AUTORITÉ
DES MARCHÉS
FINANCIERS

FINANCIAL CRIME RISK MANAGEMENT GUIDELINE

June 2012

Contents

Introduction

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

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 industry.

The scope of financial crime and the growing threat the risks related thereto 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 sector-based laws it administers, it is issuing this guideline with respect to financial crime risk management, to set out its expectations with respect to financial institutions' legal requirement to follow sound and prudent management practices and sound commercial practices.[2] The guideline favours a priori the need for financial institutions to implement risk management practices in order to prevent and detect activities associated with financial crime, and remedy same, the whole within an effective governance framework.

The principles set forth in this guideline favour a proactive approach aimed at mitigating 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 be combined with the sustained efforts of the AMF and other stakeholders, including the police forces and the 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.

Lastly, the AMF's expectations are based on core principles and guidelines issued by international organizations, including the Basel Committee on Banking Supervision (BCBS)[3], the Financial Action Task Force (FATF)[4] and the International Association of Insurance Supervisors (IAIS)[5].

---

1 *Insurers Act*, CQLR, c. A-32.1, section 463; *Deposit institution and deposit protection Act*, CQLR, c. I-13.2.2, section 42.2; *Act respecting financial services cooperatives*, CQLR, c. C-67.3, s. 565.1; *Trust companies and savings companies Act*, CQLR, c. S-29.02, section 254.

2 *Insurers Act*, CQLR, c. A-32.1, s. 50; *Act respecting financial services cooperatives*, CQLR, c. C-67.3, s. 66.1; *Deposit institution and deposit protection Act*, CQLR, c. I-13.2.2, s. 28.11; *Trust companies and savings companies Act*, CQLR, c. S-29.02, s. 34.

3 Basel Committee on Banking Supervision, *Customer due diligence for banks*, October 2001; *Core Principles Methodology*, October 2006; *Principles for the Sound Management of Operational Risk*, June 2011; *Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers*, May 2009.

4 Financial Action Task Force, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*, June 2007; *The FATF Forty Recommendations*, October 2003;*The IX Special Recommendations*, October 2004.

5 International Association of Insurance Supervisors, *Countering Fraud in Insurance (Insurance Core Principle 21 and Application Paper)*, October 2011; *Anti-Money Laundering and Combating the Financing of Terrorism (Insurance Core Principle 22)*, October 2011; *Insurance Core Principles, Standards, Guidance and Assessment Methodology*, October 2011; *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism*, October 2004;

1. 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,[6] money laundering, the illegal transfer of funds to financial or tax havens[7], 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 and detect activities that may be associated with financial crime, and remedy same effectively. These measures should also facilitate reviews, inspections and investigations relating to financial crime.

6 Generally speaking, and for purposes of this guideline, internal fraud means fraud committed by an officer, a director or an employee, whether or not in collusion with an internal or external party (for example, embezzlement by an employee) and external fraud means 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).

7 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

2. Framework for financial crime risk management

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[8] and senior management to be ultimately responsible for establishing sound and prudent financial crime risk governance management practices, including sound commercial practices.

In light of the roles and responsibilities incumbent upon them under the Governance Guideline,[9] the board of directors and senior management should, among other things:

- elaborate, approve and implement strategies, policies and procedures that 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.

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 of integrity, exemplary business conduct and ethical conduct among all employees of the institution in the performance of their duties;
- ensure that staff and officers have proper training to deal with financial crime risks and that the people assigned to risk management, compliance monitoring and primarily the prevention, detection and review of suspicious activities are honest and competent;[10]

Responsibility for developing and implementing the financial crime risk management strategy should be entrusted to the chief risk officer.[11] 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 reviews and investigations are communicated;
- ensure that the institution complies[12] with all laws, regulations and guidelines dealing with financial crime, such as the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA)[13] and the FINTRAC guidelines applicable to institutions.

Principle 2: Financial crime risk management

8 A reference to the board of directors can also include a board committee, such as a board committee established to examine specific issues.
9 Autorité des marchés financiers, *Governance Guideline*
10 Autorité des marchés financiers, *Governance Guideline*
11 Autorité des marchés financiers, *Integrated Risk Management Guideline*
12 Autorité des marchés financiers, *Compliance Guideline*
13 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17

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

The financial institution should take financial crime risks into account within its integrated risk management framework. Accordingly, it should give consideration to the interrelationships and interdependencies between risks.

The integrated risk management approach requires that financial crime risks to which the institution may be exposed be identified, assessed and quantified and that measures be implemented to mitigate such risks so as to reduce the probability of operational events associated with financial crime and their potential impact on the institution.

