposed foreign persons";[16]
- who are the mandataries of a customer or the beneficiaries of an insurance contract.[17]

[15] See note 12.

[16] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c.17), s. 9.3.

[17] The identity and verification of the beneficiary should take place no later than the payment of benefits provided for under the insurance policy.

The institution should keep an up-to-date register of its customers and their transactions. It must also protect its customers' personal information,[18] particularly so as to prevent the unauthorized use of that information.

Monitoring customer transactions

Based on the risk profile of its various customer categories, an institution should take appropriate vigilance measures, including:

- determining the criteria for controlling, monitoring and overseeing its customers' transactions, in particular as regards the source of funds, the nature of the transactions, transactions that appear to be linked, the type of currency and the country where the recipient is located;

- reviewing all transactions with no apparent economic or lawful purpose or in respect of which it has reasons to believe that the transaction is likely to be associated with financial crime;

- carrying out a more in-depth review of the context and purpose:

  - of any complex transaction or any transaction whose source of funds is questionable or inconsistent with the person's risk profile;

  - of any unusual transaction, particularly if the volume of transactions is unusual in light of the customer's history and the nature of its activities;

  - of frequent cash (or cash equivalent) transactions or transactions carried out in unusual circumstances in light of the customer's profile, and of important fund transfers carried out with no apparent purpose for a specific customer;

  - of electronic transfers[19] made by a customer through another financial institution for the purpose of making a significant amount of money available to a beneficiary (the customer or another person);

  - of any transaction with certain countries that represent a greater financial crime risk.

The institution should implement an appropriate process for minimizing fraud by its customers with respect to insurance claims. Additional measures, particularly relating to the validation of amounts claimed, should be implemented, as needed and depending on the size of the claims.

Lastly, the results of customer transaction monitoring should be recorded in management reports.

[18] *Autorité des marchés financiers*, Commercial Practices Guideline (draft), March 2011.

[19] Including fund transfers, cross-border transfers and domestic transfers.

Principle 5: Employees, officers and business relationships vigilance

The AMF expects a financial institution to conduct continuous vigilance with respect to employees, officers and those with whom it has business relationships through effective internal controls and appropriate procedures so as to detect situations likely to be associated with financial crime.

The institution should focus on preventing activities associated with financial crime involving its employees and officers. However, it should also exercise vigilance as regards individuals who might carry on criminal activities and closely monitor those with whom it has business relationships, particularly its suppliers.

Identifying vulnerabilities

An institution should identify its vulnerability to operational risk events or schemes that could involve employees in the performance of their work or officers in the fulfilment of their roles and responsibilities, such as:

- employee theft of money or property belonging to the institution;
- unauthorized use of customers' personal information;
- supplier corruption, bribes, kickbacks or commissions;
- payments to fictitious suppliers for services not rendered to the institution;
- falsification of documents, failure to record transactions and willful presentation of incorrect financial information.

Controls

The institution should implement internal controls to deal with these sources of vulnerability to financial crime risks. To this end, it should establish:

- controls focused on allocating responsibilities and segregating tasks related to customer transactions and protection of the institution's assets;
- security mechanisms for its information technology, including outsourced information technology activities, in order to prevent the unauthorized use by employees of customers' personal information;
- a rigorous and documented process for awarding contracts.

Lastly, the institution should pay close attention to clues or signals that could lead to the discovery of a scheme associated with financial crime activities, for example, deficiencies involving controls, a failure to follow established processes, an employee who often postpones his vacations or has unusual behaviour, customer complaints and missing assets following an inventory.

It should also consider possible collusion among several individuals for the purpose of sidestepping the internal controls implemented by the institution to protect itself against financial crime risks.

Principle 6: Examination of suspicious activities

The AMF expects a financial institution to carry out examination when it suspects or detects activities associated with financial crime.

The financial institution should react promptly to any situation where activities associated with financial crime are suspected or detected. The examinations may require skills in several fields of expertise, such as legal, tax or information technology skills. The institution should document the results of its examinations and ensure to achieve the various examinations within the legislative framework applicable to it.

When an institution has been the target of an activity associated with financial crime, it should use the event as a learning opportunity and, if applicable, adjust its policies and procedures to reduce the likelihood of recurrence.

An institution may also be required to co-operate with the AMF during inspections and investigations authorized under the sectorial statutes applicable to it, the scope of this collaboration shall be limited to the extent permitted by applicable law. To this end, the AMF may, during these inspections or investigations, have access to information relating to instructions and mechanisms implemented by the institution under Part 1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and could then provide them to FINTRAC[20]. If applicable, the institution may also be required to co-operate during examinations and investigations carried out by financial crime fighting authorities, including the *Sûreté du Québec*, the Royal Canadian Mounted Police and FINTRAC.

[20] Section 2.1 (b) of the memorandum of understanding signed between FINTRAC and the AMF in June 2006.

Principle 7: Communication of information

The AMF expects a financial institution to communicate information regarding activities associated with financial crime to every appropriate authority, subject to applicable laws.

In order to facilitate the application and enforcement of fiscal, penal and criminal statutes or foreign legislation involving the same matters, the AMF recalls the legal obligation for a financial institution to communicate all information concerning activities associated with financial crime to every other appropriate regulator, including the AMF, FINTRAC,[21] the *Sûreté du Québec* and the *Agence du revenu du Québec*.

An institution also has the obligation to verify and report to the AMF on[22] the existence of property in their possession or control and belonging by an entity found on the list established by the Regulations Establishing a List of Entities[23].

[21] On June 19, 2006, the AMF and FINTRAC signed a memorandum of understanding ("MOU") to share information. The MOU also seeks to prevent duplication of efforts by FINTRAC and the AMF while reducing the burden of such efforts on the institutions and representatives targeted thereby. FINTRAC website: www.canafe.ca.

[22] Under subsection 83.11(2) of the *Criminal Code* (R.S.C., 1985, c. C-46), financial institutions subject to the AMF's oversight must provide such a report.

[23] SOR/2002-284made under article 83.05 of the Criminal Code.

Supervision of sound and prudent management practices and sound commercial practices

To foster the establishment of sound and prudent management practices within financial institutions and sound commercial practices, the AMF, acting within the scope of its supervisory activities, intends to assess the degree of compliance with the principles set forth in this guideline in light of the specific attributes of each institution. Consequently, it will examine the effectiveness and relevance of the strategies, policies and procedures adopted by financial institutions as well as the quality of oversight and control exercised by their board of directors and senior management.

Financial crime risk management practices are constantly evolving. The AMF therefore expects decision makers at financial institutions to remain current with best practices and to adopt such practices, to the extent that they address their needs.