To this end, the institution should take into account of its vulnerability to the risks it faces particularly with respect to the following elements:

- internal factors such as:
  - its organizational structure, the nature of its activities, its information systems, its strategic orientations, its policies, the quality of its internal control 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, their nature and the volume of their local and cross-border transactions;
  - the information technology used;
  - its business dealings, including the outsourcing of certain functions;
  - employee versatility and turnover, employee expertise about financial crime, the quality of its labour relations, pre-hiring and periodic post-hiring background checks on employees, particularly for higher-risk functions.
- external factors such as:
  - the methods used by perpetrators of financial crime activities and the possibility of operational incidents and their potential impact;
  - legal, regulatory and normative requirements relating to the fight against financial crime, including the PCMLTFA, and changes to the designated persons list established by the United Nations;[14]
  - the economic and social context, new threats and opportunities involving financial crime as well as changes in the techniques and methods used;[15]
  - changes in international orientations for fighting financial crime.

Principle 3: Intra-group management

[14] Reference: *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. Additional information is available on the AMF website: https://lautorite.qc.ca/en/professionals/obligations-and-administrative-procedures/application-of-the-united-nations-resolution-to-suppress-terrorism/

[15] 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. https://lautorite.qc.ca/en/general-public/fraud-prevention/investor-warnings/

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 or even adversely affect their solvency and, ultimately, the reputation of the entire group, locally, nationally and internationally.

Consequently, it is important to adopt a comprehensive approach to financial crime risk management at the group level so that standards applicable to the institution are coherent across the group and entities forming part of the group can exchange information. Transparency and the free flow of information will make it possible to identify and assess areas of vulnerability and reduce financial crime risks.

Principle 4: Customer vigilance

The AMF expects a financial institution to exercise 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.

The financial institution should be vigilant with respect to customers considering the extent of risks associated primarily with monetary transactions, insurance products and investment products offered by the institution.

Know your customer

Knowing customers is an essential component of financial crime risk management. It contributes to reducing the likelihood of operational events involving the financial institution.

Knowing customers should also include their dealings with the institution's other customers and, if applicable, with other entities forming part of the institution's group. Increased 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.

To the extent possible, an institution should conduct increased diligence 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]

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

- who are the mandataries of a customer or the beneficiaries of an insurance contract.[17]

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 and monitoring 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 and 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 transactions involving large 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, be it the customer or another person.

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.

Principle 5: Vigilance with respect to employees, officers and business relations

> The AMF expects a financial institution to exercise continuous vigilance with respect to employees, officers and business relations 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 dealings, particularly its suppliers.

Identifying vulnerabilities

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

18 Autorité des marchés financiers, *Commercial Practices Guideline* and *An Act respecting the protection of personal information in the private sector*, R.S.Q. c. P-39.1.

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

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:

- collusion or any form of corruption, such as bribes, kickbacks or secret commissions from a supplier, or the falsification of documents or data;
- unauthorized use of customers' personal information;
- payments to fictitious suppliers for services not rendered to the institution;
- employee theft of money or property belonging to the institution;
- 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 of customers' personal information by employees;
- 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: Review of suspicious activities

> The AMF expects a financial institution to carry out reviews 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 reviews may require skills in several fields of expertise, such as legal, tax or information technology skills. The institution should document the results of its reviews and ensure that it carries out the reviews in accordance with the applicable legislative framework.

When an institution has been the target of an activity associated with financial crime, it should, where appropriate, use the event to 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 sector-based laws applicable to it, with the extent of such co-operation should be limited to the purposes permitted by the applicable laws. In this regard, when carrying out such inspections or investigations, the AMF may have access to information regarding the instructions and mechanisms implemented by the institution under Part 1 of the PCMLTFA and may then communicate such information to FINTRAC. If applicable, the institution may also be required to co-operate during reviews and investigations

carried out by financial crime fighting authorities, including the Sûreté du Québec, the Royal Canadian Mounted Police and FINTRAC.

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.

The AMF reminds financial institutions that, in order to facilitate the application and enforcement of fiscal, penal and criminal laws or foreign legislation involving the same matters, financial institutions have the legal obligation to communicate all information concerning activities associated with financial crime to every other appropriate authority, including the AMF, FINTRAC, the *Sûreté du Québec*, the other police forces and the *Agence du Revenu du Québec*.

The AMF and FINTRAC signed a memorandum of understanding[20] (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.

An institution also has the obligation to verify and report to the AMF[21] on the existence of property in its possession or control that is owned by an entity found on the list established by the *Regulations Establishing a List of Entities*.[22]

[20] Memorandum of Understanding to Share Information between FINTRAC and the AMF, signed on June 19, 2006. www.canafe-fintrac.gc.ca

[21] 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 to the AMF.

[22] Regulations Establishing a List of Entities (SOR/2002-284) made under section 83.05 of the Criminal Code.